BPR Group S.r.l.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. N. 231/2001

Prima Emissione del 02/04/2025

Approvato con delibera dell'Amministratore Unico in data 02 aprile 2025

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. N. 231/2001

Contenuti

PARTE GENERALE

PARTE SPECIALE

ALLEGATI

1. CODICE ETICO
2. PROTOCOLLI SPECIALI DI PREVENZIONE
3. MODELLI
4. REGOLAMENTO DELL'ORGANISMO DI VIGILANZA
5. ORGANIGRAMMA
6. MAPPA DEI RISCHI

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. N. 231/2001

PARTE GENERALE

INDICE

1. STORIA E DESCRIZIONE DELLA SOCIETA' 3

2. PREMESSA METODOLOGICA 8

3. IL DECRETO LEGISLATIVO N. 231/2001
- 3.1. NATURA DELLA RESPONSABILITA' DELL'ENTE 9
- 3.2. I SOGGETTI DESTINATARI DELLA DISCIPLINA 10
- 3.3. I REATI PRESUPPOSTO 11
- 3.4. I SOGGETTI CHE COMMETTONO IL REATO 12
- 3.5. INTERESSE E VANTAGGIO DELL'ENTE 27
- 3.6. TIPOLOGIA DI SANZIONI IRROGABILI 28

4. IL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO
- 4.1. GLI ELEMENTI COMPONENTI IL MODELLO 29
- 4.2. LA FUNZIONE ESIMENTE DEL MODELLO 30
- 4.3. OBIETTIVI E FINALITA' 31
- 4.4. APPROVAZIONE E RECEPIMENTO DEL MODELLO 32
- 4.5. MODIFICHE ED INTEGRAZIONI DEL MODELLO 33
- 4.6. ATTUAZIONE DEL MODELLO 33
- 4.7. I PRINCIPI GENERALI DI CONTROLLO 33

5. L'ORGANISMO DI VIGILANZA
- 5.1. CARATTERISTICHE E FUNZIONI 34
- 5.2. REPORTING VERSO L'ORGANISMO DI VIGILANZA 37
- 5.3. RESPONSABILITA' DELL'ORGANISMO DI VIGILANZA 39

6. LA DIFFUSIONE DEL MODELLO
- 6.1. FORMAZIONE DEL PERSONALE INTERNO 39
- 6.2. SELEZIONE DI COLLABORATORI ESTERNI E PARTNER NELLE AREE ESPOSTE A RISCHIO 40

7. SISTEMA DISCIPLINARE
- 7.1. FINALITA' 45
- 7.2. MISURE SANZIONATORIE IN CASO DI VIOLAZIONI DA PARTE DEL PERSONALE DIPENDENTE NON DIRIGENTE 46
- 7.3. MISURE SANZIONATORIE IN CASO DI VIOLAZIONI DA PARTE DEL PERSONALE DIPENDENTE DIRIGENTE 47
- 7.4. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI E DEI SINDACI 44
- 7.5. COLLABORATORI, CONSULENTI, FORNITORI E ALTRI SOGGETTI TERZI AVENTI RAPPORTI CONTRATTUALI CON BPR GROUP SRL 44
- 7.6. MISURE NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA 45

8. ADOZIONE, AUDIT PERIODICO E RIESAME
- 8.1. ADOZIONE E AGGIORNAMENTO DEL MODELLO DI ORGANIZZAZIONE E GESTIONE 46
- 8.2. VERIFICHE ISPETTIVE INTERNE 47
- 8.3. RIESAME DELLA DIREZIONE 48

1. STORIA E DESCRIZIONE DELLA SOCIETA'

Ragione sociale:	BPR Group srl
Sede legale:	Moglia (MN) via IV novembre n° 120
Numero R.E.A.:	MN - 208955
C.F.:	01920580204
Partita I.V.A.:	01920580204
Iscrizione Registro delle Imprese di Mantova	20/04/2000
Capitale sociale	€ 30.000,00 (interamente versato)

BPR Group è stata fondata nel 2000 ed è di proprietà dei due soci Marco Malavasi (Legale Rappresentante e Amministratore unico) e Cristina Vincenzi.

E' società di consulenza organizzativa ed engineering per lo sviluppo di sistemi di automazione, specializzata in Lean Thinking e Innovazione.

BPR Group opera con una visione d'insieme che consente di trovare la soluzione più adatta alle esigenze del Cliente per la analisi e riprogettazione di sistemi produttivi ed aree logistiche, nell'ambito di svariati settori industriali quali principalmente: Meccanico, Oleodinamico, Automotive, Impiantistica, Alimentare, Chimico, Biomedicale, Elettrodomestico, Civile, Legno, Servizi.

Gli ambiti di attività di BPR Group sono: consulenza, engineering, formazione, industria 4.0.

La sede consta di un'area uffici ed un'area produttiva, suddivisa in officina meccanica e montaggio impianti.

Il settore Engineering opera prevalentemente in sede, in ufficio tecnico area montaggio ed officina meccanica. In officina all'occorrenza e su richiesta del cliente vengono prodotti articoli su misura, prototipi, piccole attrezzature, ecc. La divisione Engineering è costituita da progettisti e tecnici esperti nella industrializzazione, progettazione, costificazione e sviluppo di applicazioni tecniche integrate nei processi produttivi industriali. I progetti sviluppati si caratterizzano per l'elevato contenuto innovativo, la massima efficienza flessibilità, ripetibilità e qualità delle soluzioni.

L'attività di consulenza e formazione è svolta prevalentemente presso le sedi dei clienti e solo occasionalmente nella sede di BPR Group. Considerando il tipo di lavoro effettuato gli addetti alla mansione hanno pertanto necessità di adattarsi alle esigenze del cliente per quanto riguarda, orari, tempistiche di intervento, trasferte, etc.

BPR Group è una piccola impresa ed applica il CCNL commercio terziario Confcommercio.

I clienti di BPR Group operano in svariati settori merceologici: Meccanico, Oleodinamico, Automotive, Impiantistica, Alimentare, Chimico, Biomedicale, Elettrodomestico, Civile, Legno, Servizi, con dimensioni che vanno dalla piccola, media e grande impresa.

I clienti vengono serviti con contratti specifici in base alle loro esigenze dopo avere eseguito una approfondita e condivisa analisi preliminare.

Il mercato è molto vasto e occupa svariate aree in tutta Italia, concentrandosi principalmente nelle zone dell'Emilia Romagna e Lombardia.

La clientela di BPR Group S.r.l. è costituita sia da clienti con collaborazioni continuative, sia da clienti che si avvalgono di contratti specifici e di breve durata.

BPR GROUP Srl non intrattiene rapporti commerciali a livello transnazionale.

L'azienda si avvale di collaboratori esterni che svolgono attività di formazione e consulenza presso i clienti. Si avvale inoltre di fornitori di tecnologia hardware, di software e di consulenti aziendali ambito: sicurezza, qualità, privacy, informatico, paghe, contabile e legale.

Dal 2015 BPR Group collabora con IT Innovative Technology s.r.l. startup con sede legale a Macerata e sede operativa a Moglia (MN), per sviluppare prodotti e servizi ad alto valore tecnologico che permettano alle aziende clienti di migliorare i propri processi produttivi in termini qualitativi e di performance. Collabora inoltre con alcune Università anche attraverso l'attivazione di tirocini curriculari.

BPR Group ha una struttura organizzativa verticistica di tipo tradizionale con a capo un Amministratore unico.

L'organigramma di BPR prevede le seguenti funzioni:

1. Direzione generale: ruolo ricoperto dal legale rappresentante dell'azienda;
2. CFO: sovraintende le attività amministrativo-finanziarie della società;
3. Responsabile Amministrativo: gestisce contabilità e segreteria;
4. Controller: esercita la funzione di controllo di gestione;
5. Responsabile Marketing: cura le strategie di comunicazione e marketing per trasferire a lead prospect e clienti attivi i servizi offerti da BPR;
6. Responsabile R&D: cura la progettazione e implementazione di nuovi servizi in linea con gli sviluppi del mercato;
7. Responsabile del Personale: cura le attività di selezione, amministrazione e gestione del personale dipendente;
6. RSPP e Gestione Ambiente: svolge le funzioni di Responsabile del servizio di prevenzione e protezione e si occupa degli adempimenti relativi alla gestione ambientale;

7. Business Developer: collabora con la direzione per definire periodicamente strategie e obiettivi in materia di priorità, efficienza, qualità, redditività, gestione clienti. E' figura di coordinamento delle aree: consulenza strategica, Operations, Qualità e Sistemi informativi cui sono preposti i relativi responsabili;
8. Responsabile consulenza strategica: sviluppa il business e coordina le risorse e le attività di area;
9. Responsabile Operation: sviluppa il business e coordina le risorse e le attività di area garantendo la sinergia tra consulenza, engineering e le altre funzioni aziendali;
10. Responsabile engineering: coordina e supervisiona le attività di progettazione e realizzazione di soluzioni per i clienti;
10. Responsabile sistemi informativi: presidia e coordina la gestione dell'area per garantire business continuity e sicurezza dei dati;
11. Responsabile qualità: si occupa del monitoraggio e dell'aggiornamento del sistema di gestione della Qualità certificato UNI EN ISO 9001:2015.

Le procedure ed i sistemi di controllo presenti ed applicati in azienda riguardano:

- **il sistema organizzativo interno**

  Il sistema organizzativo interno garantisce: adeguata formalizzazione, chiarezza della linea gerarchica e funzionale e sull'allocazione dei poteri, nonché segregazione delle funzioni.

  Consta di:

  - atto costitutivo e statuto;
  - deleghe di funzioni e di spesa;
  - organigramma funzionale e nominativo aggiornato;
  - sistema disciplinare;
  - sistema di formazione del personale.

- **il sistema informativo**

  La Società opera in osservanza delle prescrizioni e procedure in materia di protezione dei dati personali enunciate nel GDPR 2016/679, nonché nel D. Lgs. n. 196/2003 (Codice della privacy), così come modificato dal decreto legislativo di adeguamento 101/2018.

- **il sistema dei controlli amministrativo-contabili**

  La Società garantisce, mediante molteplici livelli di controllo - autocontrollo operatori, dei responsabili, dell'Amministratore unico - il regolare svolgimento dell'attività nel rispetto della normativa fiscale, contabile e societaria, nonché delle norme statutarie.

  Garantisce, in particolare:

  - il monitoraggio della gestione attraverso sistematici controlli dell'andamento economico-finanziario e patrimoniale della Società;
  - il monitoraggio puntuale del ciclo attivo e del ciclo passivo anche a mezzo di apposito gestionale;
  - il controllo contabile interno con il supporto del commercialista esterno;
  - il controllo di gestione operato dalle funzioni amministrative in collaborazione con il Responsabile sistemi informativi;
  - il controllo effettuato dagli organi esterni inerente ai sistemi qualità certificati;

- **Il sistema di controllo in materia di salute e sicurezza sul lavoro**

  La Società attua i contenuti del d. lgs. n. 81/2008 e della disciplina speciale in materia di salute e sicurezza sul lavoro. Sono nominati RSPP, medico competente, gli addetti alle squadre di emergenza e primo soccorso. È presente il rappresentante dei lavoratori per la sicurezza. Inoltre il management di BPR GROUP Srl si assicura che tutto il personale riceva una regolare e documentata formazione in materia di salute e sicurezza, non trascurando altresì la comunicazione a tutti i livelli dell'organizzazione. L'azienda fornisce al personale adeguati dispositivi di protezione individuale e, ove necessario, l'addestramento a cura dei preposti.

- **I sistemi di gestione e le certificazioni**

  BPR Group è dotata di sistema di gestione della qualità certificato UNI EN ISO 9001:2015 per i settori EA35 e EA37 per l'attività di "Progettazione, sviluppo ed erogazione di servizi di consulenza e formazione specializzati in Lean Thinking e Innovazione".

2. PREMESSA METODOLOGICA

Il presente documento è stato redatto ai sensi e per gli effetti di cui al Decreto Legislativo 8 Giugno 2001, n. 231.

Il decreto ha introdotto nel nostro ordinamento una nuova forma di responsabilità, poiché prevede la possibilità di infliggere sanzioni agli enti collettivi nel caso in cui questi abbiano commesso un reato a proprio interesse o vantaggio attraverso i soggetti che operano nel contesto dell'ente, siano essi soggetti apicali o subordinati.

Con la definizione del presente Modello di organizzazione, gestione e controllo BPR Group istituisce ed implementa un sistema strutturato ed organico di procedure e regole di comportamento e di attività di controllo al fine di prevenire la commissione delle diverse tipologie di illecito previste dal d. lgs. n. 231/2001 e di assicurare quindi condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

I principi e le disposizioni del presente documento trovano applicazione nei confronti degli amministratori, dei soci, dei dipendenti, dei sindaci e dei revisori ed infine di chiunque operi per conto della Società in virtù di un rapporto di natura contrattuale, di qualsivoglia tipologia, eventualmente anche temporaneo, nei limiti del proprio compito e delle responsabilità ad esso connesse.

L'adeguamento del sistema organizzativo e gestionale di BPR Group alle esigenze delineate dal Decreto Legislativo n. 231/2001 è stato coordinato dall' Amministratore Unico con l'assistenza di professionisti esterni, esperti nei diversi settori interessati dal D.Lgs. n. 231/2001, ad essa collegati.

L'attività del gruppo di lavoro finalizzata alla predisposizione del Modello si è concretizzata:

- nella identificazione di settori/attività/aree sensibili, con riferimento ai reati richiamati dal D. Lgs. n. 231/2001. Per giungere a tale risultato il team ha analizzato la struttura organizzativa e societaria della Società, previa acquisizione della relativa documentazione. Ha, inoltre, incontrato in più occasioni presso la sede della Società l'Amministratore unico e le diverse funzioni aziendali;
- nell'esame analitico delle aree sensibili, con prefigurazione delle modalità e degli strumenti attraverso i quali sarebbe possibile commettere i reati elencati nel Decreto da

parte dell'impresa, dai suoi organi amministrativi, dai dipendenti ed, in generale, dalle figure contemplate dall'art. 5 del Decreto (anche attraverso incontri e colloqui con i soggetti interessati);

- nell'individuazione delle procedure e dei protocolli esistenti – siano essi formalizzati o meno – in riferimento alle sole aree individuate come a rischio di reato;
- nella definizione di *standards* di comportamento e di controllo ovvero per le attività che, concordemente con la Società, si è ritenuto opportuno regolamentare;
- nella disciplina delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di reati;
- nell'individuazione del/i soggetto/i incaricato/i di vigilare sulla concreta applicazione del presente modello (di seguito Organismo di Vigilanza oppure OdV) con contestuale predisposizione del relativo regolamento e sistema di *reporting* da e verso l'Organismo di Vigilanza stesso;
- nell'integrazione del Codice Etico;
- nella previsione di un sistema disciplinare idoneo a sanzionare sia il mancato rispetto delle misure indicate nel Modello, sia le violazioni del Codice Etico.

3. IL DECRETO LEGISLATIVO N. 231/2001

3.1 Natura della responsabilità dell'ente

Il Decreto Legislativo n. 231/2001 ha introdotto una forma di responsabilità degli enti definita come amministrativa ma la cui natura è essenzialmente penale.

La competenza a conoscere degli illeciti amministrativi dell'ente appartiene al giudice penale, che la esercita con le garanzie proprie del procedimento penale. Inoltre, all'eventuale accertamento della responsabilità dell'ente consegue l'applicazione di sanzioni penali che possono risultare gravi e pregiudizievoli per la vita dell'ente, quali, tra le altre, la sospensione o la revoca di autorizzazioni, licenze o concessioni, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi, sino alla interdizione anche definitiva dall'esercizio dell'attività. É inoltre sempre disposta la confisca del prezzo o del profitto del reato, ovvero di somme di denaro,

beni o altre utilità di valore equivalente. Queste sanzioni conseguono alla pronuncia di una sentenza di condanna dell'ente, ma possono essere applicate anche in via cautelare, secondo gli artt. 45 e ss. del Decreto, ove sussistano gravi indizi per ritenere fondata la responsabilità.

La responsabilità dell'ente per gli illeciti amministrativi si aggiunge - e non si sostituisce - alla responsabilità personale degli autori del reato, siano essi soggetti apicali o subalterni.

3.2 I soggetti destinatari della disciplina

I soggetti destinatari della normativa sono indicati all'art. 1 del decreto.

Essi sono:

- le persone giuridiche (enti ed associazioni forniti di personalità giuridica), ivi comprese le fondazioni, le società di capitali (piccole, medie o grandi che esse siano) e quelle cooperative;
- gli enti (società di persone ed associazioni) anche sprovvisti di personalità giuridica;
- gli enti pubblici che agiscono *iure privatorum*.

3.3 I presupposti di contestazione della responsabilità amministrativa

I presupposti della responsabilità amministrativa degli enti si rinvengono nell'art. 5 del Decreto:

"L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

L'ente non risponde se le persone indicate nel comma 1 hanno agito nell'interesse esclusivo proprio o di terzi".

In sintesi, affinché quindi sorga la responsabilità ex d.lgs. 231/2001 è necessario che:

- venga commesso un reato ricompreso nel novero dei c.d. "reati – presupposto";

- lo stesso sia commesso da un soggetto inserito "organicamente" nell'ente, sia che esso ricopra una posizione apicale (lett. a), sia che esso ricopra una posizione subordinata (lett. b);
- il reato sia commesso ad interesse o a vantaggio dell'ente.

Il decreto si applica in relazione sia a reati commessi in Italia sia a quelli commessi all'estero, purché l'ente abbia nel territorio dello Stato italiano la sede principale e nei confronti dello stesso non proceda direttamente lo Stato del luogo in cui è stato commesso il reato.

3.4 I reati presupposto

I reati presupposto, ossia le fattispecie criminose che possono costituire fonte di responsabilità amministrativa dell'ente, sono individuati nella sezione III del d. lgs. n. 231/01.

Le fattispecie attualmente previste, in virtù di successivi interventi normativi che hanno ampliato il catalogo dei reati presupposto, sono le seguenti:

1. Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24, D.Lgs. n. 231/2001) [articolo modificato dalla L. 161/2017, dal D.Lgs. n. 75/2020 e dalla L. n. 137/2023]

- Malversazione di erogazioni pubbliche (art. 316-bis c.p.) [articolo modificato dal D.L. n. 13/2022]
- Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.) [articolo modificato dalla L. n. 3/2019 e dal D.L. n. 13/2022]
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art.640, comma 2, n.1, c.p.) [articolo modificato dal D.Lgs. n. 75/2020 e dalla Legge n. 90/2024]
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.) [articolo modificato dal D.L. n. 13/2022]
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p. introdotto dal d. lgs. n. 195/2021)

- Frode nelle pubbliche forniture (art. 356 c.p.) [introdotto dal D.Lgs. n. 75/2020]
- Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n.898) [introdotto dal D.Lgs. n. 75/2020]
- Turbata libertà degli incanti (art. 353 c.p.) [articolo introdotto dalla L. n. 137/2023]
- Turbata libertà del procedimento di scelta del contraente (art. 353-bis) [articolo introdotto dalla L. n. 137/2023]

2. Delitti informatici e trattamento illecito di dati (Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019]

- Documenti informatici (art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) [articolo modificato dalla Legge n. 90/2024]
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.) [articolo modificato dalla Legge n. 238/2021 e modificato dalla Legge n. 90/2024]
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) [articolo modificato dalla Legge n. 238/2021 e dalla Legge n. 90/2024]
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) [articolo modificato dalla Legge n. 238/2021 e dalla Legge n. 90/2024]
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.) [articolo modificato dalla Legge n. 90/2024]
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.) [articolo modificato dalla Legge n. 90/2024]

- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) [articolo modificato dalla Legge n. 90/2024]
- 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.) [articolo introdotto dalla Legge n. 90/2024]
- Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies c.p.) [articolo modificato dalla Legge n. 90/2024]
- Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)
- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)
- Estorsione (art. 629, comma 3, c.p.) [articolo aggiunto dalla Legge n. 90/2024]

3. Delitti di criminalità organizzata (Art. 24-ter, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009 e modificato dalla L. 69/2015]

- Associazione di tipo mafioso anche straniere (art. 416-bis c.p.) [articolo modificato dalla L. n. 69/2015]
- Associazione per delinquere (art. 416 c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.) [così sostituito dall´art. 1, comma 1, L. 17 aprile 2014, n. 62, a decorrere dal 18 aprile 2014, ai sensi di quanto disposto dall´art. 2, comma 1 della medesima L. 62/2014)
- Sequestro di persona a scopo di estorsione (art. 630 c.p.)
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990, n. 309) [comma 7-bis aggiunto dal D.Lgs. n. 202/2016]
- Tutti i delitti se commessi avvalendosi delle condizioni previste dall´art. 416-bis c.p. per agevolare l´attività delle associazioni previste dallo stesso articolo (L. 203/91)
- 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'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110 (art. 407, co. 2, lett. a), numero 5), c.p.p.)

4. Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità e corruzione (Art. 25, D.Lgs. n. 231/2001) [modificato dalla L. n. 190/2012, dalla L. 3/2019, dal D.Lgs. n. 75/2020 e dalla L. 112/2024]

- Concussione (art. 317 c.p.) [articolo modificato dalla L. n. 69/2015]
- Corruzione per l'esercizio della funzione (art. 318 c.p.) [modificato dalla L. n. 190/2012, L. n. 69/2015 e L. n. 3/2019]
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.) [articolo modificato dalla L. n. 69/2015]
- Circostanze aggravanti (art. 319-bis c.p.)
- Corruzione in atti giudiziari (art. 319-ter c.p.) [articolo modificato dalla L. n. 69/2015]
- Induzione indebita a dare o promettere utilità (art. 319-quater c.p.) [articolo aggiunto dalla L. n. 190/2012 e modificato dalla L. n. 69/2015]
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
- Pene per il corruttore (art. 321 c.p.)
- Istigazione alla corruzione (art. 322 c.p.)
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, abuso d'ufficio, di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.) [articolo modificato dalla L. n. 190/2012, dalla L n. 3/2019 e dal D.L. n. 92/2024]
- Traffico di influenze illecite (art. 346-bis c.p.) [modificato dalla L. 3/2019 e dalla L. 112/2024]
- Peculato (limitatamente al primo comma) (art. 314 c.p.) [introdotto dal D.Lgs. n. 75/2020]

- Peculato mediante profitto dell'errore altrui (art. 316 c.p.) [introdotto dal D.Lgs. n. 75/2020]
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.) [articolo introdotto dalla L. n. 112/2024]

5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis, D.Lgs. n. 231/2001) [articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009; modificato dal D.Lgs. 125/2016]

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

6. Delitti contro l'industria e il commercio (Art. 25-bis.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.)

- Turbata libertà dell'industria o del commercio (art. 513 c.p.)
- Frodi contro le industrie nazionali (art. 514 c.p.)
- Frode nell'esercizio del commercio (art. 515 c.p.)
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.)

7. Reati societari (Art. 25-ter, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. 69/2015, dal D.Lgs. n.38/2017 e dal D.Lgs. n. 19/2023]

- False comunicazioni sociali (art. 2621 c.c.) [articolo modificato dalla L. n. 69/2015]
- Fatti di lieve entità (art. 2621-bis c.c.)
- False comunicazioni sociali delle società quotate (art. 2622 c.c.) [articolo modificato dalla L n. 69/2015]
- Impedito controllo (art. 2625, comma 2, c.c.)
- Indebita restituzione di conferimenti (art. 2626 c.c.)
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.) [aggiunto dalla legge n. 262/2005]
- Formazione fittizia del capitale (art. 2632 c.c.)
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)

- Corruzione tra privati (art. 2635 c.c.) [aggiunto dalla legge n. 190/2012; modificato dal D.Lgs. n. 38/2017 e dalla L. n. 3/2019]
- Istigazione alla corruzione tra privati (art. 2635-bis c.c.) [aggiunto dal D.Lgs. n. 38/2017 e modificato dalla L. n. 3/2019]
- Illecita influenza sull'assemblea (art. 2636 c.c.)
- Aggiotaggio (art. 2637 c.c.)
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.)
- False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023) [aggiunto dal D.Lgs. n. 19/2023]

8. Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (Art. 25-quater, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2003]

- Associazioni sovversive (art. 270 c.p.)
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.)
- Circostanze aggravanti e attenuanti (art. 270-bis.1 c.p.) [introdotto dal D.Lgs. n. 21/2018]
- Assistenza agli associati (art. 270 ter c.p.)
- Arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.)
- Organizzazione di trasferimento per finalità di terrorismo (art. 270-quater.1) [introdotto dal D.L. n. 7/2015, convertito, con modificazioni, dalla L. n. 43/2015]
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies c.p.)
- Finanziamento di condotte con finalità di terrorismo (L. n. 153/2016, art. 270 quinquies.1 c.p.)

- Sottrazione di beni o denaro sottoposti a sequestro (art. 270 quinquies.2 c.p.)
- Condotte con finalità di terrorismo (art. 270 sexies c.p.)
- Attentato per finalità terroristiche o di eversione (art. 280 c.p.)
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis c.p.)
- Atti di terrorismo nucleare (art. 280 ter c.p.)
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.)
- Sequestro a scopo di coazione (art. 289-ter c.p.) [introdotto dal D.Lgs. 21/2018]
- Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo (art. 302 c.p.)
- Cospirazione politica mediante accordo (art. 304 c.p.)
- Cospirazione politica mediante associazione (art. 305 c.p.)
- Banda armata: formazione e partecipazione (art. 306 c.p.)
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.)
- Impossessamento, dirottamento e distruzione di un aereo (L. n. 342/1976, art. 1)
- Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2)
- Sanzioni (L. n. 422/1989, art. 3)
- Pentimento operoso (D.Lgs. n. 625/1979, art. 5)
- Convenzione di New York del 9 dicembre 1999 (art. 2)

9. Pratiche di mutilazione degli organi genitali femminili (Art. 25-quater.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2006]

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

10. Delitti contro la personalità individuale (Art. 25-quinquies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003; modificato dalla L. n. 199/2016]

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
- Prostituzione minorile (art. 600-bis c.p.)

- Pornografia minorile (art. 600-ter c.p.)
- Detenzione o accesso a materiale pornografico (art. 600-quater) [articolo modificato dalla Legge n. 238/2021]
- Pornografia virtuale (art. 600-quater.1 c.p.) [aggiunto dall'art. 10, L. 6 febbraio 2006 n. 38]
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.)
- Tratta di persone (art. 601 c.p.) [modificato dal D.Lgs. 21/2018]
- Acquisto e alienazione di schiavi (art. 602 c.p.)
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)
- Adescamento di minorenni (art. 609-undecies c.p.) [articolo modificato dalla Legge n. 238/2021]

11. Reati di abuso di mercato (Art. 25-sexies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005]

- Manipolazione del mercato (art. 185 D.Lgs. n. 58/1998) [articolo modificato dal D.Lgs. 107/2018 e dalla Legge n. 238/2021]
- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 D.Lgs. n. 58/1998) [articolo modificato dalla Legge n. 238/2021]

12. Altre fattispecie in materia di abusi di mercato (Art. 187-quinquies TUF) [articolo modificato dal D.Lgs. n. 107/2018]

- Divieto di manipolazione del mercato (art. 15 Reg. UE n. 596/2014)
- Divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art. 14 Reg. UE n. 596/2014)

13. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Art. 25-septies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007; modificato L. n. 3/2018]

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

14. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonchè autoriciclaggio (Art. 25-octies, D.Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014 e dal D.Lgs. n. 195/2021]

- Ricettazione (art. 648 c.p.) [articolo modificato dal D.Lgs. 195/2021]
- Riciclaggio (art. 648-bis c.p.) [articolo modificato dal D.Lgs. 195/2021]
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.) [articolo modificato dal D.Lgs. 195/2021]
- Autoriciclaggio (art. 648-ter.1 c.p.) [articolo modificato dal D.Lgs. 195/2021]

15. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (Art. 25-octies.1, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. 184/2021 e modificato dalla L. n. 137/2023]

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.)
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)
- Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.)
- Trasferimento fraudolento di valori (art. 512-bis) [articolo introdotto dalla L. n. 137/2023 e modificato dal D.L. 19/2024]

16. Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1 comma 2, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. 184/2021]

17. Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009; modificato dalla L. n. 93/2023]

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a) bis)
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1)
- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2)
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941) [modificato dalla L. n. 93/2023]

- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

18. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 116/2009]

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

19. Reati ambientali (Art. 25-undecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 121/2011, modificato dalla L. n. 68/2015, modificato dal D.Lgs. n. 21/2018 e modificato dalla L. n. 137/2023]

- Inquinamento ambientale (art. 452-bis c.p.) [articolo modificato dalla L. n. 137/2023]
- Disastro ambientale (art. 452-quater c.p.) [articolo modificato dalla L. n. 137/2023]
- Delitti colposi contro l´ambiente (art. 452-quinquies c.p.)
- Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)
- Circostanze aggravanti (art. 452-octies c.p.)
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.)
- Distruzione o deterioramento di habitat all´interno di un sito protetto (art. 733-bis c.p.)
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n.150/1992, art. 1, art. 2, art. 3-bis e art. 6)

- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D. Lgs n.152/2006, art. 137)
- Attività di gestione di rifiuti non autorizzata (D. Lgs n.152/2006, art. 256)
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D. Lgs n. 152/2006, art. 257)
- Traffico illecito di rifiuti (D. Lgs n.152/2006, art. 259)
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D. Lgs n.152/2006, art. 258)
- Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.) [introdotto dal D.Lgs. n. 21/2018]
- False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (D. Lgs n.152/2006, art. 260-bis)
- Sanzioni (D.Lgs. n. 152/2006, art. 279)
- Inquinamento doloso provocato da navi (D. Lgs. n.202/2007, art. 8)
- Inquinamento colposo provocato da navi (D. Lgs. n.202/2007, art. 9)
- Cessazione e riduzione dell´impiego delle sostanze lesive (L. n. 549/1993 art. 3)

20. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 109/2012, modificato dalla Legge 17 ottobre 2017 n. 161 e dal D.L. n. 20/2023]

- Disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3 bis, 3 ter e comma 5, D.Lgs. n. 286/1998) [articolo modificato dal D.L. n. 20/2023]
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12 bis, D.Lgs. n. 286/1998)

21. Razzismo e xenofobia (Art. 25-terdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla Legge 20 novembre 2017 n. 167, modificato dal D.Lgs. n. 21/2018]

- Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (art. 604-bis c.p.) [aggiunto dal D.Lgs. n. 21/2018]

22. 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. n. 231/2001) [articolo aggiunto dalla L. n. 39/2019]

- Frodi in competizioni sportive (art. 1, L. n. 401/1989)
- Esercizio abusivo di attività di giuoco o di scommessa (art. 4, L. n. 401/1989)

23. Reati Tributari (Art. 25-quinquesdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 157/2019 e dal D.Lgs. n. 75/2020]

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000)
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000)
- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000)
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]
- Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]
- Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000) [articolo introdotto dal D.Lgs. n. 75/2020 e modificato dal D.Lgs. n. 87/2024]

24. Contrabbando (Art. 25-sexiesdecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 75/2020]

- Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali (art. 282 D.P.R. n. 43/1973)

- Contrabbando nel movimento delle merci nei laghi di confine (art. 283 D.P.R. n. 43/1973)
- Contrabbando nel movimento marittimo delle merci (art. 284 D.P.R. n. 43/1973)
- Contrabbando nel movimento delle merci per via aerea (art. 285 D.P.R. n. 43/1973)
- Contrabbando nelle zone extra-doganali (art. 286 D.P.R. n. 43/1973)
- Contrabbando per indebito uso di merci importate con agevolazioni doganali (art. 287 D.P.R. n. 43/1973)
- Contrabbando nei depositi doganali (art. 288 D.P.R. n. 43/1973)
- Contrabbando nel cabotaggio e nella circolazione (art. 289 D.P.R. n. 43/1973)
- Contrabbando nell'esportazione di merci ammesse a restituzione di diritti (art. 290 D.P.R. n. 43/1973)
- Contrabbando nell'importazione od esportazione temporanea (art. 291 D.P.R. n. 43/1973)
- Contrabbando di tabacchi lavorati esteri (art. 291-bis D.P.R. n. 43/1973)
- Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri (art. 291-ter D.P.R. n. 43/1973)
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater D.P.R. n. 43/1973)
- Altri casi di contrabbando (art. 292 D.P.R. n. 43/1973)
- Circostanze aggravanti del contrabbando (art. 295 D.P.R. n. 43/1973)

25. Delitti contro il patrimonio culturale (Art. 25-septiesdecies, D.Lgs. n. 231/2001) [Articolo aggiunto dalla L. n. 22/2022 e modificato dalla L. n. 6/2024]

- Furto di beni culturali (art. 518-bis c.p.)
- Appropriazione indebita di beni culturali (art. 518-ter c.p.)
- Ricettazione di beni culturali (art. 518-quater c.p.)
- Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.)

- Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.)
- Importazione illecita di beni culturali (art. 518-decies c.p.)
- Uscita o esportazione illecite di beni culturali (art. 518-undecies c.p.)
- Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies c.p.)
- Contraffazione di opere d'arte (art. 518-quaterdecies c.p.)

26. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25-duodevicies, D.Lgs. n. 231/2001) [Articolo aggiunto dalla L. n. 22/2022]

- Riciclaggio di beni culturali (art. 518-sexies c.p.)
- Devastazione e saccheggio di beni culturali e paesaggistici (art. 518-terdecies c.p.)

27. Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013) [Costituiscono presupposto per gli enti che operano nell´ambito della filiera degli oli vergini di oliva]

- Commercio di sostanze alimentari contraffatte o adulterate (art. 442 c.p.)
- Adulterazione e contraffazione di sostanze alimentari (art. 440 c.p.)
- Commercio di sostanze alimentari nocive (art. 444 c.p.)
- Contraffazione, alterazione o uso di segni distintivi di opere dell´ingegno o di prodotti industriali (art. 473 c.p.)
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)
- Frode nell´esercizio del commercio (art. 515 c.p.)
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)
- Contraffazione di indicazioni geografiche denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.)

28. Reati transnazionali (L. n. 146/2006) [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]

- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al D. Lgs. 25 luglio 1998, n. 286)
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309)
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al D.P.R. 23 gennaio 1973, n. 43)
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)
- Favoreggiamento personale (art. 378 c.p.)
- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniere (art. 416-bis c.p.)

L'elenco dei reati sopra indicati è suscettibile di modifiche ed integrazioni da parte del legislatore. Da qui l'esigenza di una costante verifica sull'adeguatezza di quel sistema di regole che costituisce il modello di organizzazione, gestione e controllo, previsto dal Decreto e funzionale alla prevenzione dei reati.

3.5. I soggetti che commettono il reato

Quanto ai soggetti che impegnano la responsabilità amministrativa dell'ente, l'attenzione del legislatore va sia a coloro che rivestono formalmente la funzione di rappresentanza, di amministrazione o di direzione dell'ente, sia a coloro che la esercitano di fatto (rileva la figura dell'amministratore di fatto, così come definito dall'art. 2639 cod. civ.), e ai soggetti che la esercitano nell'ambito di strutture decentrate autonome (i c.d. direttori di stabilimento). Questi soggetti sono definiti soggetti in posizione apicale.

Quanto ai subalterni, di regola assumerà rilievo l'inquadramento in uno stabile rapporto di lavoro subordinato, ma potranno rientrare nella previsione di legge anche situazioni peculiari in cui un determinato incarico sia affidato a soggetti esterni, tenuti ad eseguirlo sotto la direzione e il controllo dei soggetti posti ai vertici dell'ente.

3.6. Interesse e vantaggio dell'ente

Il reato, per configurare una responsabilità amministrativa ai sensi del d.lgs. 231, deve essere commesso nell'interesse o a vantaggio dell'ente.

Il decreto prevede che un interesse esclusivo dell'autore dell'illecito o di terzi esclude la responsabilità. Un interesse anche soltanto minore e secondario dell'ente rileva viceversa esclusivamente ai fini della riduzione della sanzione pecuniaria, non anche dell'esimenza.

Secondo la giurisprudenza, la responsabilità prevista dal decreto sorge non solo quando il comportamento illecito abbia determinato un vantaggio per l'ente stesso, ma anche nell'ipotesi in cui, pur in assenza di tale concreto risultato, il fatto illecito abbia trovato ragione nell'interesse dell'ente. I due vocaboli esprimono infatti concetti giuridicamente diversi e rappresentano presupposti alternativi, ciascuno dotato di una propria autonomia e di un proprio ambito applicativo.

Mentre l'Interesse ha una valenza di tipo soggettivo ed in quanto tale è suscettibile di una valutazione ex ante, il "vantaggio" viceversa ha una connotazione oggettiva riferibile agli esiti effettivi della condotta del soggetto agente che, pur non avendo avuto direttamente di mira un interesse dell'ente, ha realizzato, comunque, con la sua condotta un vantaggio in suo favore. In quanto tale è verificabile ex post.

Nei reati dolosi l'interesse/vantaggio sono riferiti all'evento; viceversa nei reati colposi – in materia di sicurezza nei luoghi di lavoro o ambientale – devono essere riferiti alla condotta, ossia all'omissione di regole cautelari cogenti.

Poiché il reato di natura colposa mal si concilia comunque con il concetto di interesse, la giurisprudenza ha ritenuto che in tali casi l'interesse/vantaggio sussista quando l'autore del reato abbia agito spinto dalla necessità di contenimento dei costi aziendali, accelerare i tempi o ritmi di lavoro o aumentarne la produttività, o ancora spinto da una politica aziendale che omette investimenti in tema di sicurezza nell'ambito di uno stabilimento destinato ad essere dismesso e ciò malgrado non rinuncia a farvi lavorare gli operai" (V. Trib. Torino, 15 aprile 2011).

3.7. Tipologie di sanzioni irrogabili

In caso di accertamento della responsabilità amministrativa in capo all'ente, le sanzioni concretamente irrogabili dal giudice sono:

- pecuniarie: esse costituiscono la tipologia di sanzione "generale", poiché applicabili astrattamente a tutti i reati presupposto. Per espresso dettato legislativo, vengono commisurate alla gravità del reato commesso, al grado di corresponsabilità dell'ente, all'attività da esso svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. Vengono, infine, fissate sulla base delle condizioni economiche e patrimoniali dell'ente "allo scopo di assicurare l'efficacia della sanzione";
- interdittive: vengono applicate solo per i reati per i quali sono espressamente previste e sono tassative. Esse sono, in ordine discendente di gravità: l'interdizione dall'esercizio dell'attività; la sospensione o la revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi;
- la confisca del prezzo o del profitto (quando ciò non sia possibile la confisca può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al prodotto del reato);
- la pubblicazione della sentenza di condanna.

4. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Il Decreto prevede la possibilità per l'ente di essere sollevato dalla responsabilità amministrativa qualora provi, unitamente ad altri requisiti, di aver adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi (artt. 6 e 7 d. lgs. 231/2001).

Al fine di predisporre un Modello che possa essere ritenuto idoneo in sede di valutazione da parte del Giudice, è necessario innanzitutto riferimento alle indicazioni contenutistiche presenti nel quadro normativo.

4.1. Gli elementi componenti il Modello

Avuto riguardo al quadro normativo di riferimento – ed in particolare agli artt. 6 e 7 del Decreto Legislativo n. 231/2001 - il Modello risulta composto da:

- Procedure interne e *standards* di controllo con riferimento esclusivamente alle attività giudicate a rischio di reato;
- Codice Etico;
- Sistema disciplinare;
- Organismo di Vigilanza;
- Sistema di *reporting* da e verso l'Organismo di Vigilanza;
- Sistema di segnalazione delle condotte illecite rilevanti ai sensi del Decreto 231 o di violazioni del Modello che garantisca la riservatezza dell'identità del segnalante;
- Comunicazione e formazione.

4.2. La funzione esimente del Modello

Il Modello, se adottato ed efficacemente attuato, rappresenta per la società un efficace scudo protettivo. Esso, infatti, se adottato prima della commissione dell'illecito permette di escludere totalmente la responsabilità dell'ente (secondo il linguaggio penalistico il Modello, in questa circostanza, è una causa di esclusione della colpevolezza dell'organismo collettivo) per il reato commesso dalla persona fisica funzionalmente ad esso legata (in questo caso, perciò, sarà solo il responsabile persona fisica a venire processato ed eventualmente condannato).

Se il Modello viene adottato dopo la commissione dell'illecito, nel caso di irrogazione di sanzioni pecuniarie, determina una notevole riduzione delle medesime. D'altro canto, nell'ipotesi di irrogazione di sanzioni interdittive, le sanzioni in questione non si applicano

qualora vengano adottati comportamenti "virtuosi" quali il risarcimento del danno e/o la messa a disposizione del profitto, l'allontanamento dell'autore dell'illecito.

Infine, nel caso di adozioni di misure cautelari interdittive durante la fase delle indagini preliminari, l'adozione del Modello comporta la sospensione delle medesime (sempre in presenza dei suddetti comportamenti "virtuosi").

4.3. Obiettivi e finalità

BPR Group, adottando un Modello di organizzazione, gestione e controllo adeguato alle prescrizioni del Decreto, evidenzia che opera in condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali.

L'adozione del Modello rappresenta uno strumento di sensibilizzazione nei confronti di tutti i dipendenti e di tutti gli altri soggetti interessati da vicino alla realtà societaria di BPR Group (fornitori, clienti, consulenti ecc.), affinché tengano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire i rischi di reato esistenti.

In particolare la Società attraverso l'adozione del Modello si propone quanto segue:

- rendere consapevoli tutti coloro che lavorano in nome e per conto di BPR Group e soprattutto coloro che operano nelle aree di attività risultate a rischio di reato, di poter incorrere, in caso di violazioni delle disposizioni riportate nel Modello, nella commissione di illeciti passibili di sanzioni penali nei loro stessi confronti, e di sanzioni "amministrative" irrogabili alla Società;
- rendere consapevoli i predetti soggetti che tali comportamenti illeciti sono condannati con forza dalla Società, in quanto gli stessi sono sempre e comunque contrari, oltre che alle disposizioni di legge, anche alla cultura aziendale e ai principi etici assunti come proprie linee guida nell'attività d'impresa;
- tutelare i soggetti che eventualmente segnaleranno condotte illecite o violazioni del Modello, assicurando che a seguito delle segnalazioni non venga posto in essere alcun atto ritorsivo o discriminatorio nei confronti del segnalante;

- consentire alla Società di intervenire tempestivamente per prevenire o contrastare la commissione dei reati (elencati nella parte speciale del decreto), o quanto meno di ridurre sensibilmente il danno da essi prodotto;
- favorire un significativo salto di qualità in termini di trasparenza della *governance* societaria e dell'immagine di BPR Group.

Si evidenzia che, fatti salvi gli obiettivi e le finalità sopra enunciati, la Società ha ben presente che la valutazione del Modello riguarda la sua idoneità a minimizzare e non a escludere *tout court* la realizzazione di uno dei reati elencati nella parte speciale del Decreto da parte dei singoli soggetti.

Ciò è confermato dal fatto che il Decreto Legislativo in parola richiede espressamente che il Modello debba essere idoneo non tanto a prevenire il reato concretamente verificatosi, bensì la tipologia di reato a cui appartiene quello che effettivamente è stato posto in essere.

4.4. Approvazione e recepimento del Modello

Il Modello di organizzazione, gestione e controllo, in conformità al disposto dell'art. 6 comma I, lett. a, del Decreto Legislativo n. 231/2001, è un atto di emanazione dell'Amministratore Unico.

Il Modello integra e non sostituisce gli strumenti organizzativi e di controllo, nonché le procedure comportamentali di futura emanazione o quelli già operanti.

A tal riguardo, infatti, si precisa che il Modello costituisce uno strumento con un ambito di applicazione e finalità specifici, in quanto mira a prevenire esclusivamente la commissione dei reati previsti nel Decreto.

Tuttavia, anche secondo quanto precisato nelle linee guida emanate da Confindustria, i principi di comportamento contenuti nel presente Modello possono essere considerati come un ampliamento o un'estensione dei codici comportamentali già presenti o di futura emanazione.

4.5. Modifiche ed integrazioni del Modello

L'Amministratore Unico di BPR Group srl, su impulso dell'Organismo di Vigilanza, provvede ad effettuare le eventuali e successive modifiche ed integrazioni del Modello, del Codice Etico e del sistema disciplinare.

Ciò, allo scopo di consentire la continua rispondenza del Modello di organizzazione, gestione e controllo alle prescrizioni del Decreto n. 231/2001 e agli eventuali mutamenti intervenuti che possano incidere sulla responsabilità amministrativa dell'ente.

Le attività di modifica ed integrazione del Modello devono essere compiute nel più ampio rispetto delle singole funzioni aziendali, alle quali, pertanto, resta l'ultima parola sulla gestione delle specifiche procedure operative e degli *standards* di comportamento.

4.6. Attuazione del Modello

L'Amministratore Unico della Società prende decisioni relativamente all'attuazione del Modello mediante valutazione ed approvazione delle azioni necessarie per l'implementazione degli elementi costitutivi dello stesso.

L'attività di controllo sull'adeguatezza ed attuazione del Modello è di competenza dell'Organismo di Vigilanza (per i necessari approfondimenti su tale figura, si rinvia alla parte del Modello dedicata a tale organismo).

4.7. I principi generali di controllo

Ogni operazione, transazione, azione deve essere tracciabile, verificabile, documentata, coerente e congrua.

La salvaguardia di dati e procedure in ambito informatico deve essere compiuta nel rispetto delle misure di sicurezza enunciate nel D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) e del Regolamento Europeo 2016/679 (GDPR).

Nessuno può gestire in autonomia un intero processo.

I poteri e le responsabilità devono essere chiaramente definiti e conosciuti all'interno dell'organizzazione.

I poteri autorizzativi e di firma devono risultare coerenti con le responsabilità organizzative assegnate.

I controlli effettuati devono essere documentati.

5. L'ORGANISMO DI VIGILANZA

5.1. Caratteristiche e funzioni

Ai sensi dell'art. 6 comma I, lett. b) del Decreto deve essere costituito l'Organismo di Vigilanza. Tale organo è dotato di autonomi poteri di iniziativa e di controllo, oltre che di spesa.

Deve vigilare sul funzionamento, l'efficacia, e l'osservanza del Modello, nonché curarne il costante e tempestivo aggiornamento.

Il legislatore non fornisce indicazioni esaurienti in merito alla struttura e alla composizione di tale organismo.

Le decisioni su questi profili, quindi, secondo un'opinione condivisa, sono rimesse al libero e responsabile apprezzamento dell'ente.

La vigilanza sul Modello di Organizzazione di BPR Group srl sarà affidata ad un Organismo di Vigilanza monocratico, ritenendo tale scelta la più adeguata.

La funzione di OdV sarà ricoperata da figura con comprovata competenza ed esperienza in materia di responsabilità amministrativa negli ambiti di maggiore rilevanza aziendale.

All'Organismo di Vigilanza è attribuita dall'organo amministrativo, sin dall'atto di nomina, autonomia finanziaria mediante assegnazione di un budget di spesa che verrà, se e quando necessario, integrato e/o rifinanziato.

L'OdV dura in carica tre anni.

La retribuzione dell'OdV viene determinata dall' Amministratore unico all'atto della nomina per l'intero periodo di durata dell'ufficio.

Alla prescritta scadenza o in caso di recesso, l'OdV decade pur continuando a svolgere pro tempore le proprie funzioni, fino a nuova nomina dell'OdV stesso che dovrà avvenire entro e non oltre il termine essenziale ed inderogabile di 3 (tre) mesi.

Per l'OdV valgono le medesime cause di ineleggibilità e di decadenza che sussistono, ai sensi dell'art. 2399 c.c., per i componenti del Collegio Sindacale.

L'OdV può essere revocato dall' Amministratore unico solo per giusta causa. La revoca deve essere deliberata, previa audizione dell'interessato.

In caso di cessazione, di revoca, di morte, di rinunzia o di decadenza dell'OdV, l'Amministratore unico è obbligato a provvedere tempestivamente (e comunque entro 3 mesi) alla nomina del nuovo Organismo.

La figura ricoperta a svolgere il ruolo di OdV non deve essere stata sottoposta a procedimento penale né condannati con sentenza (anche non passata in giudicato) per uno dei reati di cui al Decreto Legislativo n. 231/2001.

L'Organismo di Vigilanza svolgerà le seguenti attività di:

- vigilanza sull'effettività del Modello, verificando in particolare la coerenza tra il Modello medesimo e le concrete procedure adottate nelle aree a rischio;
- verifica periodica che il Modello venga rispettato da parte di tutte le singole unità/aree aziendali a rischio, al fine di accertare che le procedure definite ed i presidi approntati siano seguiti nel modo più fedele possibile e risultino in concreto idonei a prevenire i rischi della commissione dei reati evidenziati;
- vigilanza affinché il Codice Etico e tutte le disposizioni in esso contenute siano rispettate da tutti i soggetti a qualsiasi titolo operanti nella Società;
- formulazione di proposte di aggiornamento e modifica del Modello agli organi competenti, in collaborazione con le funzioni aziendali coinvolte, nel caso in cui mutate condizioni aziendali e/o normative ne comportino, a suo giudizio, necessità di aggiornamento e/o implementazione.

In particolare, l'OdV, come sopra individuato:

- cura l'aggiornamento del Modello, ad opera del A.U., in conformità alle evoluzioni della legge e della giurisprudenza, oltre che in conseguenza di modifiche intervenute all'organizzazione aziendale;

- collabora con le varie funzioni aziendali interessate alla predisposizione ed integrazione della normativa interna (regole di comportamento, istruzioni operative, eventuali manuali di controllo) volta alla prevenzione dei rischi di reato mappati;
- vigila sul corretto funzionamento delle attività di controllo per ciascuna area a rischio, segnalando tempestivamente anomalie e disfunzioni del Modello, previo confronto con le aree/funzioni interessate;
- provvede a diffondere, con le modalità che ritiene più opportune, la conoscenza e la comprensione del Modello all'interno dell'azienda, prestando maggiore attenzione alle aree ritenute più esposte ai rischi di reato mappati (essenzialmente le aree/funzioni che si occupano della gestione delle risorse economiche, della contabilità, quelle che intrattengono rapporti con le pubbliche amministrazioni, la gestione della sicurezza e della salute sul lavoro);
- compie periodicamente verifiche mirate su determinate operazioni o specifici atti posti in essere nell'ambito dei processi monitorati perché sensibili;
- dispone verifiche straordinarie laddove si evidenzino disfunzioni del Modello o si sia verificata, o si abbia soltanto il sospetto che si sia verificata, la commissione di atti illeciti oggetto delle attività di prevenzione;
- effettua il monitoraggio dell'andamento delle attività a rischio, coordinandosi con le funzioni aziendali, anche tramite apposite riunioni;
- raccoglie, elabora e conserva le informazioni rilevanti in ordine al rispetto del Modello;
- redige periodicamente relazioni sull'adeguatezza e sull'efficacia del Modello, anche sulla base di quanto è emerso dalle attività di verifica e controllo, trasmettendole all'Amministratore unico e, se ritenuto opportuno, all'assemblea dei soci;
- verifica periodicamente la praticabilità e l'attuazione delle eventuali soluzioni correttive alle procedure specifiche contenute nel Modello;
- valuta e propone l'irrogazione di eventuali sanzioni disciplinari, previo il necessario coordinamento con i responsabili delle competenti funzioni/aree aziendali.

L'Organismo di Vigilanza svolge la sua attività, salvo il caso di segnalazioni e situazioni urgenti/particolari, con periodicità almeno semestrale.

L'OdV, laddove lo ritenga necessario per lo svolgimento dei suoi compiti, deve poter interloquire con gli organi direttivi e di controllo/amministrazione della Società.

Il rapporto tra la Società e il professionista componente l'OdV sarà regolato da apposito contratto redatto per iscritto.

5.2. Reporting verso l'Organismo di Vigilanza

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

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

All'OdV debbono essere obbligatoriamente trasmessi:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti per le fattispecie di reato previste dal Decreto, riguardanti la Società;
- richieste di assistenza legale avanzate dai soggetti interni alla società, in caso di avvio di un procedimento giudiziario per uno dei reati previsti dal Decreto;
- rapporti predisposti dalle strutture aziendali nell'ambito della loro attività di controllo, dai quali emergano elementi di criticità rispetto alle norme del Decreto;
- le segnalazioni (anonime e non) riguardanti condotte illecite o violazioni del Modello 231;
- in via periodica, notizie relative all'effettiva attuazione del Modello in tutte le aree/funzioni aziendali a rischio come da parte speciale e protocolli di prevenzione;
- in via periodica, notizie relative all'effettivo rispetto del Codice Etico a tutti i livelli aziendali;
- informazioni sull'evoluzione delle attività attinenti le aree a rischio. In caso di informazioni e/o notizie, anche ufficiose, relative alla commissione dei reati previsti dal Decreto o comunque riguardanti possibili violazioni del Modello (comprensivo naturalmente delle

disposizioni del codice etico) ciascuno deve rivolgersi al proprio superiore/responsabile il quale riferisce immediatamente all'OdV.

Qualora la notizia di possibile commissione di reati o violazioni del Modello coinvolga l'Amministratore unico della Società il Responsabile amministrativo informa direttamente e solamente l'OdV.

All'OdV di BPR Group srl, infine, deve essere comunicato, a cura dell'ufficio amministrativo, il sistema delle deleghe e delle procure adottato dalla Società.

I flussi informativi debbono pervenire all'OdV mediante le modalità da esso concretamente definite.

Le segnalazioni, eventualmente anche in forma anonima, aventi ad oggetto l'evidenza o il sospetto di violazione/i del Modello devono essere il più possibile circostanziate. Possono essere inviate per iscritto o attraverso l'utilizzo di una casella di posta elettronica appositamente dedicata: odv@bprgroup.it.

L'OdV agisce in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, garantendo altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente o in malafede.

L'OdV valuta le segnalazioni ricevute e decide le azioni da intraprendere, ascoltando, se necessario, l'autore della segnalazione e/o il responsabile della presunta violazione.

Ogni anno, inoltre, l'OdV trasmette all'Amministratore Unico un *report* scritto sul grado di attuazione del Modello.

L'OdV predispone un apposito data base, informatico o cartaceo, in cui viene custodito ogni report, informazione, segnalazione ai sensi del presente documento, per un periodo di 10 anni. É fatta salva l'osservanza delle disposizioni in materia di riservatezza dei dati personali e dei diritti da essa garantiti in favore degli interessati.

L'accesso al data base è consentito esclusivamente all'OdV.

5.3. Responsabilità dell'Organismo di Vigilanza

Sono opportune alcune brevi annotazioni in ordine alla responsabilità dell'Organismo di Vigilanza in caso di commissione di reato all'interno della Società.

La giurisprudenza tende ad escludere una responsabilità omissiva dell'Organismo di Vigilanza ai sensi dell'art. 40 cpv c.p., che prevede che *"il non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo"*.

Ciò perché non sussistono veri e propri poteri "impeditivi" in capo all'Organismo di Vigilanza che consentano a quest'ultimo di intervenire concretamente nel caso in cui abbia conoscenza della commissione di un illecito o di attività eventualmente prodromiche ad esso.

L'Organismo, conformemente al proprio ruolo, può limitarsi, infatti, semplicemente a segnalare le problematiche agli organi gestionali, i quali sono gli effettivi titolari dei poteri di impedimento: ciò in virtù di un principio di non ingerenza dell'Organismo di Vigilanza nella gestione della Società.

D'altro canto, l'autonomia e l'indipendenza dell'Organismo si basano su questa estraneità al potere gestionale che lo rende un mero "controllore" e non un "garante" in senso penalistico.

6. LA DIFFUSIONE DEL MODELLO

6.1. Formazione del personale interno

La Società intende garantire una corretta e completa conoscenza del Modello e del contenuto del Decreto Legislativo n. 231/2001 e degli obblighi derivanti dal medesimo.

La formazione e l'informativa è gestita dal Responsabile del personale coadiuvato dall'OdV, in stretto coordinamento con i responsabili delle aree/funzioni coinvolte nell'applicazione del Modello.

Tale sforzo formativo ed informativo è esteso anche a tutti quei soggetti che, pur non appartenendo alla compagine aziendale, potrebbero astrattamente operare nell'interesse e/o a vantaggio della Società.

Tuttavia, ai soggetti terzi è rivolta solamente l'attività di comunicazione e di formazione avente ad oggetto il Codice Etico.

L'adozione del presente documento è comunicata a tutti i soggetti che lavorano per ed in nome di BPR Group srl al momento dell'adozione dello stesso.

Tutti i dipendenti e gli apicali devono sottoscrivere un apposito modulo tramite cui attestano l'avvenuta conoscenza ed accettazione del Modello, di cui hanno a disposizione una copia cartacea o su supporto informatico.

Ai nuovi assunti viene consegnato un'informativa riguardante il Modello, comprensivo del Codice Etico, con il quale vengono assicurati agli stessi le conoscenze considerate di primaria rilevanza.

Nei contratti stipulati con i terzi vengono inserite clausole contrattuali standard, che impegnano gli stessi a non adottare comportamenti non in linea con i principi di condotta ed i valori etici cui si ispira la Società.

L'attività di formazione continuativa e di aggiornamento è organizzata dalle competenti funzioni aziendali con la supervisione dell'Organismo di Vigilanza, facendo ricorso ad incontri periodici obbligatori, modulati nei contenuti e nella frequenza, in funzione della qualifica dei destinatari e della funzione dagli stessi ricoperta.

Se ritenuto necessario dall'OdV, interverranno agli incontri professionisti esterni aventi specifiche competenze sul tema dei reati ascrivibili alla Società, dell'analisi delle procedure e dei processi organizzativi, nonché dei principi generali sulla legislazione in materia di *compliance* e dei controlli ad essi correlati.

6.2. Selezione di collaboratori esterni e partner nelle aree esposte a rischio

Su proposta dell'OdV, con decisione dell'Amministratore Unico, potranno essere istituiti nell'ambito della Società appositi sistemi di valutazione per la selezione di rappresentanti, consulenti e simili nonché di *partners* con cui la Società intenda addivenire a una qualunque forma di partnership (ad esempio una *joint venture* anche in forma di ATI) e destinati a cooperare con l'azienda nell'espletamento delle attività più esposte al rischio di reato.

7. SISTEMA DISCIPLINARE

7.1. Finalità

Il presente sistema disciplinare e sanzionatorio, parte integrante del Modello organizzativo di BPR Group srl, è adottato dall'Amministratore Unico ai sensi dell'art. 6, comma 2, lett. e) e dell'art. 7, comma 4, lett. h) del D. Lgs. 231/2001.

Esso è diretto a definire le sanzioni per il mancato rispetto dei principi contenuti nel presente Modello organizzativo, nonché nel Codice Etico.

L'applicazione delle misure disciplinari e sanzionatorie prescinde dall'avvio e dall'esito di un eventuale procedimento penale, in quanto le regole di condotta tutelate sono assunte dalla Società in piena autonomia e indipendentemente dal tipo di illecito che le violazioni del Sistema preventivo stesso possano determinare. Chi di competenza, infatti, possiede la facoltà di applicare, all'esito delle opportune valutazioni, le sanzioni che ritiene più adeguate al caso concreto, non dovendo le stesse, in virtù della loro autonomia, coincidere con le valutazioni e i convincimenti del giudice penale.

7.2. Misure sanzionatorie in caso di violazioni da parte del personale dipendente non dirigente

Le sanzioni disciplinari applicabili al personale dipendente non dirigente di cui è stata accertata la violazione delle regole e dei principi contenuti nel Modello, rientrano tra quelle previste dal C.C.N.L. applicato da BPR Group, nel rispetto delle procedure previste dall'art. 7 della Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori) ed eventuali norme speciali applicabili.

In particolare:

- incorre nei provvedimenti di rimprovero verbale o scritto il lavoratore che violi le procedure interne previste dal presente Modello (ad esempio, non osservi le procedure prescritte, ometta di fornire all'OdV le informazioni necessarie, ecc.), o adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento non conforme alle previsioni del Modello stesso e del Codice Etico.
- Incorre nel provvedimento della multa non superiore a quattro ore di retribuzione, il lavoratore che violi più volte le procedure interne del Modello o adotti,

nell'espletamento di attività nelle aree a rischio, un comportamento più volte non conforme alle prescrizioni del Modello stesso e a quelle del Codice Etico, prima ancora che dette mancanze siano state singolarmente accertate e contestate.

- Incorre nel provvedimento della sospensione dal servizio e dalla retribuzione, per un periodo da 1 a 10 giorni, il lavoratore che - nel violare le procedure interne previste dal presente Modello o adottando, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Modello stesso e a quelle del Codice Etico, nonché compiendo atti contrari all'interesse della Società - arrechi danno a BPR Group srl o la esponga ad una situazione oggettiva di pericolo alla integrità dei beni della azienda.

  Inoltre, incorre nella medesima sanzione il lavoratore che violi le misure previste a tutela dei soggetti che segnalano illeciti, nonché chi effettui la segnalazione di illeciti che poi si rivelino infondati.

- Incorre nel provvedimento del licenziamento con preavviso il lavoratore che adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento non conforme alle previsioni del Modello e del Codice Etico, diretto alla commissione di un reato tra quelli direttamente ascrivibili alla Società ai sensi del Decreto n. 213/2001.

- Incorre nel provvedimento del licenziamento senza preavviso il lavoratore che adotti, nell'espletamento delle attività nelle aree a rischio, un comportamento palesemente in violazione delle prescrizioni del presente Modello e/o del Codice Etico, tale da determinare la concreta applicazione a carico della Società di misure sanzionatorie previste dal Decreto 231/2001.

Non può essere adottato alcun provvedimento nei confronti del lavoratore senza avergli preventivamente e per iscritto contestato l'addebito e senza averlo sentito a sua difesa. La contestazione dovrà essere notificata al lavoratore entro 15 giorni dalla data in cui l'impresa è venuta a conoscenza del fatto contestato.

Il lavoratore entro il termine di 5 giorni dalla data di ricevimento della contestazione potrà richiedere di essere sentito a sua difesa con la facoltà di farsi assistere da un rappresentante dell'associazione sindacale cui aderisce o conferisce mandato.

La sanzione disciplinare dovrà essere comunicata dall'impresa al lavoratore entro e non oltre 15 giorni dal ricevimento della giustificazione scritta o dalla data in cui il lavoratore è stato sentito a sua difesa.

Il tipo e il *quantum* delle sanzioni disciplinari sopra menzionate sono stabiliti, sulla base:

- dell'intenzionalità del comportamento o del grado di negligenza, imprudenza o imperizia con riguardo alla prevedibilità dell'evento;
- del comportamento complessivo del lavoratore, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- delle mansioni svolte dal lavoratore;
- della posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- delle altre particolari circostanze che accompagnano la violazione disciplinare.

L'accertamento delle suddette infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni rientrano nella competenza della Direzione Aziendale.

Il sistema disciplinare viene costantemente monitorato dall'OdV.

7.3. Misure sanzionatorie in caso di violazioni da parte del personale dirigente

La violazione delle prescrizioni e delle procedure previste o richiamate nel Modello di organizzazione e nel Codice etico che espongano gravemente la società al rischio di commissione di uno dei reati di cui al d.lgs. n. 231 del 2001 e all'applicazione delle sanzioni ivi previste, qualora siano imputabili a personale con qualifica dirigenziale sono punite - ad integrazione delle disposizioni di cui al CCNL dirigenti applicato - con le seguenti sanzioni:

a) licenziamento con preavviso

b) licenziamento senza preavviso

In particolare:

1) incorre nel LICENZIAMENTO CON PREAVVISO il dirigente che adotti, nell'espletamento delle attività nelle aree sensibili, una condotta gravemente non conforme a prescrizioni, protocolli e procedure di cui al Modello di organizzazione o al Codice etico e sia diretta in modo inequivocabile al compimento di un reato presupposto ex d.lgs. n. 231 del 2001;

2) incorre nel LICENZIAMENTO PER GIUSTA CAUSA il dirigente che adotti, nell'espletamento delle attività nelle aree a rischio una condotta che violi gravemente e

palesemente le prescrizioni, i protocolli e le procedure di cui al Modello di organizzazione o al Codice etico e tale da determinare il rischio di concreta applicazione a carico della Società di misure sanzionatorie previste dal d.lgs. n. 231 del 2001, nonché da far venire meno il vincolo fiduciario dell'ente nei suoi confronti e da imporre, per la loro gravità, la risoluzione immediata del rapporto di lavoro senza preavviso.

Ove il dirigente sia munito di procura con potere di rappresentare all'esterno BPR Group Srl, l'irrogazione della sanzione disciplinare comporta anche la revoca automatica della procura stessa.

Nei confronti del dirigente sottoposto ad indagini preliminari ovvero sottoposto ad azione penale per uno dei reati previsti dal d.lgs. n. 231 del 2001, la Società può disporre, in ogni fase del procedimento penale in atto e nel rispetto di quanto stabilito dal CCNL, la sospensione dal servizio in via cautelare.

7.4 . Misure sanzionatorie nei confronti degli Amministratori

Nel caso in cui l'Amministratore Unico violi le procedure previste dal Sistema preventivo o adotti, nell'espletamento di attività nelle aree a rischio, un comportamento non conforme alle prescrizioni del Sistema stesso, l'OdV informa l'Assemblea dei soci che, in caso di lievi irregolarità procederà al richiamo scritto; nei casi più gravi, potrà revocarne il mandato per giusta causa.

7.5. Collaboratori, consulenti, fornitori e altri soggetti terzi aventi rapporti contrattuali con BPR Group srl

Qualsiasi inosservanza delle regole comportamentali indicate nel Modello, nonché qualsiasi violazione delle disposizioni e dei principi stabiliti nel Codice Etico da parte di collaboratori, consulenti, fornitori e altri soggetti terzi, può determinare, in conformità a quanto previsto in specifiche clausole contrattuali inserite nelle lettere di incarico o convenzioni, le seguenti sanzioni:

a) DIFFIDA al puntuale rispetto delle prescrizioni e delle procedure definite nel Modello e nel Codice etico qualora la violazione delle medesime configuri irregolarità di lieve rilevanza;

b) RISOLUZIONE ANTICIPATA del contratto in caso di gravi e palesi comportamenti posti in essere in violazione delle previsioni e procedure di cui al Modello di organizzazione e al Codice etico, salvo, in ogni caso, il risarcimento dei danni derivanti da dette condotte, ivi compresi i danni determinati dall'applicazione da parte del giudice delle misure sanzionatorie previste dal d.lgs. n. 231 del 2001.

I provvedimenti sono disposti dall'Amministratore unico in collaborazione con il Responsabile amministrativo.

7.6. Misure nei confronti dell'Organismo di vigilanza

In caso di violazione del Modello di organizzazione e del Codice etico di BPR Group da parte del componente dell'Organismo di vigilanza, in relazione alla gravità dell'infrazione, è prevista l'adozione dei seguenti provvedimenti:

a) Diffida al puntuale rispetto della disciplina di cui al d. lgs. n. 231/2001, del Modello di organizzazione e gestione, del Codice etico e del regolamento dell'Organismo di vigilanza;

b) Revoca dell'incarico da parte dell'Amministratore unico.

In particolare, il componente dell'Organismo di vigilanza, incorre:

a) nel provvedimento di DIFFIDA: qualora, nel violare le disposizioni del Modello di organizzazione, del Codice etico e del proprio regolamento, ponga in essere atti che arrechino o possano arrecare danno all'azienda, esponendola ad una situazione oggettiva di pericolo riguardante l'integrità del patrimonio;

b) nel PROVVEDIMENTO DI REVOCA qualora, nel violare le disposizioni del Modello di organizzazione, del Codice etico e del proprio regolamento, ponga in essere atti che risultino che risultino diretti in modo univoco al compimento di un reato sanzionato ai sensi del d.lgs. n. 231 del 2001 e tali da determinare il rischio di concreta applicazione a carico della Società delle misure sanzionatorie previste dal decreto.

I provvedimenti sono disposti dall'Amministratore unico, previa audizione dell'interessato, anche su segnalazione dei singoli responsabili di funzione.

8. ADOZIONE, AUDIT PERIODICO E RIESAME DEL MODELLO

8.1. Adozione e aggiornamento del Modello di organizzazione e gestione

L'Amministratore Unico di BPR Group adotta il presente Modello ed informa di tale adozione con specifica comunicazione affissa in bacheca.

Le stesse modalità informative sono adottate in caso di aggiornamento del Modello.

Gli aggiornamenti del Modello si rendono necessari ogniqualvolta avvengano modificazioni esogene (esempio: sistema normativo) o endogene (esempio: organigramma/integrazione attività aziendale) che richiedano di variarne le previsioni allo scopo di mantenerne l'efficienza.

La gestione degli aggiornamenti si esplica anche nella corretta gestione dei flussi informativi:

- Segnalazione criticità: i soggetti preposti devono dare immediata informazione all'Amministratore unico e all'Organismo di vigilanza delle criticità di qualsiasi natura emerse nel corso della gestione delle attività;
- Tracciabilità: i soggetti designati alla gestione dei rapporti con la P.A. devono documentare l'attività svolta, mantenendo traccia delle informazioni o dei documenti forniti anche da altre funzioni interne ed indicando i soggetti che hanno eventualmente intrattenuto con l'ente pubblico coinvolto;
- Reportistica: il Responsabile, ovvero persona da questi designata, deve compilare apposito report, da inviare all'Organismo di vigilanza nelle periodicità dallo stesso indicate. Il flusso informativo ha come scopo quello di permettere all'Organismo di vigilanza di essere informato su potenziali situazioni a rischio reato e di vigilare sull'applicazione del Modello Organizzativo e del Codice etico. Tuttavia, laddove nello svolgimento delle attività dovessero emergere criticità di qualsiasi natura, l'Organismo di vigilanza dovrà essere tempestivamente informato;
- Conservazione della documentazione: tutta la documentazione deve essere archiviata a cura del Responsabile delegato e conservata presso la sede della società.

8.2. Verifiche ispettive interne

Il Responsabile audit interno predispone, entro il mese di gennaio di ogni anno, un piano annuale di verifiche interne e lo sottopone all'approvazione dell'Amministratore unico. Il piano viene trasmesso ai responsabili di funzione interessati.

Possono essere effettuati anche audit straordinari, ad esempio in caso di infortuni, incidenti o quasi incidenti, ovvero per aree specifiche che presentano maggiori criticità e richiedono audit più frequenti.

L'audit deve interessare tutti gli ambiti del Modello e i risultati sono valutati in fase di riesame.

L'audit è finalizzato a valutare determinati aspetti:

- modifiche significative nella struttura produttiva o nelle politiche aziendali;
- risultati di precedenti audit;
- segnalazioni;
- rapporti di non conformità dei sistemi di gestione;
- incidenti e infortuni (in particolare quelli gravi);
- presenza di processi lavorativi di particolare complessità e/o rischiosità;
- contesti produttivi molto differenziati.

Il Responsabile, sulla scorta del piano annuale delle verifiche approvato dall'Amministratore unico, predispone il programma di verifica interna e lo comunica al responsabile di funzione da ispezionare con almeno 7 giorni di anticipo. Predispone inoltre eventuali liste di controllo/di riscontro che fanno riferimento alle sezioni del Manuale e ai protocolli di prevenzione di cui deve essere verificata la corretta applicazione.

Il Responsabile audit conduce quindi le verifiche in collaborazione con l'Organismo di vigilanza.

Durante la verifica le informazioni possono essere raccolte mediante interviste, esame dei documenti ed osservazioni dirette sulle attività svolte. Deve essere dato particolare rilievo all'individuazione delle non conformità e/o anomalie.

Ogni verifica interna comprende:

- la verifica della conoscenza delle procedure e dell'applicazione conforme dei protocolli del Modello di organizzazione e gestione;

- il controllo dell'attuazione ed efficacia di azioni correttive richieste a seguito di precedenti visite ispettive;
- la verifica della disponibilità e dello stato di aggiornamento della documentazione delle attività richiesta dal Modello;

Al termine della verifica ispettiva, il Responsabile audit interno, assieme al responsabile di funzione, redige il rapporto di verifica interna.

Nel rapporto vengono riportati:

- attività ispezionata;
- argomenti trattati;
- eventuali liste di controllo utilizzate;
- nomi delle persone contattate
- descrizione delle non conformità rilevate
- valutazione dei risultati della verifica
- firma del verificatore e del responsabile di funzione.

Il Responsabile, in collaborazione con l'Organismo di vigilanza, richiederà al responsabile dell'attività verificata di definire, entro un tempo determinato, le azioni correttive necessari per la rimozione delle cause delle eventuali non conformità rilevate e di definire altresì responsabilità e tempi per l'attuazione.

Il rapporto di verifica è trasmesso all'Amministratore unico e all'Organismo di vigilanza ai fini dell'attività di riesame e dell'attivazione di eventuali procedimenti sanzionatori.

8.3. Il riesame della Direzione

L'Amministratore unico, in collaborazione con l'Organismo di vigilanza, deve provvedere con cadenza annuale al riesame del Modello Organizzativo per verificare che:

- sia attuato con efficacia;
- sia idoneo per il mantenimento ed il miglioramento nel tempo delle misure adottate;
- garantisca il raggiungimento degli obiettivi di sicurezza e salute sul lavoro;
- permetta di esprimere una valutazione sulle prestazioni complessive;
- consenta di programmare le attività per il miglioramento continuo.

I risultati che scaturiscono da questo processo, in relazione al periodo indagato possono portare, se necessario, a modificare il Modello, la sua articolazione di funzioni, i suoi obiettivi o a programmare interventi di miglioramento.

L'incontro di riesame è convocato dall'Amministratore unico con apposito ordine del giorno recante "Riesame della Direzione del Modello di organizzazione, gestione e controllo". E' presieduto dal medesimo e coinvolge normalmente tutti i responsabili di funzione. Viene nominato un segretario per registrare l'attività svolta e redigere successivamente il Rapporto del Riesame.

Oggetto del riesame sono:

- risultati dei precedenti riesami con riferimento ai protocolli di prevenzione e alla loro attuazione;
- esiti delle azioni intraprese nel precedente riesame e la loro efficacia;
- risultati delle verifiche interne eseguite e azioni correttive eventualmente intraprese;
- risultati di eventuali audit dei sistemi di gestione certificati e azioni correttive intraprese;
- dati sugli infortuni e malattie professionali, incidenti e situazioni di emergenza e l'analisi delle relative cause;
- cambiamenti, interni ed esterni, rilevanti per l'ente e l'emergere di eventuali nuovi rischi di commissione di reati;
- programma formativo: svolgimento ed esiti;
- report o segnalazioni ricevute/pervenute dall' Organismo di vigilanza;
- eventuali sanzioni applicate.

L'esito del riesame deve essere verbalizzato annotando gli elementi trattati e le azioni che si è deciso di attuare e/o le soluzioni ad eventuali problemi riscontrati. Limitatamente alla materia della salute e sicurezza sul lavoro, qualora il datore di lavoro lo ritenga opportuno, può far coincidere il riesame con la riunione periodica, di cui all'art. 35 del d. lgs n. 81/08 e s.m.i. Diversamente, è opportuno che questo processo sia attuato almeno una volta all'anno.

I verbali di riesame sono trasmessi per conoscenza all'Organismo di vigilanza e sono archiviati presso la Direzione.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. N. 231/2001

PARTE SPECIALE

SEZIONI

1. FINALITA' DELLA PARTE SPECIALE

2. REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

3. REATI SOCIETARI

4. CORRUZIONE TRA PRIVATI

5. REATI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI

6. REATI AMBIENTALI

7. REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E SICUREZZA SUL LAVORO

8. REATI IN MATERIA DI DIRITTO D'AUTORE

9. REATI TRIBUTARI

10. RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA, AUTORICICLAGGIO E DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

SEZIONE 1 - FINALITA' DELLA PARTE SPECIALE

1. Finalità della parte speciale 2

1.1. Struttura della parte speciale 3

1.2. Specifiche circa i delitti tentati 4

1. Finalità della Parte speciale

La Parte Speciale ha la finalità di definire linee, regole e principi di comportamento che tutti i destinatari del Modello di organizzazione, gestione e controllo 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 ha lo scopo di:

- indicare le modalità che gli esponenti aziendali sono chiamati ad osservare ai fini della corretta applicazione del Modello
- fornire all'Organismo di Vigilanza 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 ai contenuti dei seguenti documenti:

- Modello 231
- Codice Etico
- Procedure e disposizioni
- Procure e deleghe
- Regolamenti Operativi
- Comunicazioni organizzative
- Sistemi di gestione delle problematiche di sicurezza e ambientali
- Regolamento e Modulistica in linea con le indicazioni del Reg U.E. 679/16

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

1.1. Struttura della Parte speciale

La presente Parte Speciale è composta da più sezioni, definite sulla base dell'attività di analisi svolta, con cui sono state preliminarmente individuate, nell'ambito dell'elenco dei reati presupposto della responsabilità amministrativa degli enti, le fattispecie di reato rilevanti e con teorica probabilità di verificazione in considerazione della governance di BPR Group, della tipologia di attività svolta, delle dimensioni aziendali, dell'ambito territoriale di riferimento, delle politiche aziendali e dei sistemi interni di gestione e controllo già esistenti.

Le sezioni della Parte Speciale, corrispondenti ai reati che, seppure in astratto, considerati il sistema organizzativo e i sistemi di controllo interni in essere, possono avere probabilità di verificazione sono le seguenti:

SEZIONE 02	Reati contro la Pubblica Amministrazione
SEZIONE 03	Reati societari
SEZIONE 04	Reati Corruzione tra privati
SEZIONE 05	Delitti informatici e trattamento illecito di dati
SEZIONE 06	Reati ambientali
SEZIONE 07	Reati di omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro
SEZIONE 08	Delitti in materia di violazione del diritto d'autore
SEZIONE 09	Reati tributari
SEZIONE 10	Ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio e delitti in materia di strumenti di pagamento diversi dai contanti.

In ogni sezione sono descritte le singole fattispecie di reato, le specifiche attività "sensibili" in cui ricorre un astratta probabilità di consumazione dei reati esaminati, i soggetti destinatari, ossia le figure aziendali coinvolte in dette attività sensibili, i protocolli generali di prevenzione e specifici con individuazione dei flussi informativi nei confronti dell'Organismo di vigilanza.

Nella definizione del sistema di prevenzione sono assicurati:

- una chiara articolazione delle funzioni e segregazione delle medesime;
- che ogni operazione, transazione, azione rilevante risulti verificabile, documentata, coerente e congrua;
- idonei meccanismi di controllo;
- flussi informativi nei confronti dell'Organismo di vigilanza.

Il Modello di organizzazione e gestione e i relativi protocolli assumono le procedure ed i sistemi di gestione già in essere in BPR Group e li integrano e rafforzano per assicurare un efficace sistema preventivo con riferimento specifico alla responsabilità amministrativa degli enti e ai principi che la governano.

1.2. Specifiche circa i delitti tentati

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti rilevanti ai fini della responsabilità amministrativa degli enti, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 del d.lgs. 231/2001). L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e per suo conto.

PARTE SPECIALE

SEZIONE 2 - REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

INDICE

2.1 Introduzione e funzione della parte speciale dedicata ai reati contro la P.A. 3
2.2 Criteri per la definizione di pubblica amministrazione e di soggetti incaricati di un pubblico servizio 4
2.3 Le fattispecie di reato richiamate dal D.Lgs 231/01 8
2.3.1 Peculato (art 314 c.p. – art. 316 c.p.) 8
2.3.2 Malversazione di erogazioni pubbliche (Art. 316 bis c.p mod. D.Lgs.. n. 150/2022) 8
2.3.3 Indebita percezione di erogazioni pubbliche (Art. 316 ter c.p. mod.L. 3/2019 e D.Lgs. n. 150/22) 9
2.3.4 Truffa in danno dello Stato o di altro Ente Pubblico o dell'Unione Europea (Art. 640 – Comma 2, n. 1, c.p. mod. Dlgs. n. 75/2020 e dalla Legge n. 90/2024) 10
2.3.5 Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640 bis mod. dalla L.161/2017 e dal D.Lgs. n. 150/2022) 10
2.3.6 Frode informatica in danno dello Stato o di altro Ente Pubblico (Art. 640 ter c.p.mod. D.Lgs. n. 150/22...11
2.3.7 Frode nelle pubbliche forniture (art. 356 c.p. introdotto dal D.Lgs. n. 75/2020) 11
2.3.8 Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n.898 - D.Lgs. n. 75/2020) 11
2.3.9 Turbata libertà degli incanti (art. 353 c.p. introdotto dalla L. n. 137/2023) 12
2.3.10 Turbata libertà del procedimento di scelta del contraente (art. 353-bis articolo introdotto dalla L. n. 137/2023) 12
2.3.11 Concussione (Art. 317 c.p. modificato da L.69 del 27 maggio 2015) 13
2.3.12 Corruzione per l'esercizio della funzione – Corruzione per un atto contrario ai doveri d'ufficio – Circostanze aggravanti-Induzione indebita a dare o promettere utilità-Corruzione di persona incaricata di pubblico servizio (Art. 318, 319,319bis,319quater e 320 c.p. modificati da L.69 del 27 maggio 2015) 13
2.3.13 Corruzione in atti giudiziari (Art. 319-ter c.p. modificato da L.69 del 27 maggio 2015) 15
2.3.14 Pene per il corruttore (Art. 321 c.p.) 15
2.3.15 Istigazione alla corruzione (Art. 322 c.p.) 15
2.3.16 Peculato, concussione, corruzione ed istigazione alla corruzione di membri degli organi e di funzioni della comunità europee e di stati esteri (Art. 322 bis c.p. mod. dalla L. n. 190/2012, n. 3/2019 e dal D.L. n. 92/2024) 16
2.3.17 Traffico di influenze illecite (art. 346-bis c.p. modificato dalla L. 3/2019 e dalla L. 112/2024) 16
2.3.18 Indebita destinazione di denaro o cose mobili (art. 314-bis c.p. introdotto dalla L. n. 112/2024) 17
2.4 Le attività sensibili relative ai reati contro la Pubblica Amministrazione 18
2.5 Organi e funzioni aziendali coinvolte 18
2.6 Principi e governance 23
2.7 Norme generali di comportamento 24
2.8 Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili 26
2.9 I controlli dell'Organismo di Vigilanza..... 28
2.10. Flussi informativi all'Organismo di vigilanza 29

2.1. Introduzione e funzione della parte speciale dedicata ai reati contro la Pubblica Amministrazione

Obiettivo della presente Parte Speciale è che tutti i destinatari adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire il verificarsi dei reati in essa considerati.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare le procedure che i Dipendenti, gli Organi Sociali, i Collaboratori esterni e i Partner della Società sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

Provvede a fornire, inoltre, indicazioni riferite a ciascuna delle suddette categorie di reati, al fine di facilitare la comprensione delle attività e delle funzioni nell'ambito delle quali possono essere commessi i reati di cui al Decreto.

L'Amministratore Unico nel definire tale documento, a ulteriore conferma della volontà aziendale di operare secondo principi "etici" così come già contemplati nella propria regolamentazione interna, intende sensibilizzare tutto il personale a mantenere comportamenti corretti e idonei a prevenire la commissioni di reati.

A tale scopo vengono disciplinati nel presente documento i principi e le regole di comportamento da porre alla base dell'operatività aziendale.

Tali principi e regole richiamano, focalizzandoli ai fini della prevenzione dei reati connessi al Decreto ed eventualmente integrandoli, quelli previsti nel Codice Etico/Codice di Comportamento Interno e nelle procedure aziendali interne attualmente in vigore, quali individuati nella Parte Generale del Modello.

In via generale, a tutto il personale dell'azienda:

- È fatto obbligo di rispettare le regole, i principi e le procedure aziendali previste nel Modello e nei documenti interni della Società richiamati nel Modello e nei quali il medesimo si articola;

- È fatto 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 tempo per tempo vigente e, in particolare, i reati di cui al Decreto;

- Violare in tutto o in parte le regole, i principi e le procedure aziendali previste nel Modello e nei documenti interni della società richiamati nel Modello e nei quali il medesimo si articola.

La violazione delle norme aziendali e, in particolare, di quelle richiamate nel presente documento, comporta l'applicazione del sistema disciplinare illustrato nella Parte Generale.

I medesimi obblighi e divieti si applicano, per le attività e i comportamenti loro rispettivamente attribuiti o comunque ai quali sono tenuti nell'esercizio dell'ufficio o dell'incarico, ai componenti degli Organi Sociali della società, ai Collaboratori esterni e ai Partner.

2.2. Criteri per la definizione di pubblica amministrazione e di soggetti incaricati di un pubblico servizio

Obiettivo del presente capitolo è quello di indicare dei criteri generali e fornire un elenco esemplificativo di quei soggetti qualificati come "soggetti attivi" nei reati rilevanti ai fini del Decreto, ovvero di quei soggetti la cui qualifica è necessaria ad integrare fattispecie criminose previste nel Decreto.

In aggiunta sono riportate anche delle indicazioni in merito alle fattispecie di reato che si possono compiere in relazione alle diverse categorie di soggetti coinvolti.

Enti della Pubblica Amministrazione

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

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

Nel tentativo di formulare una preliminare classificazione di soggetti giuridici appartenenti a tale categoria è possibile richiamare, da ultimo, l'art. 1, comma 2, D.Lgs. 165/2001 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, il quale definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato.
A titolo esemplificativo, si possono indicare quali soggetti della pubblica amministrazione, i seguenti enti o categorie di enti:

Istituti e scuole di ogni ordine e grado e le istituzioni educative		=
Enti ed amministrazioni dello Stato ad ordinamento autonomo		Ministeri - Camera e Senato - Dipartimento Politiche Comunitarie -Autorità Garante della Concorrenza e del Mercato - Autorità per l'Energia Elettrica ed il Gas - Autorità per le Garanzie nelle Comunicazioni - Banca d'Italia – Consob - Autorità Garante per la protezione dei dati personali - Agenzia delle Entrate – ISVAP - COVIP
Regioni		Tutte
Province		Tutte
Comuni		Tutte
Comunità montane e loro consorzi ed associazioni		=
Camere di Commercio, Industria, Artigianato e Agricoltura e loro associazioni		Tutte
Tutti gli enti pubblici non economici nazionali, regionali e locali		INPS – CNR – INAIL – INPDAI - ISTAT – ENASARCO – ASL - Enti e Monopoli di Stato - RAI

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose previste dal Decreto.

In particolare le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali¨ e degli "Incaricati di Pubblico Servizio".

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".

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

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

o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

Tale ultima definizione normativa individua, innanzitutto, la delimitazione "esterna" della funzione amministrativa. Tale delimitazione è attuata mediante il ricorso a un criterio formale che fa riferimento 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.

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

Vengono quindi pacificamente definite come "funzioni pubbliche" quelle attività amministrative che rispettivamente ed alternativamente costituiscono esercizio di:

- Poteri deliberativi
- Poteri autoritativi
- Poteri certificativi

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".

Per fornire un contributo pratico alla risoluzione di eventuali "casi dubbi", può essere utile ricordare che 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 formino legittimamente la volontà e/o la portino all'esterno in forza di un potere di rappresentanza.

Esatto sembra infine affermare, in tale contesto, che non assumono la qualifica in esame altri soggetti che, sebbene di grado tutt'altro che modesto, svolgano solo mansioni preparatorie alla formazione della volontà dell'ente (e così, i segretari amministrativi, i geometri, i ragionieri e gli ingegneri, tranne che, in specifici casi e per singole incombenze, non "formino" o manifestino la volontà della pubblica amministrazione).

Incaricati di un pubblico servizio

La definizione della categoria di "soggetti incaricati di un pubblico servizio" si rinviene all'art. 358 c. p. il quale recita che "sono 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 legislatore puntualizza la nozione di "pubblico servizio" attraverso due ordini di criteri, uno positivo ed uno negativo. Il "servizio", affinché possa definirsi pubblico, deve essere disciplinato – del pari alla "pubblica funzione" - 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 accessorietà delle attività rispetto a quella pubblica in senso stretto.

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

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

Sulla base di quanto sopra riportato, si potrebbe ritenere che l'elemento discriminante per indicare se un soggetto rivesta o meno la qualifica di "incaricato di un pubblico servizio" è rappresentato, non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale. È importante dunque tenere a mente che, ad esempio, allorché una banca svolga l'attività di concessionaria per la riscossione delle imposte, in quella veste essa è incaricata di pubblico servizio. Bisogna perciò sempre esaminare con attenzione il tipo di rapporto che si instaura con un ente terzo e nel caso di dubbio sulla natura giuridica, rivolgersi immediatamente alla funzione specifica per approfondimenti e chiarimenti.

2.3. Le fattispecie di reato richiamate dal D.Lgs. 231/01

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d.lgs. n. 231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

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 dagli art. 24 e art.25 del D.Lgs. 231/01.

2.3.1. Peculato (Artt. 314 c.p.-316 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio che avendo per ragioni del suo ufficio o servizio il possesso o comunque la disponibilità di danaro o di altra cosa se ne appropria.

La pena prevista per tale reato dall'art. 1. della legge n.69 del 27 maggio 2015 che ha modificato l'art. 314 c.p., è la reclusione da quattro a dieci anni e sei mesi.
Si applica invece la pena della reclusione da sei mesi a tre anni quando il colpevole ha agito al solo scopo di fare uso momentaneo della cosa e questa viene immediatamente restituita.

Esempio
Un pubblico ufficiale utilizza la carta di credito aziendale per ragioni private.
Il D. lgs. n. 75 /2020 ha inserito nel catalogo dei reati presupposto anche la fattispecie del "Peculato mediante profitto dell'errore altrui" di cui all'art. 316 c.p. che punisce con la reclusione da sei mei a tre anni "il pubblico ufficiale o l'incaricato di un pubblico servizio, il quale, nell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui, riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità". La pena è della reclusione 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.

2.3.2. Malversazione a danno dello Stato o dell'Unione Europea (Art. 316 bis c.p. come modificato dal D.L. n. 13/2022)

Tale ipotesi di reato si configura nel caso in cui, chiunque, estraneo alla pubblica amministrazione, dopo avere ottenuto contributi, sovvenzioni, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo da parte dello Stato italiano o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per le finalità cui erano destinate (la condotta, infatti, consiste nell'avere 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.

Per i dipendenti il reato in oggetto potrà configurarsi nell'ipotesi in cui le sovvenzioni siano erogate a favore della azienda perché ne fruisca direttamente ovvero perché si faccia tramite della loro distribuzione ai privati destinatari dell'erogazione.

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.

Esempio
I dipendenti dell'azienda, cui sia stata affidata la gestione di un finanziamento pubblico, utilizzano i fondi per scopi diversi da quelli per i quali il finanziamento è stato erogato (ad esempio, fondi ricevuti per scopi di formazione del personale dipendente vengono utilizzati per coprire le spese di corsi già effettuati autonomamente dalla società).

2.3.3. Indebita percezione di erogazioni pubbliche (Art. 316 ter c.p. mod. dalla L. n. 3/2019 e dal D.L. n. 13/2022)

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, concessi o erogati dallo Stato, da altri enti pubblici o dalla Comunità 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 viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Il reato in oggetto è punito con la reclusione da sei mesi a tre anni. La pena è della reclusione da sei mesi a quattro anni se il fatto offende gli interessi finanziari dell'Unione europea e il danno o il profitto sono superiori a euro 100.000.
Quando la somma indebitamente percepita è pari o inferiore a 3.999,96 Euro, si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da 5.164 Euro a 25.822 Euro. Tale sanzione non può, comunque, superare il triplo del beneficio conseguito.

Il reato di cui all'art. 316-ter c.p. potrebbe configurarsi in capo alla società sotto forma di concorso nel reato. In particolare, eventuali comportamenti scorretti dell'azienda nel rilascio di garanzie fideiussorie necessarie per l'ottenimento di erogazioni pubbliche da parte di propri clienti garantiti possono integrare gli estremi di un concorso nel reato previsto dal Decreto.

Esempio

Un funzionario aziendale rilascia, in violazione della procedura aziendale adottata, una garanzia fideiussoria necessaria per l'ottenimento di un finanziamento pubblico da parte di un proprio Cliente, pur essendo a conoscenza che il garantito non possiede i requisiti di legge per l'ottenimento dell'erogazione pubblica.

2.3.4. Truffa in danno dello Stato o di altro Ente Pubblico o dell'Unione Europea (Art. 640 – Comma 2, numero 1, c.p.)

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato oppure ad altro ente pubblico o all'Unione Europea.

La pena prevista è quella della reclusione da uno a cinque anni e della multa da 309 Euro a 1.549 Euro.

Esempio

Nella predisposizione di documenti o dati per la partecipazione a procedure di gara, la società fornisce alla Pubblica Amministrazione informazioni non veritiere.

2.3.5. Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640 bis, mod. dall'art. 2, comma 1, lettera d), del D.L. 25 febbraio 2022, n. 13)

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche.

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.

La pena prevista per il reato in oggetto è quella della reclusione della reclusione da due a sette anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità' europee.

Esempio

A titolo esemplificativo, si veda il caso precedente di cui all'art. 640 c.p.: la finalità deve consistere nell'ottenimento di un finanziamento o contributo pubblico.

2.3.6. Frode informatica in danno dello Stato o di altro Ente Pubblico (Art. 640 ter c.p.)

Tale ipotesi di reato si configura nel caso in cui, l'autore del reato alterando il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno

Tale reato è punito con la reclusione da sei mesi a tre anni e con la multa da 51 a 1.032 euro ovvero.
La pena è della reclusione da uno a cinque anni e della multa da 309euro a 1.549 euro se il fatto è commesso a danno dello Stato o di un altro ente pubblico., ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.
Infine se il fatto è commesso con furto o indebito utilizzo dell'identità digitale, in danno di uno o più soggetti, la pena è la reclusione da due a sei anni e la multa da 600 a 3000 Euro.

Esempio
In concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, l'azienda violasse il sistema informatico della Pubblica Amministrazione al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

2.3.7. Frode nelle pubbliche forniture (art. 356 c.p.) [introdotto dal D.Lgs. n. 75/2020]

L'art. 356 c.p., introdotto nel catalogo dei reati presupposti dal d. lgs. n. 75/2020, punisce con la reclusione da uno a cinque anni e con la multa non inferiore a euro 1.032 chi commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi nei contratti conclusi con lo Stato, o con un altro ente pubblico, ovvero con un'impresa esercente servizi pubblici o di pubblica necessità.
La pena è aumentata se la fornitura concerne: 1) sostanze alimentari o medicinali, ovvero cose od opere destinate alle comunicazioni per terra, per acqua o per aria, o alle comunicazioni telegrafiche o telefoniche; 2) cose od opere destinate all'armamento o all'equipaggiamento delle forze armate dello Stato; 3) cose od opere destinate ad ovviare a un comune pericolo o ad un pubblico infortunio.

2.3.8. Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n.898) [introdotto dal D.Lgs. n. 75/2020]

La fattispecie, inserita nel catalogo dei reati presupposto dal d. lgs. n. 75/2020, recependo la Direttiva (UE) 2017/1371, punisce chiunque, mediante l'esposizione di dati o notizie falsi, consegue indebitamente, per sé o per altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a

carico totale o parziale del Fondo europeo agricolo di garanzia (FEAGA) e del Fondo europeo agricolo per lo sviluppo rurale (FESR). Alle suddette erogazioni sono assimilate le quote nazionali previste dalla normativa comunitaria a complemento delle somme a carico di detti Fondi, nonché le erogazioni poste a totale carico della finanza nazionale sulla base della normativa comunitaria.

La pena prevista è la reclusione da sei mesi a tre anni; da sei mesi a quattro anni quando il danno o il profitto sono superiori a euro 100.000. Quando la somma indebitamente percepita è pari od inferiore a 5.000 euro si applica soltanto una sanzione amministrativa.

2.3.9. Turbata libertà degli incanti (art. 353 c.p.) [articolo introdotto dalla L. n. 137/2023]

La fattispecie, inserita nel catalogo dei reati presupposto dal d. lgs. n. 137/2023 punisce chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche amministrazioni ovvero ne allontana gli offerenti
Le pene previste sono la reclusione da sei mesi a cinque anni e la multa da euro 103 a euro 1.032.
Se il colpevole è persona preposta dalla legge o dall'autorità agli incanti o alle licitazioni suddette la reclusione è da uno a cinque anni e la multa da euro 516 a euro 2.065.
Le pene stabilite in questo articolo si applicano anche nel caso di licitazioni private per conto di privati dirette da un pubblico ufficiale o da persona legalmente autorizzata ma sono ridotte alla metà.

La norma si colloca tra i delitti dei privati contro la pubblica amministrazione. La ratio è quella di assicurare efficace tutela rispetto alla fase di formazione dell'attività negoziale della pubblica amministrazione, con specifico riguardo alla scelta dei contraenti e al rispetto delle regole volte a disciplinare le gare cui l'amministrazione risulti interessata.
Il reato è reato di pericolo, che pertanto si configura non solo nel caso di danno effettivo, ma anche in presenza di un danno mediato e potenziale, non occorrendo l'effettivo conseguimento del risultato perseguito dagli autori dell'illecito, ma la semplice idoneità degli atti ad influenzare l'andamento della gara.

2.3.10. Turbata libertà del procedimento di scelta del contraente (art. 353-bis) [articolo introdotto dalla L. n. 137/2023]

La fattispecie, inserita nel catalogo dei reati presupposto dal d. lgs. n. 137/2023, punisce chiunque con violenza o minaccia o con doni, promesse, collusioni o altri mezzi fraudolenti turba il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della pubblica amministrazione.
Le pene previste sono la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro

1.032.
Il delitto mira a punire le condotte volte ad alterare l'iter procedimentale diretto all'emanazione di un bando di gara od atto equipollente. Si tratta pertanto di un reato di pericolo. Il bene giuridico tutelato dalla norma può essere ravvisato in prima battuta, nella trasparenza e nella correttezza del procedimento volto a stabilire il contenuto del bando o di atto equipollente. In realtà, si tratta di un reato plurioffensivo. I beni giuridici tutelati dall'art. 353-bis c.p, sono anche l'imparzialità ed il buon andamento della pubblica amministrazione e la libera iniziativa economica dei privati, specificamente, la libera concorrenza. Lo scopo della norma è quello di arginare il fenomeno delle gare di appalto mirate a favorire determinati operatori economici. In particolare si vuole evitare che tra una pluralità di partecipanti, uno di questi abbia probabilità di aggiudicazione "facile" determinata dall'alterazione della procedura prodromica all'emanazione del bando di gara, stabilendone e predeterminandone i requisiti, il contenuto e sue le peculiari caratteristiche.

2.3.11. Concussione (Art. 317 c.p.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua posizione, costringa taluno a procurare o a promettere a sé o ad altri denaro o altre utilità non dovutegli.

La pena prevista per tale reato dall'art.3 della legge n.69 del 27 maggio 2015 che ha modificato l'art. 317 c.p. è la reclusione da sei a dodici anni.

Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal Decreto, o allorquando la società svolga attività di incaricato di pubblico servizio (ad es. quando svolge l'attività volta alla riscossione tributi).

Esempio
Un dipendente, nell'esercizio delle proprie funzioni nell'attività di riscossione dei tributi, costringe un soggetto a versare una somma maggiore rispetto al tributo dovuto, procurando un vantaggio all'azienda. Tuttavia sembra più plausibile un'ipotesi di concorso in concussione.

2.3.12. Corruzione per un atto d'ufficio – Corruzione per un atto contrario ai doveri d'ufficio – Circostanze aggravanti-Induzione indebita a dare o promettere utilità-Corruzione di persona incaricata di pubblico servizio (Art. 318, 319,319bis,319quater e 320 c.p.)

Art.318 Corruzione per un atto d'ufficio
Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, riceve indebitamente per sé o per altri, denaro o altri vantaggi o ne accetta la promessa.

L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).
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 o dell'incaricato del pubblico servizio.
La pena prevista per tale reato dall'art.1 della legge n.69 del 27 maggio 2015 che ha modificato l'art. 318 c.p. è la reclusione da uno a sei anni.

Esempio
Sindaco che agevola appalti in favore dei cari o agevola l'affidamento degli appalti in favore delle persone a lui più vicine.

Art.319 Corruzione per un atto contrario ai doveri d'ufficio
Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per omettere o ritardare un atto d'ufficio (determinando un vantaggio in favore dell'offerente), riceve indebitamente per sé o per altri, denaro o altri vantaggi o ne accetta la promessa.
La pena prevista per tale reato dall'art.1 della legge n.69 del 27 maggio 2015 che ha modificato l'art. 319 c.p. è la reclusione da sei a dieci anni.

Esempio
Medico che favorisce la prescrizione e la vendita di medicinali di una determinata ditta farmaceutica ottenendo da questa denaro o altro per sè e per i suoi cari.

Art.319 bis Circostanze aggravanti
La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

Art.319 quater Induzione indebita a dare o promettere utilità
Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale abusando dei suoi poteri induce taluno a dare o a promettere per sé o per altri, denaro o altra utilità.
La pena prevista per tale reato dall'art.1 della legge n.69 del 27 maggio 2015 che ha modificato l'art. 319 quater è la reclusione da sei a dieci anni e sei mesi.

Esempio
Un dirigente offre una somma di denaro ad un funzionario di un ufficio pubblico allo scopo di ottenere il rapido rilascio di un provvedimento amministrativo necessario per l'esercizio dell'attività

della società.

Art.320 Corruzione di persona incaricata di un pubblico servizio
Le disposizioni degli artt. 318 e 319 si applicano anche all'incaricato di un pubblico servizio.
Le pene comunque sono ridotte in misura non superiore ad un terzo.

2.3.13. Corruzione in atti giudiziari (Art. 319-ter c.p.)

Tale ipotesi di reato si configura nel caso in cui la società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere o altro funzionario).

La pena prevista per tale reato **dall'art.1 della legge n.69 del 27 maggio 2015 che ha modificato l'art. 319 ter** è la reclusione da sei a 12 anni.

Se dal fatto deriva la ingiusta condanna alla reclusione non superiore a cinque anni, la pena è della reclusione da sei a quattordici anni. Se l'ingiusta condanna alla reclusione è superiore ai cinque anni o all'ergastolo, la pena è della reclusione da otto a venti anni.

Esempio
Un dirigente versa denaro ad un cancelliere del Tribunale affinché accetti, seppur fuori termine, delle memorie o delle produzioni documentali, consentendo quindi di superare i limiti temporali previsti dal codice di procedura penale a tutto vantaggio della propria difesa.

2.3.14. Pene per il corruttore (Art. 321 c.p)

Le stesse pene previste dagli artt. 318,319,319 bis,319 ter,320 si applicano a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità.

2.3.15. Istigazione alla corruzione (Art. 322 c.p.)

Tale ipotesi di reato rappresenta una "forma anticipata" del reato di corruzione. In particolare il reato di istigazione alla corruzione si configura tutte le volte in cui, in presenza di un comportamento finalizzato alla commissione di un reato di corruzione, questa non si perfezioni in quanto il pubblico ufficiale rifiuta l'offerta o la promessa non dovuta e illecitamente avanzatagli per indurlo a compiere ovvero ad omettere o ritardare un atto del suo ufficio.

Tale reato è punito con le pene previste per i reati di cu agli artt. 318 e 319 c.p., ridotte di un terzo.

Esempio

Si veda il caso enunciato relativamente al reato di corruzione per un atto d'ufficio o contrario ai doveri d'ufficio con conseguente rifiuto dell'offerta del dipendente da parte del pubblico ufficiale.

2.3.16. Peculato, concussione, corruzione ed istigazione alla corruzione di membri degli organi e di funzioni della comunità europee e di stati esteri (Art. 322 bis c.p.)

L'articolo in oggetto prevede che le ipotesi di reato sopra analizzate si applichino anche nei confronti dei seguenti soggetti, i quali sono assimilati ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi:

- membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;
- funzionari e agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- membri e addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
- coloro che, nell'ambito di altri Stati membri dell'Unione europea svolgono funzioni e attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;
- persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche internazionali;
- Le pene previste sono le stesse degli artt. 314, 316,320,322 c.p.

2.3.17. Traffico di influenze illecite (art. 346-bis c.p.) [modificato dalla L. 3/2019 e dalla L. 112/2024]

L’art. 346 bis, introdotto nel 2021 e successivamente modificato dalla L. L. 3/2019 e dalla L. 112/2024, punisce con la reclusione da un anno a quattro anni e sei mesi chi utilizzando intenzionalmente allo scopo relazioni esistenti con un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità economica, per remunerare un pubblico ufficiale o un incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis, in relazione

all'esercizio delle sue funzioni, ovvero per realizzare un'altra mediazione illecita.

Per altra mediazione illecita si intende la mediazione per indurre il pubblico ufficiale o l'incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis a compiere un atto contrario ai doveri d'ufficio costituente reato dal quale possa derivare un vantaggio indebito.
La stessa pena si applica a chi indebitamente dà o promette denaro o altra utilità economica.
La pena è aumentata se il soggetto che indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità economica riveste la qualifica di pubblico ufficiale o di incaricato di un pubblico servizio o una delle qualifiche di cui all'articolo 322-bis. La pena è altresì aumentata se i fatti sono commessi in relazione all'esercizio di attività giudiziarie o per remunerare il pubblico ufficiale o l'incaricato di un pubblico servizio o uno degli altri soggetti di cui all'articolo 322-bis in relazione al compimento di un atto contrario ai doveri d'ufficio o all'omissione o al ritardo di un atto del suo ufficio.

Esempio:
Condotta di chi sfrutta i rapporti con un pubblico ufficiale o un incaricato di pubblico servizio per farsi promettere o fornire denaro o vantaggi derivanti dalla "mediazione"; paga direttamente un pubblico ufficiale o un incaricato di pubblico servizio per ottenere favori in contrasto con i precetti della pa; paga o promette somme di denaro o altri vantaggi a soggetti della pa.

2.3.18. Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.) [articolo introdotto dalla L. n. 112/2024]

La fattispecie di cui all'art. 314 bis introdotta nel catalogo dei reati presupposto dalla L. n. 112/2024, punisce con la reclusione da sei mesi a tre anni il pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, li destina ad un uso diverso da quello previsto da specifiche disposizioni di legge o da atti aventi forza di legge dai quali non residuano margini di discrezionalità e intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale o ad altri un danno ingiusto.
La pena è della reclusione da sei mesi a quattro anni quando il fatto offende gli interessi finanziari dell'Unione europea e l'ingiusto vantaggio patrimoniale o il danno ingiusto sono superiori ad euro 100.000.

La condotta descritta dall'art. 314-bis c.p., consiste nella destinazione da parte del pubblico ufficiale o dell'incaricato di pubblico servizio del denaro o di altra cosa mobile ad un uso diverso da quello previsto da specifiche disposizioni di legge, sovrapponendosi alla condotta tipica del peculato per distrazione, che ha sempre costituito una delle espressioni tipiche del reato di abuso d'ufficio.
Il legislatore ha sostanzialmente mantenuto il reato di abuso d'ufficio nella forma del peculato per distrazione denominandolo "Indebita destinazione di denaro o cose mobili".

2.4. Le attività sensibili relative ai reati contro la Pubblica Amministrazione

Sulla base della normativa attualmente in vigore e delle analisi svolte, le Aree Sensibili identificate nelle quali è maggiore il rischio che siano posti in essere comportamenti illeciti nei rapporti con la Pubblica Amministrazione riguardano in via generale le seguenti attività:

- nelle quali si instauri un rapporto contrattuale con la P.A. A titolo d'esempio si considerino i processi di aggiudicazione e gestione di commesse pubbliche, i contratti di finanziamento su progetti di rilievo pubblicistico, i rapporti con uffici del Ministero del Lavoro o Enti previdenziali;
- nelle quali si instauri un rapporto con le istituzioni e le Autorità di Vigilanza;
- relative alla gestione degli acquisti, delle consulenze e delle liberalità;
- che comportino la gestione delle verifiche e delle ispezioni;
- che comportino la gestione dell'erogazione del credito anche attraverso fondi pubblici, sia nella fase d'acquisizione che dell'erogazione di contributi, in qualsiasi modo denominati, destinati a pubbliche finalità, sia nello svolgimento di funzioni in regime di concessione, in quanto regolate da norme di diritto pubblico ed atti autoritativi. A titolo d'esempio, si considerino i processi di acquisizione e gestione di finanziamenti agevolati per interventi formativi, finanziamenti a Clientela con agevolazioni pubbliche, rapporti di Tesoreria con Enti della P.A., riscossione tributi, servizi di concessione, pagamento e custodia per conto della P.A.;
- che comportino la gestione dei servizi informatici.

2.5. Organi e funzioni aziendali coinvolti

In relazione alle descritte Attività Sensibili, si ritengono particolarmente coinvolti i seguenti organi e funzioni nello svolgimento delle proprie attività commerciali, finanziarie, di informazione e di controllo sia in favore della società stessa sia in favore della clientela. I medesimi sono destinatari della presente Parte speciale.

▪ **Amministratore Unico**

I profili di rischio attengono alle funzioni di controllo sulle Aree Sensibili e alla gestione delle relazioni esterne (PA, privati)

▪ **CFO**

I profili di rischio attengono alla sfera decisionale e di gestione delle relazioni esterne (PA, privati)

▪ **Responsabile amministrativo**

L'attività di tale funzione aziendale potrebbe essere considerata a rischio in relazione ai rapporti intercorrenti con la Pubblica Amministrazione per gli adempimenti di varia natura ed ispezioni di organi di controllo e la gestione del ciclo attivo-passivo, contabilità, rimborsi spesa, ecc.

▪ **Responsabile operations/engineering**

L'attività di tale funzione aziendale potrebbe essere considerata a rischio in relazione ai rapporti intercorrenti con la Pubblica Amministrazione per la richiesta di autorizzazioni/permessi o per la gestione di progetti o commesse.

▪ **RSPP-Gestione ambiente**

L'attività di tale funzione aziendale potrebbe essere considerata a rischio in relazione ai rapporti intercorrenti con la Pubblica Amministrazione per adempimenti e visite ispettive in materia di sicurezza sul lavoro e gestione ambientale.

▪ **Responsabile risorse umane**

L'attività di tale funzione aziendale potrebbe essere considerata a rischio in relazione ai rapporti intercorrenti con la Pubblica Amministrazione nella gestione e amministrazione del personale.

Nel corso dell'attività di analisi condotta nell'ambito delle varie funzioni aziendali, sono state individuate le "Aree a Rischio Reato" suddivise in:

AREE RISCHIO "REATO DIRETTO"	Aree nel cui ambito sono poste in essere attività che per effetto di contatti diretti con i funzionari pubblici e/o incaricati di un pubblico servizio, comportino il rischio di commissione di uno o più dei reati contro la P.A.
AREE A RISCHIO "STRUMENTALI"	Aree strumentali alla realizzazione dei reati contro la P.A., ossia aree che gestiscono strumenti di tipo finanziario e/o mezzi sostitutivi che possono supportare la commissione e dei reati nelle aree a rischio reato diretto.

In considerazione delle attività aziendali e delle tipologie di contatti con la Pubblica Amministrazione, sono state individuate le seguenti aree a rischio. Si precisa che laddove un'area presenta le caratteristiche sia di area a rischio diretto che strumentale, onde evitare duplicazioni, la stessa è stata classificata sotto la prima tipologia.

Nell'ambito di ciascuna "area a rischio reato diretto" sono stati individuate le principali "attività sensibili", ossia quelle attività, all'interno di tali aree, al cui svolgimento è connesso il rischio di commissione dei reati considerando la sussistenza di rapporti diretti con i soggetti sopra definiti come Pubblica Amministrazione.
Di seguito si riportano le "aree a rischio reato diretto" con una breve descrizione delle attività che le compongono e l'elenco delle "aree a rischio strumentale".

ATTVITA'A RISCHIO REATO DIRETTO

Partecipazione a gare e/o appalti indetti da Enti della P.A. **Rapporti con la PA per contratti di servizio**	Si tratta dell'attività di negoziazione/stipulazione e/o esecuzione di contratti/convenzioni di concessioni con soggetti per l'attività di partecipazione a a) gare/appalti indette per l'affidamento dei servizi nonché b) rapporti intrattenuti con la Pubblica amministrazione (e.g. Prefetto) per la stipula di contratti di servizio. - Rapporti intrattenuti con le competenti autorità pubbliche in occasione della predisposizione e trasmissione delle domande volte all'ottenimento e/o rinnovo dei necessari permessi, licenze, autorizzazioni, etc. - Pagamento alle autorità pubbliche competenti dei diritti/tasse dovuti per legge al momento della presentazione dell'istanza volta all'ottenimento dei necessari permessi, autorizzazioni e licenze - Rapporti intrattenuti con la Pubblica Amministrazione e con soggetti ad essa assimilati in occasione delle verifiche ispettive periodiche effettuate da parte delle autorità competenti volte a controllare l'effettiva sussistenza dei presupposti sottostanti alla concessione e/o al rinnovo delle autorizzazioni licenze e permessi - Rapporti intrattenuti con l'Autorità di tutela dell'ambiente (Nuclei speciali delle Forze dell'Ordine, ispettori ASL, funzionari Enti locali ecc.) in occasione di verifiche volte a controllare la tutela della sicurezza sul lavoro e ambiente
Raccolta e trasporto di rifiuti	Si tratta dell'attività di esecuzione di contratti/convenzioni per l'attività di raccolta e trasporto rifiuti.
Relazioni esterne ed istituzionali	- Rapporti con la Pubblica Amministrazione e/o con soggetti ad essa assimilati in occasione della programmazione ed esecuzione dei lavori - Rapporti con la Pubblica Amministrazione e/o con soggetti ad essa assimilati in occasione di rapporti istituzionali, richieste autorizzazioni, pratiche varie, sponsorizzazioni nei vari ambiti - Rapporti con la Pubblica Amministrazione e/o con soggetti ad essa assimilati in occasione di richieste di autorizzazioni, pareri e pratiche varie per erogazioni liberali a terzi

AREE A RISCHIO REATO DIRETTO

Area fiscale	- Gestione dei rapporti con gli enti pubblici competenti in occasione delle visite ispettive, dei controlli e/o degli accertamenti - Gestione adempimenti amministrativi e fiscali, rapporti con Uffici Tributari (dichiarazione dei redditi, dichiarazione Iva, dichiarazione sostituto d'imposta)
Affari legali	- Avvio di procedimenti giudiziari o stragiudiziali dinnanzi alle competenti autorità - Gestione dei rapporti con gli enti pubblici competenti relativamente a autorizzazioni sanitarie, denunce per tributi locali, violazioni del Codice della Strada, rifiuti e pratiche varie - Gestione dell'attività di contenzioso in tutti i gradi di giudizio anche attraverso l'ausilio di legali esterni
Gestione erogazioni pubbliche	- Gestione delle domande avente ad oggetto la richiesta di finanziamenti, contributi ed aiuti pubblici nonché collazione e predisposizione della documentazione a supporto della domanda - Gestione dell'utilizzo dei finanziamenti, contributi ed aiuti pubblici conseguiti dalle competenti autorità nazionali e comunitarie - Gestione dell'attività di rendicontazione delle attività svolte all'ente pubblico erogatore - Gestione delle eventuali verifiche ispettive da parte delle competenti autorità nazionali e comunitarie al fine di verificare la destinazione dei contributi e dei finanziamenti ottenuti
Gestione dei trattamenti previdenziali del personale	Si tratta dell'attività di gestione e amministrazione degli aspetti retributivi e previdenziali connessi al personale dirigente, dipendente e ai collaboratori esterni e dei relativi rapporti con enti previdenziali ed assistenziali.
Gestione della salute e sicurezza	- Predisposizione e trasmissione alle competenti autorità della documentazione necessaria al fine di porre in essere i relativi adempimenti inerenti la salute e sicurezza sul lavoro (D.Lgs. 81/08 e successive modifiche)

		- Gestione dei rapporti con gli enti pubblici competenti in occasione delle visite ispettive, controlli e/o accertamenti
	Gestione delle problematiche ambientali	- Predisposizione e trasmissione alle competenti autorità della documentazione necessaria al fine di porre in essere i relativi adempimenti legali e non (pratiche amministrative e di attività riguardanti notifiche per nuovi impianti) - Gestione dei rapporti con gli enti pubblici competenti in occasione delle visite ispettive, controlli e/o accertamenti
	Amministrazione	- Gestione dei rapporti con gli enti pubblici competenti in occasione delle visite ispettive, controlli e/o accertamenti

STRUMENTALI	**SISTEMI INFORMATIVI**
	FINANZA E TESORERIA
	CONTABILITÀ FORNITORI
	CONTABILITÀ CLIENTI
	GESTIONE OMAGGI, LIBERALITA' E SPONSORIZZAZIONI
	ACQUISTI MATERIALI TECNICI E VARI

Eventuali integrazioni delle suddette aree a rischio reato potranno essere proposte all'Amministratore Unico dall'Organismo di Vigilanza e dagli altri organi di controllo della società per effetto dell'evoluzione dell'attività di impresa e conseguentemente di eventuali modifiche dell'attività svolta dalle singole funzioni aziendali.

L'analisi del rischio della commissione dei reati di cui alla presente Sezione della Parte speciale in relazione alle aree ed attività sensibili sopra indicate e mappate riscontra un livello di rischio BASSO in considerazione dei seguenti elementi di sintesi.
BPR Group fornisce prestazioni di consulenza, servizi e forniture a imprese; allo stato attuale non si rivolge a pubbliche amministrazioni e non partecipa pertanto a tal fine a gare pubbliche. I rapporti con le pubbliche amministrazioni sono quelli tipici di qualsiasi organizzazione d'impresa e riguardano principalmente l'area degli adempimenti fiscali, previdenziali, assicurativi, sicurezza sul lavoro ed ambiente e di gestione di eventuali visite ed ispezioni. La maggior parte delle attività è

gestita in via telematica ed avvalendosi del professionista esterno incaricato. L'azienda è dotata di sistemi informativi interni e software gestionali che consentono un puntuale presidio delle attività di gestione e della loro correttezza. BPR Group si avvale talora di finanziamenti pubblici ma il processo è gestito con il supporto di enti/professionisti specializzati con un monitoraggio esterno-interno di tutte le fasi. Nella storia aziendale non ci registrano anomalie e/o contenziosi di particolare rilevanza.

2.6. Principi e governance

Premesso quanto sopra, si individuano qui di seguito i principi che informano le specifiche procedure interne dell'azienda previste in relazione a qualsiasi operazione/attività che coinvolga un ente della Pubblica Amministrazione, nonché le regole di condotta che sottendono alle specifiche previsioni di comportamento elaborate dalla società in relazione a tale ambito di applicazione.
Si stabilisce pertanto che tutte le regole, i processi e le prassi operative nei rapporti con la P.A. devono rispettare i principi e le regole di comportamento nel seguito delineate.

Principi

Tutte le operazioni/attività che coinvolgono in qualsiasi modo un ente della Pubblica Amministrazione devono essere poste in essere nel pieno rispetto delle leggi vigenti, del Codice Etico e del Codice di Comportamento Interno, delle regole contenute nel presente Modello, delle policy e delle procedure aziendali, dei valori e delle politiche della società.

La struttura aziendale è articolata in modo tale da soddisfare i requisiti fondamentali di formalizzazione, chiarezza, comunicazione e separazione dei ruoli richiesti in generale nel Decreto e di peculiare importanza nella gestione dei rapporti con la Pubblica Amministrazione, in particolare per ciò che concerne l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

La società è dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, mansionari etc.) improntati a principi generali di:

- conoscibilità all'interno della società;
- chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;
- chiara descrizione delle linee di riporto.

Il sistema di deleghe

In linea di principio il sistema di deleghe, formalizzato in apposito documento approvato dall'Amministratore Unico, stabilisce espressamente le facoltà di autonomia gestionale per natura di spesa e di impegno, ivi inclusi quelli nei confronti della Pubblica Amministrazione.

Si intende per "delega" quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative.

I requisiti essenziali del sistema di deleghe, ai fini di una efficace prevenzione dei reati sono i seguenti:

- Le funzioni che intrattengono per conto della Società rapporti con la P.A. devono essere individuate e preferibilmente dotate di delega formale in tal senso;
- Le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;
- Ciascuna delega deve definire in modo specifico:
  - I poteri del delegato;
  - Il soggetto (organo o individuo) cui il delegato riporta gerarchicamente.
- I poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- Il delegato deve disporre di eventuali poteri di spesa adeguati alle funzioni conferitegli.

L'Organismo di Vigilanza verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative (tali sono quei documenti interni all'azienda con cui vengono conferite le deleghe), raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

2.7. Norme generali di comportamento

I soggetti destinatari della presente Parte Speciale coinvolti nelle attività elencate nei paragrafi precedenti devono rispettare principi e norme di comportamento di seguito dettate, nel rispetto degli obblighi normativi, delle procedure aziendali e del Codice Etico aziendale.

Coerentemente con i principi del Codice Etico, i rapporti tra la società e la Pubblica Amministrazione, devono essere condotti in conformità alla legge e nel rispetto dei principi di lealtà, correttezza, trasparenza e verificabilità.

È obbligatorio segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

Si sottolinea che è assolutamente vietato:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, assunti individualmente o nel particolare contesto in cui si collocano, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/2001);
- Promettere, offrire o acconsentire all'elargizione di denaro o altre utilità (beni materiali, servizi, etc.) a pubblici ufficiali o incaricati di pubblico servizio, o a loro familiari, che possano influenzare l'indipendenza del giudizio o indurre ad assicurare un vantaggio per la società;
- Accordare vantaggi di qualsiasi natura (promessa di assunzione, etc.) in favore di rappresentanti della Pubblica Amministrazione che possano determinare le stesse conseguenze previste al punto precedente;
- Distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo eccedente le normali pratiche commerciali o di cortesia, comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale) ed in particolare, è vietata qualsiasi forma di regalo a funzionari pubblici o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico o culturale, o la brand image della società. I regali offerti - salvo quelli di modico valore, devono essere documentati in modo adeguato a consentire le verifiche da parte dell'OdV;
- Mettere in atto o favorire operazioni in conflitto di interesse dell'azienda, nonché attività in grado di interferire con la capacità di assumere decisioni imparziali nell'interesse dell'azienda nel rispetto del Codice Etico e delle normative applicabili;
- Effettuare prestazioni in favore dei Consulenti e dei Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- Riconoscere compensi in favore dei Consulenti e dei Partner che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;
- Effettuare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati, o comunque utilità a carico di bilanci pubblici, e/o per partecipare a gare o simili o risultarne vincitori;
- Effettuare comunque dichiarazioni o attestazioni non veritiere ad organismi pubblici tali da indurre in errore tali soggetti, da creare un indebito profitto o vantaggio a favore della società e/o arrecare un danno all'ente pubblico;
- Destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;

- Violare i principi e le procedure aziendali previste nella presente sezione della Parte Speciale.

Al fine di scongiurare la commissione dei reati di cui alla presente sezione devono essere realizzati i seguenti presidi di controllo:

- Distribuzione delle responsabilità e previsione di adeguati livelli autorizzativi nelle attività di predisposizione, presentazione e ricezione di dati, informazioni e documenti verso/da rappresentanti della Pubblica Amministrazione, allo scopo di evitare sovrapposizioni funzionali o eccessive concentrazioni di potere;
- Formale identificazione del soggetto deputato ad intrattenere rapporti con la PA. in relazione a ciascuna Potenziale Attività a Rischio;
- Gestione in modo trasparente e univoco di qualsiasi rapporto professionale instaurato con membri della Pubblica Amministrazione o con soggetti qualificabili come Pubblici Ufficiali o Incaricati di Pubblico Servizio;
- Attività di reporting all'OdV di eventuali situazioni di irregolarità.

2.8. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Gli Organi Sociali, gli amministratori, i dipendenti e i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali, nell'ambito delle attività da essi svolte, devono rispettare le regole ed i divieti elencati al precedente paragrafo e ai fini dell'attuazione degli stessi devono rispettare le procedure specifiche qui di seguito descritte, oltre alle Regole e Principi Generali già contenuti nella Parte Generale del Modello 231.
In particolar modo nella gestione dei rapporti con la Pubblica Amministrazione devono essere osservate, tra le altre, le regole di comportamento di seguito indicate:

- Agli Organi Sociali, Dipendenti, Consulenti e Partner che materialmente intrattengono rapporti con la PA per conto dell'azienda deve essere formalmente conferito potere in tal senso dalla società (con apposita delega per i membri degli organi sociali e per i dipendenti - anche tramite il responsabile, individuato in base al sistema delle comunicazioni organizzative, ovvero nel relativo contratto di servizio o di consulenza o di partnership per gli altri soggetti destinatari del Modello 231). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica delega scritta che rispetti tutti i criteri elencati nella Parte Generale;

- I contratti tra l'azienda, i Consulenti e Partner che abbiano, anche solo potenzialmente, impatto sulle Potenziali Aree a Rischio devono essere definiti per scritto in tutte le loro condizioni e termini e devono contenere clausole standard al fine di garantire il rispetto del D.Lgs. 231/2001;

- Le dichiarazioni rese ad organismi pubblici nazionali o comunitari ai fini dell'ottenimento di contributi, finanziamenti, ed in genere di benefici a carico di bilanci pubblici, devono contenere

solo elementi veritieri e, l'impegno della società, in caso di ottenimento degli stessi, all'effettiva utilizzazione dei fondi ottenuti secondo le finalità previste dalla specifica normativa di riferimento. In ogni caso, ciascuna delle dichiarazioni di cui al presente capo, ivi incluse le autocertificazioni ammesse dalla legge o dai bandi, devono essere corredate da documentazione idonea ad attestarne la veridicità, anche se eventualmente non richiesta dal destinatario di tali dichiarazioni;

- Alle ispezioni giudiziarie, tributarie e amministrative (es. relative al D.Lgs. 81/08 e successive modifiche, a verifiche tributarie, INPS, etc.) devono partecipare i soggetti a ciò espressamente delegati, dando avviso dell'avvio dell'ispezione/accertamento al Legale rappresentante ed all'OdV. Di tutto il procedimento relativo all'ispezione devono essere redatti e conservati appositi verbali. Nel caso il verbale conclusivo evidenziasse criticità, l'OdV ne deve essere informato con nota scritta da parte del responsabile coinvolto;

- La stipulazione di contratti/convenzioni con soggetti pubblici da parte della Società a seguito della partecipazione a procedure ad evidenza pubblica (asta pubblica, appalto-concorso, licitazione privata e trattative private) deve essere condotta in conformità ai principi, criteri e disposizioni dettate dal presente Modello;

- Qualunque tipo di erogazione di fondi:
  - deve essere deliberata previa adeguata istruttoria cui partecipino soggetti e funzioni diverse all'interno dell'azienda, in modo da minimizzare il rischio di una manipolazione illecita dei dati ed aumentare la condivisione delle conoscenze e delle decisioni aziendali;
  - presuppone una approfondita conoscenza della clientela, così da consentire una valutazione della coerenza e della compatibilità dell'operazione con il profilo del cliente, soprattutto laddove quest'ultimo non svolga attività di rilievo economico;
  - ai collaboratori esterni e partner che materialmente intrattengono rapporti con la P.A. per conto dell'azienda, deve essere formalmente conferito potere in tal senso dall'azienda stessa, con apposita clausola contrattuale;

- L'Organismo di Vigilanza deve essere informato con nota scritta di qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la P.A..

Si rinvia espressamente ai Protocolli speciali di prevenzione allegati al presente Modello di organizzazione, gestione e controllo.

2.9. I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui agli artt. 24 e 25 del Decreto, commessi nell'interesse o a vantaggio dell'azienda diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello.

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati di cui agli artt. 24 e 25 del Decreto sono i seguenti:

- Proporre che vengano redatte o aggiornate eventuali procedure per prevenire la commissione dei reati nei rapporti con la Pubblica Amministrazione, di cui alla presente Parte Speciale; con riferimento a tale punto l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di commissione dei suddetti reati, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere; o proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Parte Speciale;

- Monitorare sul rispetto delle eventuali procedure interne per la prevenzione dei reati oggetto della presente Parte Speciale. Sulla base dei flussi informativi ricevuti l'Organismo di Vigilanza condurrà verifiche mirate su determinate operazioni effettuate nell'ambito delle Aree Sensibili, volte ad accertare da un lato il rispetto di quanto stabilito nel Modello e nei protocolli, dall'altro l'effettiva adeguatezza delle prescrizioni in essi contenute a prevenire i reati potenzialmente commissibili;

- Esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute. L'Organismo di Vigilanza, inoltre, è tenuto alla conservazione dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

2.10. Flussi informativi all'Organismo di vigilanza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace attuazione del Modello e di curarne l'aggiornamento dovranno essere assicurati i seguenti flussi informativi periodici:

Documenti	Periodicità	Soggetto tenuto
○ Schema di bilancio in via preventiva ○ Bilancio CEE approvato e documentazione collegata ○ Variazione significativa dei criteri contabili applicati nella determinazione delle poste di bilancio ○ Variazioni eventualmente apportate al Piano dei Conti ○ Report riconciliazione contabilità/banca ○ Elenco eventuali posizioni di insolvenza ○ Copia di eventuali transazioni ○ Elenco sponsorizzazioni, contributi, liberalità con indicazione del beneficiario e tipologia	Annuale	Responsabile Amministrativo
○ Elenco incarichi professionali/consulenze affidati ○ Notifica delle assunzioni effettuate ○ Report rimborsi spese dipendenti/amministratori/collaboratori ○ Report spese di rappresentanza	Annuale	Responsabile RU
○ Report pratiche in essere con enti pubblici (autorizzazioni, permessi, ecc.) ○ Verbali delle visite ispettive da parte di enti pubblici di controllo	Semestrale All'atto di visite/ispezioni	Ufficio tecnico RSPP Responsabile RU Responsabile amministrativo RSPP
In merito a progetti/attività a finanziamento pubblico: ○ Richiesta di contributo/finanziamento ○ Comunicazione di concessione del contributo/finanziamento ○ Report sull'andamento del progetto ○ Copia registro in caso di attività di formazione ○ Documentazione inerente la rendicontazione del progetto	All'atto della richiesta contributo e gestione di ogni progetto finanziato	Responsabile amministrativo Responsabile RU Responsabile R&D
In merito a eventuali contenziosi: ○ Segnalazione pre-contenziosi e contenziosi aperti e loro chiusura ○ Elenco delle transazioni, conciliazioni e rinunce con indicazione delle controparti e degli importi correlativi	Annuale	Amministratore Unico CFO Responsabile amministrativo

○ Segnalazione di eventuali violazioni del regolamento informatico ○ Segnalazione di eventuali criticità nei sistemi di archiviazione/backup ○ Denunce alle autorità competenti a fronte di violazioni della security	Al verificarsi della condizione	Coordinatore Sistemi informativi Responsabile sistemi informativi Amministratore di sistema

Tutti i destinatari della presente Parte speciale sono in ogni caso tenuti ad effettuare segnalazioni all'Organismo di vigilanza qualora rilevino eventuali non conformità relative all'applicazione del flusso; al rispetto di procedure/regolamenti; al rispetto delle disposizioni del Modello di organizzazione, gestione e controllo, del Codice etico e in generale del d. lgs. n. 231/2001 e smi.

PARTE SPECIALE

SEZIONE 3 - REATI SOCIETARI

INDICE

3.1 Introduzione e funzione della parte speciale dedicata ai reati societari 3
3.2 Le fattispecie di reato richiamate dal D.Lgs 231/01 3
3.2.1 False comunicazioni sociali (art. 2621, 2621 bis, 2621 ter c.c. mod. L.69 del 27 maggio 2015) 4
3.2.2 False comunicazioni sociali delle società quotate (art. 2622 c.c. mod..69 del 27 maggio 2015) 5
3.2.3 Impedito controllo (art. 2625 c.c. modificato da D.Lgs n.39 del 27 gennaio 2010) 5
3.2.4 Indebita restituzione dei conferimenti (art. 2626 c.c.) 6
3.2.5 Illegale ripartizione degli utili o delle riserve (art. 2627 c.c.) 6
3.2.6 Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.) 6
3.2.7 Operazioni in pregiudizio dei creditori (art. 2629 c.c.) 7
3.2.8 Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.) 7
3.2.9 Formazione fittizia del capitale (art.2632 c.p.) 8
3.2.10 Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.) 8
3.2.11 Illecita influenza sull'assemblea (art. 2636 c.c.) 8
3.2.12 Aggiotaggio (art. 2637 c.c.) 9
3.2.13 Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.) 9
3.2.14 False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023) 9
3.3 Le attività sensibili relative ai reati societari 10
3.4 Organi e funzioni aziendali coinvolte 11
3.5 Principi e regole di comportamento 12
3.6 Principi e norme generali di comportamento 12
3.7 Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili 13
3.8 I controlli dell'Organismo di Vigilanza 17
3.9 Flussi informativi all'Organismo di Vigilanza 18

3.1. Introduzione e funzione della Parte Speciale dedicata ai reati societari

La presente Parte Speciale si riferisce a comportamenti posti in essere dai dipendenti e dagli organi Societari dell'azienda, nonché dai suoi collaboratori esterni e dai suoi partner, come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale è che tutti i destinatari, conducano comportamenti conformi a quanto ivi rescritto al fine di impedire il verificarsi degli illeciti di cui all'art. 25-ter del Decreto.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- Indicare i principi procedurali e le regole di comportamento che i destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza e ai responsabili delle funzioni aziendali che cooperano con tale organismo gli strumenti esecutivi per esercitare le attività di controllo, di monitoraggio e di verifica.

La società adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione delle fattispecie delittuose di seguito descritte.

3.2. Le fattispecie di reato richiamate dal D.Lgs. 231/01

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D.Lgs. n. 231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

L'art. 25-ter del Decreto contempla la maggior parte dei reati societari che costituiscono, al momento, insieme agli abusi di mercato, i soli reati autenticamente economici di cui può essere chiamata a rispondere la Società e che, in quanto non occasionati dall'esercizio della specifica attività aziendale, sono qualificabili come reati generali.

Di seguito si riporta una breve descrizione dei reati societari richiamati dall'art. 25-ter (Reati societari) del D.Lgs. 231/01 e s.m.i.

3.2.1. False comunicazioni sociali (Art. 2621, 2621 bis, 2621 ter c.c.)

Questo reato si realizza tramite:

- l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni idonee ad indurre in errore i destinatari sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, con l'intenzione di ingannare i soci o il pubblico;
- l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.

La pena prevista per tale reato dall'art. 9. della legge n.69 del 27 maggio 2015 che ha modificato l'art. 2621, è la reclusione da uno a cinque anni.

L'art. 10. della legge n.69 del 27 Maggio 2015 introduce gli articoli 2621 bis e ter del codice civile e recita:

Art. 2621-bis Fatti di lieve entità

Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.

Art. 2621-ter Non punibilità per particolare tenuità

Ai fini della non punibilità per particolare tenuità del fatto, di cui all'articolo 131-bis del codice penale, il giudice valuta, in modo prevalente, l'entità dell'eventuale danno cagionato alla società, ai soci o ai creditori conseguente ai fatti di cui agli artt.2621 e 2621bis.

Si precisa che:

- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- le informazioni false o omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;
- la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Esempio

L'Amministratore Unico ignora l'indicazione del responsabile amministrativo circa l'esigenza di un accantonamento (rettifica) al Fondo svalutazione crediti a fronte della situazione di crisi di un cliente, ed iscrive un ammontare di crediti superiore al dovuto; ciò al fine di non far emergere una perdita che comporterebbe l'assunzione di provvedimenti sul capitale sociale (artt. 2446 e 2447 c.c.).

3.2.2. False comunicazioni sociali delle società quotate (Art.2622 c.c.)

Alle società indicate nel comma precedente sono equiparate:

- le società emittenti strumenti finanziari per i quali è stata presentata una richiesta di ammissione alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;
- le società emittenti strumenti finanziari ammessi alla negoziazione in un sistema multilaterale di negoziazione italiano;
- le società che controllano società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea;
- le società che fanno appello al pubblico risparmio o che comunque lo gestiscono.

Le disposizioni di cui ai commi precedenti si applicano anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi.

L'art. 11. della legge n.69 del 27 maggio 2015 sostituisce l'articolo 2622 del codice civile e recita:

Art. 2622 False comunicazioni sociali delle società quotate

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società emittenti strumenti finanziari ammessi alla negoziazione in un mercato regolamentato italiano o di altro Paese dell'Unione europea, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico consapevolmente espongono fatti materiali non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da tre a otto anni.

3.2.3. Impedito controllo (art. 2625 c.c. modificato da D.Lgs n.39 del 27 gennaio 2010)

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

Il reato è punito con la sanzione amministrativa di 10.329 Euro.

Se la condotta ha però cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa.

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58.

Esempio

Un funzionario della società rifiuta di fornire alla società di revisione i documenti richiesti per l'espletamento dell'incarico, quali, ad esempio, quelli concernenti le azioni legali intraprese dalla società per il recupero di crediti.

3.2.4. 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 ai soci o la liberazione degli stessi dall'obbligo di eseguirli. La pena prevista è fino ad un anno di reclusione.

Esempio

L'Assemblea dell'azienda, su proposta dell'Amministratore Unico, delibera la compensazione di un debito di un socio nei confronti della società con il credito da conferimento che quest'ultima vanta nei confronti del socio medesimo, attuando di fatto una restituzione indebita del conferimento.

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

Tale condotta criminosa 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.
La pena prevista è fino ad un anno di reclusione.
Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Esempio

L'Assemblea della Società, su proposta dell'Amministratore Unico, delibera la distribuzione di dividendi che costituiscono, non un utile di esercizio, ma fondi non distribuibili perché destinati dalla legge a riserva legale.

3.2.6. Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)

Questo reato si perfeziona con l'acquisto o la sottoscrizione di azioni o quote sociali della società controllante, che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.
La pena prevista è fino ad un anno di reclusione.
Si fa presente che se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio, relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

Esempio
L'Organo amministrativo procede all'acquisto o alla sottoscrizione di azioni della società o di una società controllante fuori dai casi di cui all'artt. 2357, 2359-bis del codice civile, cagionando in tal modo una lesione del patrimonio sociale.

3.2.7. Operazioni in pregiudizio dei 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 altra società o scissioni, che cagionino danno ai creditori.
Il reato è punito, a querela della persona offesa, da sei mesi a tre anni.
Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.
Esempio
L'organo amministrativo delibera una riduzione del capitale sociale senza osservare i presupposti richiesti dalla legge, cagionando in tal modo un danno ai creditori sociali.

3.2.8. Omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.)

Il reato si perfeziona nel caso in cui l'amministratore di una società con azioni quotate non comunichi agli altri amministratori e al Revisore Unico un interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, cagionando a seguito di tale omissione un danno alla società o a terzi.
Tale ipotesi di reato non può configurarsi in capo all'azienda se questa non è quotata.

Esempio
Un amministratore di una società quotata, nel corso di una riunione dell'Amministratore Unico della stessa, convocato per valutare e deliberare un'acquisizione societaria ad un prezzo eccessivo rispetto

al reale valore del target, non comunica agli altri consiglieri che sua moglie è proprietaria di una partecipazione di maggioranza nella società oggetto dell'acquisizione.

3.2.9. Formazione fittizia del capitale (art. 2632 c.c.)

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

Esempio
L'Assemblea dell'azienda, su proposta dell'Amministratore Unico, delibera l'aumento del capitale sociale con un conferimento di beni sopravvalutati in modo rilevante.

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

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

Il reato è punito, a querela della persona offesa, da sei mesi a tre anni.
Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

3.2.11. Illecita influenza sull'assemblea (art. 2636 c.c.)

La "condotta tipica" prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.
La pena prevista è da sei mesi a tre anni di reclusione.

Esempio
L' Amministratore Unico della società, al fine di ottenere una deliberazione favorevole dell'assemblea e il voto determinante anche del socio di maggioranza, predispone e produce nel corso dell'adunanza assembleare documenti alterati, diretti a far apparire migliore la situazione economica e finanziaria di un'azienda che lo stesso Amministratore Unico intende acquisire, in modo da ricavarne un indiretto profitto.

3.2.12. Aggiotaggio (art. 2637 c.c.)

La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di società o gruppi.
La pena prevista è da uno a cinque anni di reclusione.

Esempio
Il Direttore Generale dell'azienda diffonde al mercato la notizia del mancato rilascio da parte societaria di una polizza fideiussoria richiesta nell'ambito di un'operazione avente ad oggetto il trasferimento di azioni di una società non quotata. A causa di tale comunicazione il potenziale acquirente rinuncia a concludere il contratto di compravendita dei suddetti titoli.

3.2.13. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.)

La condotta criminosa si realizza attraverso l'esposizione nelle comunicazioni alle autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero con l'occultamento, in tutto o in parte, con altri mezzi fraudolenti di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

L'art.101 comma 1 del D.Lgs n.180 del 16 novembre 2015 stabilisce che agli effetti della legge penale, le autorità' e le funzioni di risoluzione di cui al decreto di recepimento della direttiva 2014/59/UE sono equiparate alle autorità
e alle funzioni di vigilanza.

Esempio
Il Direttore Generale della Società omette di comunicare alla Consob l'acquisizione di una partecipazione rilevante, al fine di evitare possibili controlli dell'autorità di vigilanza

3.2.14. False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023 aggiunto dal D.Lgs. n. 19/2023)

L'art. 54 del D. Lgs. 19/2023 punisce con la reclusione da 6 mesi a 3 anni "chiunque, al fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all'articolo 29, forma documenti in tutto o in parte falsi, altera documenti veri, rende dichiarazioni false oppure omette

informazioni rilevanti". In caso di condanna ad una pena non inferiore a mesi 8 di reclusione, al responsabile sarà applicata altresì la pena accessoria dell'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese, prevista dall'art. 32-bis c.p.

La condotta si realizza mediante la formazione di documenti falsi, l'alterazione di documenti veri, la presentazione di false dichiarazioni, ovvero l'omissione di informazioni rilevanti. Con riferimento all'elemento soggettivo, il delitto è punito a titolo di dolo specifico consistente nel fine di far apparire adempiute le condizioni per il rilascio del certificato preliminare di cui all'art. 29 del D. Lgs. 19/2023.
Il certificato preliminare è un atto rilasciato dal notaio attestante l'adempimento degli atti e delle formalità preliminari alla realizzazione di una fusione transfrontaliera. Il citato art. 29, in particolare, stabilisce che, su richiesta della società italiana partecipante alla fusione transfrontaliera, il notaio rilascia il certificato preliminare attestante il regolare adempimento, in conformità alla legge, degli atti e delle formalità preliminari alla realizzazione della fusione.

3.3. Le attività sensibili relative ai reati societari

L'art. 6, comma 2, lett. a) del D.Lgs. 231/01 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Sulla base delle caratteristiche specifiche di BPR Group e della mappatura di dettaglio delle aree e funzioni aziendali i reati che possono astrattamente avere possibilità di verificazione, il cui rischio è in ogni caso valutato BASSO, sono:

- ✓ **False comunicazioni sociali (art. 2621 c.c.)**
- ✓ **False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.)**

Gli altri reati previsti dall'art. 25-ter non sono stati, allo stato attuale, valutati rilevanti in quanto la probabilità di commissione di tali reati è ritenuta remota o impossibile in relazione alle caratteristiche di BPR Group, società che non opera nei mercati finanziari e a livello internazionale/transfrontaliero. La società si riserva di aggiornare il presente Modello 231 nel caso in cui dovesse emergere la significatività di uno o più degli altri reati sopra elencati.

Principali Aree a rischio e attività sensibili interessate:

- **Predisposizione di bilanci e documentazione di natura contabile**: si tratta delle attività relative alle chiusure, contabili, alla contabilizzazione dei dati e alla predisposizione del bilancio d'esercizio della Società e dei relativi allegati;
- **Gestione della Contabilità Generale:**
- **Imputazione delle scritture contabili in contabilità generale;**
- **Verifiche sui dati contabili immessi a sistema e quelli inviati al consulente esterno;**
- **Predisposizione di documenti ai fini delle delibere assembleari e delle decisioni dell'Amministratore Unico**: si tratta delle attività di predisposizione della documentazione relativa all'oggetto dell'Assemblea e dell'Amministratore Unico per consentire a questi ultimi di esprimersi sulle materie di propria competenza sottoposte ad approvazione;
- **Gestione delle comunicazioni verso soci:** si tratta dell'attività di predisposizione della documentazione oggetto di comunicazioni verso soci.

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

a) degli standard di controllo generali;
b) dei principi di comportamento individuati nel Codice Etico;
c) di quanto già regolamentato dalla documentazione e dalle procedure aziendali;
d) delle disposizioni di legge.

È responsabilità del legale rappresentante segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche/integrazioni da apportare alla Parte Speciale, in accordo a quanto previsto dalla Parte Generale.

3.4. Organi e funzioni aziendali coinvolte

In relazione alle descritte Attività Sensibili, si ritengono particolarmente coinvolti i seguenti organi e funzioni aziendali:

- **Amministratore Unico**
  I profili di rischio attengono alle funzioni di controllo sulle Aree Sensibili, nonché le attività relative alla gestione dei valori svolte sia per conto della società sia per conto della clientela.
- **Responsabile amministrativo**
  L'attività di questa funzione si considera astrattamente a rischio per la gestione della corretta rappresentazione dei risultati economici, degli adempimenti fiscali ed i rapporti con le Autorità di Vigilanza.

3.5. Principi e regole 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 normativa interna aziendale relativa al sistema amministrativo, finanziario e contabile.
I destinatari, inoltre, sono tenuti ad operare sulla base della *best practice* cui l'azienda si ispira nell'esercizio delle proprie funzioni, sul fondamento che qualsiasi condotta attiva od omissiva posta in essere in violazione diretta od indiretta dei principi normativi e delle regole procedurali interne che attengono alla formazione della documentazione contabile ed alla rappresentazione esterna, così come all'esercizio delle attività di controllo e di vigilanza è da considerare come commessa in danno della azienda stessa.

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, le politiche e le procedure aziendali nonché le regole contenute nel Modello 231 e nella presente parte speciale operando, in questo modo, in coerenza con i valori e i principi che sono alla base dell'attività d'impresa in azienda.

In generale, il sistema di organizzazione, gestione e controllo della società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della Società, devono conoscere e rispettare:

- La normativa italiana e straniera applicabile alle attività svolte;
- Il Codice Etico Aziendale ed Appendice Applicativa;
- Il presente Modello 231;
- Le procedure e le linee guida aziendali nonché tutta la documentazione attinente al sistema di organizzazione, gestione e controllo della società.

3.6 Principi e norme generali di comportamento

In linea generale al fine di perseguire la prevenzione dei Reati Societari è fatto espresso divieto a tutti i Soggetti destinatari del Modello 231 di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25-ter del D.Lgs. 231/01, nonché di porre in essere

comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Parte Speciale.

Con riferimento a quanto espresso sopra, la società obbliga i suoi Amministratori, dipendenti e soggetti terzi che agiscono in rappresentanza della società al rispetto, in particolare, dei seguenti principi:

- I bilanci e le comunicazioni sociali previsti dalla Legge devono essere redatti con chiarezza e rappresentare in modo corretto e veritiero la situazione patrimoniale, economica e finanziaria della società;
- È vietato, anche mediante condotte dissimulate, restituire i conferimenti effettuati dai soci o liberarli dall'obbligo di eseguirli, fuori dai casi di legittima riduzione del capitale sociale;
- È vietato ripartire utili non effettivamente conseguiti o distribuire riserve indisponibili;
- È vietato effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di Legge a tutela dei creditori;
- È vietato formare od aumentare fittiziamente il capitale delle società, mediante attribuzione di quote per somma inferiore al loro valore nominale, sottoscrizione reciproca di quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti, ovvero del patrimonio delle società in caso di trasformazione.

Quanti venissero a conoscenza di omissioni, manomissioni, falsificazioni o trascuratezza della contabilità o della documentazione di supporto sulla quale le registrazioni contabili si fondano, sono tenuti a riferire i fatti al responsabile individuato nel Legale rappresentante e all'Organismo di Vigilanza.

Per ogni operazione contabile deve essere conservata agli atti sociali un'adeguata documentazione di supporto dell'attività svolta, in modo da consentire l'agevole registrazione contabile e la ricostruzione dell'operazione.

3.7. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

I Destinatari e in generale Organi Sociali, Amministratori, dipendenti nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, dovranno tener conto, oltre a quanto precedentemente descritto e relativamente ad ognuna delle fattispecie di reato ritenute rilevanti per la Società, delle previsioni di seguito Indicate:

1. **False comunicazioni sociali (art. 2621 c.c.)**
2. **False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.)**

Ai fini di prevenire i reati di false comunicazioni sociali e di false comunicazioni sociali in danno della Società, dei soci o dei creditori, i soggetti sopra indicati hanno l'espresso obbligo di tenere un

comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla
formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società.

A tale riguardo, deve essere loro cura, a titolo esemplificativo, astenersi da:

a) rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società;
b) omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società;
c) porre la massima attenzione e accuratezza nell'acquisizione, elaborazione e illustrazione dei dati e delle informazioni utilizzati in modo tale da fornire una presentazione veritiera e corretta corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività.

Inoltre, gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, dovranno tener conto, oltre a quanto precedentemente definito delle procedure e regole aziendali che prevedono:

- il rispetto del Codice Etico e delle sue specifiche previsioni riguardanti il corretto comportamento di tutti i soggetti coinvolti nelle attività di formazione del bilancio o di altri documenti similari, quali ad esempio:

a) massima collaborazione, veridicità, autenticità ed originalità della documentazione e delle informazioni trattate;
b) chiarezza e correttezza della rappresentazione patrimoniale e finanziaria della società;
c) completezza, segnalazione di eventuali omissioni, manomissioni, falsificazioni o trascuratezza della contabilità o della documentazione di supporto sulla quale le registrazioni contabili si fondano, etc.

- il rispetto del calendario di chiusura, finalizzato alla redazione del bilancio indicante:
    a) Data di chiusura dei periodi contabili;
    b) Data di chiusura delle scritture contabili;
    c) Data di predisposizione della Bozza del Bilancio e del Bilancio definitivo.

- la chiara definizione della responsabilità della veridicità, autenticità ed originalità della documentazione e delle informazioni e dei dati forniti dal Responsabile della determinazione delle varie poste/fondi;

- il supporto documentale a corredo delle informazioni e dei dati forniti dal Responsabile di cui al punto precedente;

- il controllo, da parte del consulente esterno incaricato nella predisposizione del bilancio delle voci aggregate di Bilancio confrontandole con quelle dell'anno precedente, mantenendo evidenza del riscontro effettuato e delle eventuali motivazioni relative a scostamenti anomali;

- la tracciabilità informatica delle operazioni effettuate.

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Societari aziendali (e dei Dipendenti e Collaboratori esterni nella misura necessaria alla funzione 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 (art. 25-ter del D.Lgs. n. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

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

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure interne, in tutte le attività finalizzate alla formazione del bilancio 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 della società;
2. tenere comportamenti corretti, nel rispetto delle norme di legge e delle procedure interne, ponendo la massima attenzione ed accuratezza nell'acquisizione, elaborazione ed illustrazione dei dati e delle informazioni relative agli strumenti finanziari emessi da altre società del Gruppo, necessarie per consentire agli investitori di pervenire ad un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della società, sull'evoluzione della sua attività, nonché sugli strumenti finanziari e relativi diritti;
3. 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;
4. assicurare il regolare funzionamento degli Organi Societari, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;

5. evitare di porre in essere operazioni simulate o diffondere notizie false idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari;
6. effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate.

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

- con riferimento al precedente punto 1:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà sulla situazione economica, patrimoniale e finanziaria della società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società.

- con riferimento al precedente punto 2:

- alterare i dati e le informazioni destinati alla predisposizione dei prospetti informativi eventualmente predisposti dalla società;
- illustrare i dati e le informazioni utilizzati in modo tale da fornire una presentazione non corrispondente all'effettivo giudizio maturato sulla situazione patrimoniale, economica e finanziaria della società e sull'evoluzione della sua attività, nonché sugli strumenti finanziari e relativi diritti.

- con riferimento al precedente punto 3:

- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- acquistare o sottoscrivere azioni della società o di società controllate fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale;
- effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- procedere a formazione e/o aumenti fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale.

- con riferimento al precedente punto 4:

- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che, in altro modo, ostacolino lo svolgimento dell'attività di controllo e di revisione della gestione sociale da parte del Revisore Unico o della società di revisione o che comunque la ostacolino;

- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare.

- con riferimento al precedente punto 5:

- pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio aventi ad oggetto strumenti finanziari non quotati ed idonei ad alterarne sensibilmente il prezzo ovvero al fine di incidere sul pubblico affidamento in merito alla stabilità patrimoniale societaria.

- con riferimento al precedente punto 6:

- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni periodiche previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di vigilanza cui è soggetta l'attività aziendale, nonché omettere di dar corso con sollecitudine all'invio dei dati e della documentazione eventualmente richiesta dalle predette autorità;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, ovvero occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della società;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte dell'Autorità di vigilanza.

Si rinvia espressamente ai Protocolli speciali di prevenzione allegati al presente Modello di organizzazione, gestione e controllo.

3.8. I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della società.

I compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

- proporre che vengano costantemente redatte o aggiornate le eventuali procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;

- monitorare sul rispetto delle eventuali procedure interne per la prevenzione dei reati societari. L'Organismo di Vigilanza è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

3.9. Flussi informativi all'Organismo di vigilanza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace attuazione del Modello e di curarne l'aggiornamento dovranno essere assicurati i seguenti flussi informativi periodici:

Documenti	Periodicità	Soggetto tenuto
○ Schema di bilancio in via preventiva (come da Parte speciale 2. Reati commessi nei confronti della PA) ○ Bilancio CEE approvato e documentazione collegata (come da Parte speciale 2. Reati commessi nei confronti della PA) ○ Copia delibera approvazione bilancio di esercizio	Annuale	Responsabile amministrativo
○ Notifica di operazioni straordinarie con documentazione attestante (perizie, atti notarili, comunicazioni registro imprese)		Amministratore Unico Responsabile Amministrativo

Tutti i destinatari della presente Parte speciale sono altresì tenuti ad effettuare segnalazioni all'Organismo di vigilanza qualora rilevino eventuali non conformità relative all'applicazione del flusso; al rispetto di procedure/regolamenti; al rispetto delle disposizioni del Modello di organizzazione, gestione e controllo, del Codice etico e in generale del d. lgs. n. 231/2001 e smi.

PARTE SPECIALE

SEZIONE 4 - CORRUZIONE TRA PRIVATI

INDICE

4.1 Introduzione e funzione della parte speciale dedicata 3
4.2 Le fattispecie di reato richiamate dal D.Lgs 231/01 3
4.2.1 Corruzione tra privati ((art.2635 c.c. modificato dal D.Lgs. n .38 del 15 Marzo 2017) 3
4.2.2 Istigazione alla Corruzione tra privati (art.2635 bis c.c. introdotto dal D.Lgs. n .38 del 15 Marzo 2017) 4
4.2.3 Pene Accessorie (art. 2635 ter c.c. introdotto dal D.Lgs. n.38 del 15 Marzo 2017) 4
4.3 Le attività sensibili relative ai reati societari 5
4.4 Organi e funzioni aziendali coinvolte 6
4.5 Principi e regole di comportamento 7
4.6 Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili 8
4.7 I controlli dell'Organismo di Vigilanza 10
4.8 Flussi all'Organismo di Vigilanza 11

4.1. Introduzione e funzione della parte speciale

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Dipendenti e dagli Organi Societari dell'azienda, nonché dai suoi Collaboratori esterni e dai suoi Partner, come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale è che tutti i Destinatari, conducano comportamenti conformi a quanto ivi rescritto al fine di impedire il verificarsi degli illeciti di cui all'art. 25-ter del Decreto in relazione ai reati di corruzione tra privati come di seguito descritti.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- Indicare i principi procedurali e le regole di comportamento che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza - e ai responsabili delle funzioni aziendali che cooperano con tale organismo - gli strumenti esecutivi per esercitare le attività di controllo, di monitoraggio e di verifica.

La società adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione delle fattispecie delittuose di seguito descritte.

4.2. Le fattispecie di reato richiamate dal D.Lgs. 231/01

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D.Lgs. n. 231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

Di seguito si riporta una breve descrizione dei reati societari richiamati dall'art. 25-ter (Reati societari) del D.Lgs. 231/01 con specifico ed esclusivo riferimento ai reati di corruzione tra privati che si ritiene potrebbero trovare manifestazione nell'ambito delle attività svolte dall'azienda.

4.2.1. Corruzione tra privati (art. 2635 c.c.) modificato dal D.Lgs. n.38 del 15 Marzo 2017 e modificato dalla Legge n.3/2019

Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per se' o per altri, denaro o altra

utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, sono puniti con la reclusione da uno a tre anni.

Si applica la stessa pena se il fatto è commesso da chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse da quelle proprie dei soggetti di cui al precedente periodo.

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.

Chi, anche per interposta persona, offre, promette o dà denaro o altra utilità non dovuti alle persone indicate nel primo e nel secondo comma, è punito con le pene ivi previste.

Le pene stabilite sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Fermo quanto previsto dall'art. 2641, la misura della confisca per valore equivalente non può essere inferiore al valore delle utilità date, promesse o offerte.

4.2.2. Istigazione alla Corruzione tra privati (art. 2635 bis c.c.) introdotto dal D.Lgs. n.38 del 15 Marzo 2017 e modificato dalla Legge n. 3/2019

Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.

La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per se' o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata.

4.2.3. Pene Accessorie (art. 2635 ter c.c.) introdotto dal D.Lgs. n.38 del 15 Marzo 2017

La condanna per il reato di cui all'articolo 2635, primo comma, importa in ogni caso l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese di cui all'articolo 32-bis del codice penale nei confronti di chi sia già stato condannato per il medesimo reato o per quello di cui all'articolo 2635-bis, secondo comma.

4.3. Le attività sensibili relative ai reati di corruzione tra privati

L'art. 6, comma 2, lett. a) del D.Lgs. 231/01 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

Nell'ambito di ciascun reato, sulla base della mappatura di dettaglio delle aree aziendali a rischio, sono state individuate le attività da ritenersi maggiormente "sensibili" come di seguito riportato.

Principali Aree a rischio e attività sensibili interessate:

- **Gestione della Contabilità Generale:**
- **Imputazione delle scritture contabili** in contabilità generale
- **Verifiche sui dati contabili** immessi a sistema e quelli inviati al consulente esterno
- **Predisposizione di bilanci e documentazione di natura contabile**: si tratta delle attività relative alle chiusure contabili, alla contabilizzazione dei dati e alla predisposizione del bilancio d'esercizio della Società e dei relativi allegati
- **Rapporti con clienti e fornitori**
- **Selezione del Personale**
- **Rapporti con Banche/finanziarie/creditori**

Nel caso in cui esponenti della Società si trovino a dover gestire attività sensibili diverse da quelle sopra elencate, le stesse dovranno comunque essere condotte nel rispetto:

a) degli standard di controllo generali
b) dei principi di comportamento individuati nel Codice Etico
c) di quanto regolamentato dalla documentazione e dagli atti aziendali
d) delle disposizioni di legge

È responsabilità del legale rappresentante segnalare tempestivamente all'Organismo di Vigilanza eventuali modifiche/integrazioni da apportare alla Parte Speciale, in accordo a quanto previsto dalla Parte Generale

4.4. Organi e funzioni aziendali coinvolte

In relazione alle descritte Attività Sensibili, si ritengono particolarmente coinvolti i seguenti organi e funzioni aziendali:

Amministratore Unico
I profili di rischio attengono alle funzioni di controllo sulle Aree Sensibili, nonché le attività relative alla gestione dei valori svolte sia per conto della società sia per conto della clientela.

CFO
L'attività di questa funzione si considera a rischio per la gestione dei rapporti con Istituti di credito, assicurativi, fornitori diversi e clienti.

Incaricati Acquisti
L'attività di questa funzione si considera a rischio per la gestione dei rapporti con i Fornitori della Società.

Area Commerciale
L'attività di queste funzioni si considera a rischio per la gestione dei rapporti con i Clienti della Società.

Ufficio Amministrativo
L'attività di questa funzione si considera a rischio per la gestione della corretta rappresentazione dei risultati economici, degli adempimenti fiscali ed i rapporti con le Autorità di Vigilanza.

Ufficio Risorse Umane
L'attività di questa funzione si considera a rischio per la gestione delle assunzioni del personale.

All'interno del ciclo attivo, il reato di corruzione tra privati potrebbe essere commesso da parte di Amministratori (apicali) e/o di Responsabili della Funzione interessata (sottoposti), nonché da sottoposti alla direzione e alla vigilanza di tali soggetti (sottoposti):
i) nella vendita di beni ad altra società, con lo scopo di ottenere dal cliente la conclusione di un contratto;
ii) nell'esecuzione di prestazioni di servizi ad altra società, al fine di corrompere un concorrente durante la partecipazione a una "gara privata" affinché lo stesso presenti condizioni peggiori.

Nel ciclo passivo, invece, il reato di corruzione potrebbe essere integrato nei confronti dei fornitori della Società per ottenere beni/servizi a migliori condizioni e/o a prezzi più favorevoli.

Per quanto riguarda, invece, la gestione del processo di selezione del personale, la corruzione potrebbe essere commessa mediante l'assunzione da parte della Società di persone a conoscenza di segreti industriali di Società concorrenti al fine di ottenere la rivelazione di tali segreti.

Con riferimento, infine, al rapporto con gli Istituti di Credito/Finanziari o Creditori, il reato potrebbe essere commesso, da un lato, nei rapporti con le banche, mediante la corruzione di funzionari per ottenere benefici economici, dall'altro, nei rapporti con le finanziarie, tramite la corruzione di un dipendente al fine di evitare che la Società sia segnalata alla U.I.F.

Da ultimo, il reato di corruzione potrebbe integrarsi nei rapporti con i creditori con lo scopo di concludere transazioni più vantaggiose per la Società ovvero al fine di ritardare l'azione esecutiva.

L'analisi del rischio della commissione dei reati di cui alla presente Sezione in relazione alle aree ed attività sensibili sopra indicate e mappate riscontra un livello di rischio BASSO in considerazione della segregazione delle funzioni che assicura un controllo costante dei processi interessati e delle procedure osservate nella gestione di rapporti con enti o soggetti privati.

4.5. Principi e regole 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 normativa interna aziendale relativa al sistema amministrativo, finanziario e contabile nonché relativa al Codice Etico.

I destinatari, inoltre, sono tenuti ad operare sulla base della best practice cui l'azienda si ispira nell'esercizio delle proprie funzioni, sul fondamento che qualsiasi condotta attiva od omissiva posta in essere in violazione diretta od indiretta dei principi normativi e delle regole procedurali interne che attengono alla formazione della documentazione contabile ed alla rappresentazione esterna, così come all'esercizio delle attività di controllo e di vigilanza è da considerare come commessa in danno della azienda stessa.

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, le politiche e le procedure aziendali nonché le regole contenute nel Modello 231 e nella presente parte speciale operando, in questo modo, in coerenza con i valori e i principi che sono alla base dell'attività d'impresa in azienda.

In generale, il sistema di organizzazione, gestione e controllo della società rispetta i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, i procuratori aziendali nonché gli agenti, i collaboratori e le controparti contrattuali che operano in nome e per conto della Società, devono conoscere e rispettare:

- La normativa italiana e straniera applicabile alle attività svolte
- Il Codice Etico Aziendale
- Il presente Modello 231
- Le procedure e le linee guida aziendali nonché tutta la documentazione attinente il sistema di organizzazione, gestione e controllo della società.

4.6 Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Preliminarmente, si evidenzia da un lato che il Modello della Società ha una sezione dedicata ai rapporti con la P.A. (al cui interno hanno un ruolo preminente i reati di corruzione), dall'altro che la Società adotta e persegue politiche aziendali finalizzate alla prevenzione dei reati di corruzione espresse nel Codice Etico vigente.

Inoltre, taluni principi di comportamento richiamati nelle Sezioni 2 e 3 della Parte speciale del presente Modello sono, altresì, idonei a minimizzare il rischio di reato oggetto della presente sezione: la procedura di selezione del personale, la gestione degli omaggi, la procedura di gestione della tesoreria e la formalizzazione di un sistema di deleghe e procure per la gestione dei rapporti con le banche (per citare le principali).

Al fine, poi, di garantire il più possibile la prevenzione del compimento da parte dei Destinatari del Modello di azioni che possono concretizzare la fattispecie contemplata nella presente Parte Speciale, la Società deve adottare e predisporre una serie di principi generali di comportamento, fermo restando il rigoroso rispetto del Modello, del Codice Etico e delle procedure sopra "suggerite".

In particolare, ai destinatari è fatto divieto di:

- ricevere, pretendere, corrispondere e offrire direttamente o indirettamente, compensi di qualunque natura, regali, vantaggi economici o altra utilità da, o a, un soggetto privato e/o l'ente da esso direttamente o indirettamente rappresentato che: i) eccedano un modico valore e il limiti di ragionevoli prassi di cortesia e, comunque, ii) siano suscettibili di essere interpretati come volti a influenzare indebitamente i rapporti tra la Società e il predetto soggetto e/o l'ente da esso direttamente o indirettamente rappresentato, a prescindere dalla finalità di perseguimento, anche esclusivo, dell'interesse o del vantaggio della Società;

- corrispondere “facilitation payments”, ovvero i pagamenti di modico valore non ufficiali, effettuati allo scopo di velocizzare, favorire o assicurare l’effettuazione di un’attività di routine o comunque prevista nell’ambito dei doveri dei soggetti privati con cui la Società si relaziona;

- utilizzare fondi o mezzi personali allo scopo di aggirare l’applicazione dei contenuti della Presente Parte Speciale.

Inoltre, ogni attività svolta nelle aree sensibili sopra indicate, deve essere accuratamente e regolarmente riflessa nei documenti contabili.

È, infatti, responsabilità della Società di redigere documenti contabili che riflettano con un dettaglio ragionevole ciascuna operazione, nonché stabilire e eseguire controlli adeguati al fine di garantire che:

- le operazioni siano effettive ed eseguite solo a fronte di un’autorizzazione del management;
- le operazioni siano registrate al fine di permettere la redazione del bilancio in conformità con i principi contabili di riferimento;
- il valore dei beni inserito a bilancio sia riscontrato, con una certa periodicità, con gli inventari e siano adottate appropriate misure in riferimento alle differenze riscontrate.

Nessuna pratica qualificabile come di natura corruttiva, inclusi i facilitation payments, può essere giustificata o tollerata per il fatto che essa è “consuetudinaria” nel settore di business o nel Paese nel quale l’attività è svolta.

Non è consentito imporre o accettare alcuna prestazione ove la stessa possa essere realizzata, solamente, pregiudicando i valori ed i principi del Codice Etico o violando le procedure del Modello applicabili e le normative.

Inoltre, gli Organi Sociali, l’Amministratore, i dipendenti ed i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, dovranno tener conto, oltre a quanto precedentemente definito delle procedure e regole aziendali che prevedono:

- il rispetto del Codice Etico e delle sue specifiche previsioni riguardanti il corretto comportamento di tutti i soggetti coinvolti nelle attività di formazione del bilancio o di altri documenti similari, quali ad esempio:
  a) Massima collaborazione, veridicità, autenticità ed originalità della documentazione e delle informazioni trattate
  b) Chiarezza e correttezza della rappresentazione patrimoniale e finanziaria della società
  c) Completezza, segnalazione di eventuali omissioni, manomissioni, falsificazioni o trascuratezza della contabilità o della documentazione di supporto sulla quale le

registrazioni contabili si fondano, etc.,

- il rispetto del calendario di chiusura, finalizzato alla redazione del bilancio indicante:
  a) Data di chiusura dei periodi contabili
  b) Data di chiusura delle scritture contabili
  c) Data di predisposizione della Bozza del Bilancio e del Bilancio Definitivo

- la chiara definizione della responsabilità della veridicità, autenticità ed originalità della documentazione e delle informazioni e dei dati forniti dal Responsabile della determinazione delle varie poste/fondi;
- il supporto documentale a corredo delle informazioni e dei dati forniti dal Responsabile di cui al punto precedente;
- la tracciabilità informatica delle operazioni effettuate;
- la tracciabilità informatica degli scambi tra gli interlocutori delle operazioni di acquisto/vendita.

Si rinvia espressamente ai Protocolli speciali di prevenzione allegati al presente Modello di organizzazione, gestione e controllo.

4.7. I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della società.

L'Organismo di Vigilanza dovrà avere evidenza e mantenere traccia:
- di quanto posto in essere nella società al fine di fornire opportune indicazioni per la corretta redazione del bilancio;
- per quanto concerne il conferimento di eventuali incarichi da parte dell'OdV, lo stesso dovrà mantenere agli atti evidenza delle valutazioni circa le proposte, gli ambiti e le scelte effettuate da sottoporre all'Amministratore Unico degli incarichi conferiti.

L'Organismo di Vigilanza dovrà, inoltre, esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni.

Inoltre, i compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

- proporre che vengano costantemente redatte e aggiornate le eventuali procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;
- monitorare sul rispetto delle eventuali procedure interne per la prevenzione dei reati societari.
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.
L'Organismo di Vigilanza è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti

4.8. Flussi informativi all'Organismo di vigilanza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace attuazione del Modello e di curarne l'aggiornamento dovranno essere assicurati i seguenti flussi informativi periodici:

Documenti	Periodicità	Soggetto tenuto
Ad integrazione dei flussi informativi richiesti nella Sezione 2 (Reati PA): o verbali degli enti privati certificatori o nuovi accordi di partenariato/accordi commerciali quadro	Al verificarsi della condizione	Amministratore Unico Responsabile Qualità

Tutti i destinatari della presente Sezione della Parte speciale sono altresì tenuti ad effettuare segnalazioni all'Organismo di vigilanza qualora rilevino eventuali non conformità relative all'applicazione del flusso; al rispetto di procedure/regolamenti; al rispetto delle disposizioni del Modello di organizzazione, gestione e controllo, del Codice etico e in generale del d. lgs. n. 231/2001 e smi.

PARTE SPECIALE

SEZIONE 5 - REATI INFORMATICI E DI TRATTAMENTO ILLECITO DEI DATI

INDICE

5.1	Introduzione e funzione della parte speciale dei reati informatici e di trattamento illecito dei dati	3
5.2	Criteri per la definizione dei reati informatici e di trattamento illecito dei dati	3
5.3	Le fattispecie di reato richiamate dal D.Lgs. 231/2001	4
5.3.1	Falsità in documenti informatici (art. 491-bis c.p. modificato da D.lgs 7 del 15 gennaio 2016)	5
5.3.2	Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p. mod. Legge n. 90/2024	5
5.3.3	Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p. mod. Legge n. 238/2021 e Legge n. 90/2024)	6
5.3.4	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p. mod. Legge n. 238/2021 e Legge n. 90/2024)	8
5.3.5	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p. mod. Legge n. 238/2021 e Legge n. 90/2024)	9
5.3.6	Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p. mod. da D.lgs 7 del 15 gennaio 2016 e Legge n. 90/2024	9
5.3.7	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p. mod. da D.lgs 7 del 15 gennaio 2016 e Legge n. 90/2024	10
5.3.8	Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p. mod. da D.lgs 7 del 15 gennaio 2016 e Legge n. 90/2024)	10
5.3.9	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.) [articolo introdotto dalla Legge n. 90/2024]	11
5.3.10	Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p. mod. da D.lgs 7 del 15 gennaio 2016 e Legge n. 90/2024	11
5.3.11	Frode informatica (art. 640-ter c.p.)	12
5.3.12	Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art.640-quinquies c.p.)	13
5.3.13	Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)	13
5.3.14	Estorsione (art. 629, comma 3, c.p. aggiunto dalla Legge n. 90/2024)	14
5.4	Le attività sensibili relative ai reati informatici e di trattamento illecito di dati	14
5.5	Organi e funzioni aziendali coinvolte	15
5.6	Principi e norme generali di comportamento	16
5.7	Principi di riferimento specifici alla regolamentazione delle attività sensibili	17
5.8	I controlli dell'Organismo di Vigilanza	20
5.9	Flussi informativi all'Organismo di Vigilanza	20

5.1. Introduzione e funzione della parte speciale dei reati informatici e di trattamento illecito dei dati

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Dipendenti e dagli Organi Sociali aziendali, nonché dai suoi Collaboratori esterni e dai Partner come già definiti nella Parte Generale.

Obiettivo della presente Parte Speciale e che tutti i Dipendenti e gli altri soggetti eventualmente autorizzati adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di impedire il verificarsi degli illeciti in essa considerati.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- Indicare i principi procedurali e le regole di comportamento che i Dipendenti e gli altri soggetti eventualmente autorizzati sono chiamati ad osservare ai fini della corretta applicazione del Modello.

- Fornire all'Organismo di Vigilanza, nonché ai responsabili delle altre funzioni aziendali che cooperano con lo stesso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

La società adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione dei reati di seguito descritti.

5.2. Criteri per la definizione dei reati informatici e di trattamento illecito dei dati

Ad integrazione delle definizioni elencate nella Parte Generale del Modello, si consideri la seguente ulteriore definizione da applicare alla presente Parte Speciale:

"**Delitti Informatici**": sono i delitti richiamati dall'art. 24-bis del Decreto e disciplinati dal codice penale agli artt. 491-bis, 615-ter, 615-quater, 615-quinquies, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies e 640-quinquies, art. 629, comma 3, c.p e art. 1, comma 11, D.L. 21 settembre 2019, n. 105.

5.3. Le fattispecie di reato richiamate dal D.Lgs. 231/01

La legge 18 marzo 2008, n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento intero" ha ampliato le fattispecie di reato che possono generare la responsabilità delle società. L'art. 7 del predetto provvedimento ha introdotto nel D. lgs. n. 231/2001 l'art. 24 - bis "Delitti informatici e trattamento illecito di dati", che riconduce la responsabilità amministrativa degli enti ai reati individuati nelle sezioni seguenti.

La Legge n. 238 del 23 dicembre 2021 (c.d. Legge Europea) – entrata in vigore in data 1° febbraio 2022 – recante disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea, ha apportato – tra le altre – alcune modifiche alla disciplina di alcuni reati informatici richiamati dall'art. 24-bis del D.Lgs. 231/2001, di alcuni dei delitti contro la personalità individuale ex 25-quinquies D.Lgs. 231/2001 (estensione della condotta del reato di detenzione di materiale pornografico anche all' accesso intenzionale; introduzione di aggravanti specifiche al reato di adescamento di minorenni) e la modifica dei reati di market abuse richiamati dall' 25-sexies D.Lgs. 231/2001.

La legge n. 90/2024 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e dei reati informatici", adottata allo scopo di rafforzare il sistema di cybersicurezza nazionale e prevenire nonché contrastare la commissione di reati informatici, è intervenuta con la previsione di una serie di disposizioni orientate a garantire una migliore capacità di protezione dagli attacchi informatici e a fornire una risposta efficiente dinnanzi a queste emergenze nonché con un inasprimento del sistema sanzionatorio.

Il primo Capo della legge prevede, fra l'altro, l'introduzione di obblighi di segnalazione di alcuni tipi di incidenti informatici che abbiano impatto su reti, sistemi informativi e servizi informatici.

Il secondo Capo, che racchiude gli articoli dal 16 al 24, contiene le "Disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari". In tale sezione trovano spazio tutte le modifiche che la Legge ha inteso apportare tanto al Codice Penale, quanto al Codice di Procedura Penale e al D.Lgs. n. 231/2001, al fine di fronteggiare la commissione dei reati informatici.

Si descrivono qui di seguito le singole fattispecie di reato per le quali l'art. 24-bis del D.Lgs. n. 231/2001 prevede una responsabilità degli enti nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi.

5.3.1. Falsità in documenti informatici (art. 491-bis c.p. modificato da D.lgs 7 del 15 gennaio 2016)

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, co. 1, lett. p), D.Lgs. 82/2005, salvo modifiche ed integrazioni).

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli.

Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato.

A tal proposito il D.Lgs 7 del 15 gennaio 2016 aggiunge: "*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici".*

5.3.2. Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p. mod. Legge n. 90/2024)

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". Tale delitto è punito con la reclusione fino a tre anni.
La pena è della reclusione da uno a cinque anni:

- 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.

5.3.3. Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p. mod. Legge n. 238/2021 e Legge n. 90/2024)

Tale reato si realizza quando un soggetto, "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 pena è della reclusione sino a due anni e con la multa sino a euro 5.164.

La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615 ter, secondo comma, numero 1) ossia 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.

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma ossia sistemi di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'art. 615-quater, pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.
I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (ad esempio, badge, carte di credito, bancomat e smart card).

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio, policy Internet).

L'art. 615-quater, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente di un'azienda autorizzato ad un certo livello di accesso al sistema informatico che ottenga illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno dell'azienda oppure carpisca in altro modo fraudolento o ingannevole il codice di accesso.

5.3.4. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p. mod. Legge n. 238/2021 e Legge n. 90/2024)

Tale ipotesi di reato si integra qualora un soggetto "fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni", nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico. Tale reato è punito con la reclusione da sei mesi a quattro anni.

La pena è della reclusione da uno a cinque anni:

- 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.

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

La fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato si integra, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente.

5.3.5. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p. mod. Legge n. 238/2021 e Legge n. 90/2024)

Questa fattispecie di reato si realizza quando qualcuno, "fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi". Tale reato è punito con la reclusione da uno a quattro anni.

La condotta vietata dall'art. 617-quinquies è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate. 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.

Il reato si integra, ad esempio, a vantaggio dell'ente, nel caso in cui un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato (se privo delle necessarie autorizzazioni) si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche.

5.3.6. Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p. mod. da D.lgs 7 del 15 gennaio 2016 e Legge n. 90/2024)

Tale fattispecie reato si realizza quando un soggetto "distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui". Tale reato è punito con la reclusione da sei mesi a tre anni.

Il D.Lgs 7 del 15 gennaio 2016 recita: *"Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità' di operatore del sistema, la pena è della reclusione da uno a quattro anni."*

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.

5.3.7. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p. mod. da D.lgs 7 del 15 gennaio 2016 e Legge n. 90/2024

Tale reato si realizza quando un soggetto "commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità". Tale reato è punito con la reclusione da uno a quattro anni.

La sanzione è da tre a otto anni se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

Il Dlgs 7 del 15 gennaio 2016 recita: "*la pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di 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 sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato.

5.3.8. Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p. mod. da D.lgs 7 del 15 gennaio 2016 e Legge n. 90/2024)

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". Tale reato è punito con la reclusione da uno a cinque anni.

Il Dlgs 7 del 15 gennaio 2016 recita: "*la pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema*".

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.

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).

5.3.9. 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.) [articolo introdotto dalla Legge n. 90/2024]

L'art. 16, co. 1, lett. q), legge n. 90 del 2024 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e dei reati informatici" introduce una ulteriore fattispecie criminosa, vale a dire il delitto di detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

Il novellato art. 635-quater.1 c.p. in particolare punisce chiunque, 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, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici.

Le pene previste sono la reclusione fino a due anni e la multa fino a euro 10.329. La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1). La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma.

5.3.10. Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p. mod. da D.lgs 7 del 15 gennaio 2016 e Legge n. 90/2024

Questo reato si configura quando "il fatto di cui all'art. 635-quater (Danneggiamento di sistemi informatici o telematici) è diretto a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento".

Tale reato è punito con la pena della reclusione da uno a quattro anni.

La sanzione è della reclusione da tre a otto anni se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se lo stesso è reso, in tutto o in parte, inservibile.

Il Dlgs 7 del 15 gennaio 2016 recita: "*la pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema*".

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (art. 635-ter), quel che rileva è che il sistema sia utilizzato per il perseguimento di pubblica utilità 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.

5.3.11. Frode informatica (art.640-ter c.p.)

Questo reato si configura quando chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

La pena prevista è la reclusione da sei mesi a tre anni e la multa da € 51 a €1.032.

La pena va da uno a cinque anni e la multa da €309 a €1.549 se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Se poi il fatto è commesso con furto e indebito utilizzo in danno di qualcuno la reclusione va da due a sei anni e la multa da €600 a € 3.000.

Il delitto è punibile a querela della persona offesa, salvo che ricorra un'altra circostanza aggravante.

5.3.12. 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". Tale reato è punito con la reclusione fino a tre anni e con la multa da Euro 51 a Euro 1.032.

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

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

Con il decreto-legge n. 105 del 2019, convertito nella legge n. 133 dello stesso anno – è stato definito il Perimetro di sicurezza cibernetica nazionale al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale o la fornitura di un servizio essenziale per lo Stato e dal cui malfunzionamento, interruzione, anche parziali o utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale.

Come indicato nel DPCM 31 luglio 2020, n. 131, i soggetti pubblici e privati - che forniscono tali servizi o esercitano tali funzioni - sono stati individuati sulla base di specifici criteri e nell'ambito di diversi settori strategici– interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche, enti previdenziali/lavoro – dalle Amministrazioni competenti nei rispettivi settori.

I soggetti inclusi nel perimetro di sicurezza cibernetica sono tenuti a predisporre annualmente l'elenco degli asset ritenuti "strategici" per la fornitura dei servizi essenziali e funzioni essenziali di rispettiva pertinenza e, con riferimento a tali asset, ad adottare misure nell'ottica di assicurare elevati livelli di sicurezza e a notificare eventuali incidenti al CSIRT (Computer Security Incident Response Team) attivo presso l'ACN. Le misure di sicurezza, che i soggetti inclusi nel Perimetro sono tenuti ad adottare, e le modalità di notifica degli incidenti sono state definite con il DPCM 14 aprile 2021, n. 81.
Inoltre, i soggetti inclusi nel perimetro, ai sensi dell'articolo 1, comma 6, del decreto legge n. 105/2019 – attuato con il Decreto del Presidente della Repubblica 5 febbraio 2021, n. 54 - sono tenuti a comunicare al Centro di Valutazione e Certificazione Nazionale (CVCN) – l'intenzione di acquisire beni, sistemi e servizi ICT da impiegare sui propri asset "strategici" e appartenenti a determinate categorie di cui al DPCM 15 giugno 2021.
Il comma 11 bis della legge prevede che la violazione degli obblighi di informazione e la trasmissione

di informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi o ai fini delle comunicazioni previste o per lo svolgimento delle attività ispettive e di vigilanza è punito con la reclusione da uno a tre anni.

Il reato viene contestualmente inserito nell'elenco dei reati presupposto ai sensi del d. lgs. n. 231/2001 e smi.

5.3.14. Estorsione (art. 629, comma 3, c.p.) [articolo aggiunto dalla Legge n. 90/2024]

La norma, introdotta dalla Legge n. 90/2024 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e dei reati informatici", punisce con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000 chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità.

La norma introduce la nuova fattispecie criminosa dell'estorsione informatica sanzionandola più aspramente dell'estorsione semplice. Il legislatore ha ritenuto opportuno prevedere un'autonoma fattispecie di reato per gli attacchi c.d. ransomware ovverosia per quelle condotte volte a cifrare illecitamente i dati di terzi e a chiedere il pagamento di una somma per la decifratura degli stessi.

5.4. Le attività sensibili relative ai reati informatici

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal Decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

L'analisi dei processi ha consentito di individuare le seguenti "attività sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24 - bis del d.lgs. 231/2001:

a. Gestione dei profili utente e del processo di autenticazione
b. Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio
c. Gestione e protezione degli strumenti informatici
d. Gestione degli accessi da e verso l'esterno

e. Gestione e protezione delle reti
f. Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD, hard disk,…)
g. Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.)

I delitti trovano come presupposto 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).

L'analisi del rischio della commissione dei reati di cui alla presente Sezione in relazione alle aree ed attività sensibili sopra indicate e mappate riscontra un livello di rischio BASSO in considerazione dei sistemi di IT security adottati, delle procedure in essere costantemente attuate e verificate e della segregazione delle funzioni che assicura un puntuale controllo dei processi e la rilevazione di eventuali errori o anomalie.

5.5. Organi e funzioni aziendali coinvolte

In relazione alle descritte Attività Sensibili – tutte astrattamente ipotizzabili – si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali

- **Responsabile Informatico**
  In relazione alle Attività Sensibili questa funzione è coinvolta per la gestione e la corretta dotazione di strumenti informatici ai dipendenti ed il controllo su tutto il sistema informatico aziendale

- **Amministratore Unico**
  I profili di rischio attengono alle funzioni di controllo sulle Aree Sensibili

- **Responsabile risorse umane**
  In relazione ad Attività Sensibili di cui sopra questa funzione è coinvolta per i rapporti che intrattiene con tutti gli esponenti aziendali e con la formazione, informazione in merito all'utilizzo dei sistemi informatici della società
- **Amministratore di Sistema**
  Figura esterna nominata da Amministratore Unico per materie di sicurezza informatica

5.6. Principi e norme generali di comportamento

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella presente parte speciale del Modello.

In generale, il sistema di organizzazione, gestione e controllo della società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli Amministratori, gli Organi Sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, devono conoscere e rispettare:

1. gli standard generali di controllo
2. i principi di comportamento individuati nel Codice Etico
3. quanto regolamentato dalla documentazione e dagli atti aziendali
4. le disposizioni di legge

Ciò posto al fine di perseguire la prevenzione dei Reati Informatici è fatto espresso divieto a tutti i Soggetti coinvolti di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 24-bis del D. Lgs. 231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi ivi richiamati.

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:

- Previsione nel Codice Etico di specifiche indicazioni volte a impedire la commissione dei reati informatici sia all'interno della società che tramite apparecchiature non soggette al controllo della stessa
- 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

Conseguentemente, gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nello svolgimento delle attività a rischio hanno l'espresso obbligo di perseguire i seguenti principi generali di controllo:

- **Esistenza di procedure:** devono esistere disposizioni aziendali, regolamenti o procedure formalizzate idonee a fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili

- **Gestione delle segnalazioni:** raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio per i reati informatici rilevati da soggetti interni e esterni all'ente

- **Riporto all'OdV:** riferire prontamente all'OdV eventuali situazioni di irregolarità

5.8. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, ecc.), gli Organi Sociali, gli Amministratori, i dipendenti ed i procuratori nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nello svolgimento delle attività a rischio sono tenuti, al fine di prevenire e impedire il verificarsi dei reati di cui all'art. 24-bis del D.Lgs. 231/01, al rispetto delle regole e procedure aziendali emesse a regolamentazione di tale attività a rischio.

Tali regole e procedure prevedono controlli specifici e concreti a mitigazione dei fattori di rischio caratteristici di tale area quali:

- Utilizzo degli strumenti informatici
- Gestione e assegnazione delle credenziali di autenticazione/password
- Utilizzo della rete aziendale e della rete internet
- Utilizzo della posta elettronica
- Software e applicazioni presenti sugli strumenti aziendali
- Documento di attestazione presenza di sistemi di protezione antivirus e antispam
- Esistenza di una serie di procedure, in materia di "privacy" che disciplinano gli aspetti legati al corretto utilizzo delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni
- Attuazione del progetto di formazione, volta a sensibilizzare tutti gli utenti e/o particolari figure professionali, con l'obiettivo di diffondere all'interno della società le politiche, gli obiettivi e i piani previsti in materia di sicurezza informatica e al fine di soddisfare i requisiti previsti in materia di privacy
- Consegna a ciascun dipendente della Società, contestualmente all'assegnazione del pc e/o dell'indirizzo di posta elettronica di eventuali regolamenti o procedure interne per l'utilizzo degli strumenti informatici
- Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che costituiscono il patrimonio dell'azienda oggetto di protezione (es. controllo degli accessi, videosorveglianza)
- Attuazione di un sistema che prevede il tracciamento periodico delle operazioni che possono influenzare la sicurezza dei dati critici (registrazione dei log on e log off).

Principi procedurali specifici

In particolare, si elencano qui di seguito le regole che devono essere rispettate dalla società e dai dipendenti e dagli altri soggetti eventualmente 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;
- 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;
- è obbligatorio segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

L'azienda si impegna a attuare i seguenti adempimenti:

- informare adeguatamente i dipendenti e gli altri soggetti eventualmente autorizzati

dell'importanza di mantenere i propri codici di accesso (username e password) confidenziali e di non divulgare gli stessi a soggetti terzi;
- informare i dipendenti e agli altri soggetti eventualmente autorizzati della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccare l'accesso al pc "lock computer", qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;
- fornire un accesso da e verso l'esterno (connessione alla rete Internet) esclusivamente ai sistemi informatici dei dipendenti o di eventuali soggetti terzi che ne abbiano la necessità ai fini lavorativi o connessi all'amministrazione societaria;
- limitare gli accessi alla stanza server unicamente al personale autorizzato;
- proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;
- fornire ogni sistema informatico di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
- prevedere la possibilità di limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e file);
- qualora per la connessione alla rete Internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna WiFi), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni all'azienda, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti;
- prevedere un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti e degli altri soggetti eventualmente autorizzati con scadenza della password ogni 3 mesi;
- limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei dipendenti e degli altri soggetti eventualmente autorizzati (i.e. connessione tramite VPN).

Si richiamano espressamente e integralmente le prescrizioni e le procedure specifiche previste nei seguenti documenti aziendali:

- Regolamento Strumenti Informatici collaboratori - 01/02/2024;
- Regolamento aziendale per l'utilizzo degli strumenti informatici - 01/02/2024.

5.9. I controlli dell'Organismo di vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della società.

I compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

- proporre che vengano costantemente redatte o aggiornate le eventuali procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;
- monitorare sul rispetto delle eventuali procedure interne per la prevenzione dei reati societari. L'Organismo di Vigilanza è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

5.10. Flussi informativi all'Organismo di vigilanza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace attuazione del Modello e di curarne l'aggiornamento dovranno essere assicurati i seguenti flussi informativi periodici:

Documenti	Periodicità	Soggetto tenuto
○ report sull'attuazione dei regolamenti aziendali ○ report verifiche hardware, software e reti ○ acquisto e implementazione di nuovi software, database, programmi ○ report di anomalie rilevanti dei sistemi informatici riscontrata ○ denunce alle autorità competenti a fronte di violazioni della security.	Annuale Semestrale Al verificarsi della condizione	Responsabile IT

Tutti i destinatari della presente Parte speciale sono altresì tenuti ad effettuare segnalazioni all'Organismo di vigilanza qualora rilevino eventuali non conformità relative all'applicazione del flusso; al rispetto di procedure/regolamenti; al rispetto delle disposizioni del Modello di organizzazione, gestione e controllo, del Codice etico e in generale del d. lgs. n. 231/2001 e smi.

PARTE SPECIALE

SEZIONE 6 - REATI AMBIENTALI

INDICE

6.1	Introduzione e funzione della parte speciale dei reati ambientali	3
6.2	Criteri per la definizione dei reati ambientali	3
6.3	Le fattispecie di reato richiamate dal D.Lgs. 231/2001	4
6.3.1	Inquinamento ambientale - (Art 452 bis c.p. inserito da L. N 68 del 22 maggio 2015 e modificato dalla L. n. 137/2023	4
6.3.2	Disastro ambientale- (Art 452 quater c.p. inserito da L. N 68 del 22 maggio 2015 e modificato dalla L. n. 137/2023)	4
6.3.3	Delitti colposi contro l'ambiente- (Art 452 quinquies c.p. inserito da L. N 68 del 22 maggio 2015, mod. L. n. 137/2023)	5
6.3.4	Traffico e abbandono di materiale ad alta radioattività- (Art 452 sexies c.p. inserito da L. N 68 del 22 maggio 2015)	5
6.3.5	Circostanze aggravanti- (Art 452 octies c.p. inserito da L. N 68 del 22 maggio 2015)	6
6.3.6	Attività' organizzate per il traffico illecito di rifiuti (Art 452 quaterdecies c.p. inserito da D.lgs 21 del 1marzo 2018 in sostituzione dell'art.260 del D.Lgs 152/2006).	6
6.3.7	Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette – (Art. 727 bis c.p.)	7
6.3.8	Distruzione o deterioramento di habitat all'interno di un sito protetto – (Art. 733 bis c.p).	7
6.3.9	Commercio internazionale delle specie di flora e di fauna selvatiche – (Artt. 1, 2,3bis e 6 L. n. 150/1992)	7
6.3.10	Scarichi di acque reflue Sanzioni penali – (Art. 137 D. Lgs. n. 152/2006 modificato da D.Lgs n.46/2014)	8
6.3.11	Attività di gestione di rifiuti non autorizzata- (Art.256 D. Lgs. n. 152/2006 modificato da D.Lgs n.46/2014)	9
6.3.12	Bonifica dei siti – (Art.257 D. Lgs. n. 152/2006)	9
6.3.13	Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari- (Art.258 D.Lgs. n. 152/2006 modificato dall'art. 35, D.gs del 3 dicembre 2010, n. 205).	10
6.3.14	Traffico illecito di rifiuti – (Art. 259 D. Lgs. n. 152/2006)	11
6.3.15	Sistema informatico di controllo della tracciabilità dei rifiuti – (Art.260 bis D.Lgs. n. 152/2006 modificato dall'art. 36, Decreto legislativo del 3 dicembre 2010, n. 205 e dal D.Lgs del 7 luglio 2011, n. 121)	11
6.3.16	Sanzioni per superamento valori limite di emissione-(Art. 279 D. Lgs. n. 152/2006 modificato da D.Lgs n.46/2014)	13
6.3.17	Inquinamento doloso provocato da navi – (Art. 8 D. Lgs. n. 202/2007)	13
6.3.18	Inquinamento colposo provocato da navi – (Art. 9 D. Lgs. n. 202/2007)	14
6.3.19	Cessazione e riduzione dell'impiego delle sostanze lesive – (Art.3 Legge n. 549/1993)	14
6.4	Le attività sensibili relative ai reati ambientali	16
6.5	Organi e funzioni aziendali coinvolte	17
6.6	Principi e regole di comportamento	17
6.7	Principi e norme generali di comportamento	18
6.8	Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili	19
6.9	Controlli dell'Organismo di Vigilanza	19
6.10	Flussi informativi all'Organismo di vigilanza	20

6.1. Introduzione e funzione della parte speciale dei reati ambientali

La presente Parte Speciale si riferisce ai reati previsti dal D. Lgs. 121/2011 (di seguito anche "Reati ambientali") richiamati dall'Art. 25-undecies del d. lgs. n. 231/2001 e s.m.i. ed illustra i comportamenti che devono essere tenuti dai soggetti che operano nelle relative aree a rischio reato al fine di prevenire la consumazione dei reati presupposto della responsabilità amministrativa degli enti.

Nello specifico, la presente Parte Speciale ha lo scopo di:

- Indicare i principi procedurali e le regole di comportamento che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- Fornire all'Organismo di Vigilanza e ai Responsabili delle altre funzioni della società, che cooperano con tale organismo, gli strumenti esecutivi necessari affinché gli stessi possano esercitare le attività di controllo, monitoraggio e verifica.

La società adotta, in applicazione dei principi e delle regole di comportamento contenute nella presente Parte Speciale, le procedure interne ed i presidi organizzativi atti alla prevenzione dei reati di seguito descritti.

6.2. Criteri per la definizione dei reati ambientali

Si definisce reato ambientale 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.

Con la legge 22 maggio 2015, n. 68, recante "Disposizioni in materia di delitti contro l'ambiente" vengono introdotte nell'ordinamento fattispecie di aggressione all'ambiente costituite sotto forma di delitto. La legge è stata successivamente modificata dalla L. n. 137/2023.

Una innovazione attesa da lungo tempo, nel corso del quale la risposta sanzionatoria a fenomeni criminali di massiccio, quando non irreparabile, inquinamento dell'ecosistema è stata affidata all'utilizzo – sovente discusso e comunque non privo di criticità sia sul piano sostanziale che sotto l'aspetto processuale/probatorio – del cd. disastro "innominato".

Proprio in funzione della necessità di uscire dalle difficoltà interpretative ed applicative di una norma indiscutibilmente legata ad altri contesti di "disastro", più immediatamente percepibili sul piano fenomenico, e allo stesso tempo volendo chiudere il cerchio del catalogo sanzionatorio presidiando penalmente ogni livello di alterazione peggiorativa delle matrici ambientali, il legislatore ha dunque introdotto nel codice penale due nuove figure delittuose (inquinamento ambientale e

disastro ambientale), accompagnandole con altre previsioni incriminatrici giudicate necessarie per la tenuta complessiva del sistema e con ulteriori interventi di raccordo con il Codice dell'Ambiente e con la disciplina della responsabilità degli enti.

6.3. Le fattispecie di reato richiamate dal D.Lgs. 231/01

Di seguito, l'elenco dei reati contemplati dall'Art. 25-undecies (di seguito, anche "Reati ambientali") del Decreto e il testo delle relative disposizioni.

6.3.1. Inquinamento ambientale- Art 452 bis c.p.

Questo reato introdotto dall'articolo 1, comma 1 della legge n.68 del 22 maggio 2015 successivamente modificato dalla L. n. 137/2023 si verifica allorché abusivamente si cagiona un inquinamento (deterioramento o una 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, storico, artistico, o in danno di specie di animali o vegetali protette, la pena viene aumentata.

Esempio
Le aziende, specie quelle abusive, per risparmiare sui costi di smaltimento sotterrano o bruciano gli scarti di lavorazione

6.3.2. Disastro ambientale -Art 452 quater c.p.

Questo reato introdotto dall'articolo 1, comma 1 della legge n.68 del 22 maggio 2015 successivamente modificato dalla L. n. 137/2023 si verifica allorché abusivamente si altera irreversibilmente l'equilibrio di un ecosistema, e l'eliminazione di questa alterazione risulti onerosa e conseguibile con provvedimenti eccezionali.

Sono inoltre da tenere in conto gli effetti lesivi per il numero delle persone offese o esposte al pericolo.

La pena prevista, fuori di casi previsti per l'articolo 434c.p. (crollo di costruzioni o altri disastri dolosi) è la reclusione da cinque a quindici anni. Quando il reato è commesso in un'area naturale protetta o sottoposta a vincolo paesaggistico, storico, artistico, o in danno di specie di animali o vegetali

protette, la pena viene aumentata.

Esempio
Tra i disastri ambientali si annovera quello del 10 luglio 1976 a Seveso dove una nube di tetraclorobenzoparadiossina viene rilasciata da una fabbrica di pesticidi esponendo a livelli mai registrati di diossina 37.000 persone, 80.000 animali e l'intero territorio circostante.

6.3.3. Delitti colposi contro l'ambiente -Art 452 quinquies c.p.

Questo reato introdotto dall'articolo 1, comma 1 della legge n.68 del 22 maggio 2015 si verifica quando uno dei fatti contemplati negli articoli precedenti 452- bis e 452-quater è commesso per colpa (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 pena 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.

Esempio
Ad aprile 2016 a Genova si è rotto il tubo di una condotta di una raffineria e sono fuoriuscite 50 tonnellate di petrolio che hanno inquinato gravemente il terreno e due corsi d'acqua limitrofi, tramite i quali parte del petrolio è arrivato in mare.

6.3.4. Traffico e abbandono di materiale ad alta radioattività -Art 452 sexies c.p.

Questo reato introdotto dall'articolo 1, comma 1 della legge n.68 del 22 maggio 2015 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.

Il reato è punito con la reclusione da due a sei anni e con la multa da 10.000 a Euro 50.000. 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.

Esempio

Nel periodo 1993-2005 sono stati registrati circa 300 casi tra furti sostanze radioattive nell'ex Urss. Secondo Associated Press, alcuni cittadini russi – tra cui ex agenti dei servizi segreti – hanno portato avanti un mercato nero di materiale nucleare nell'Europa dell'Est, con l'intento esplicito di mettere in contatto i venditori con acquirenti legati allo Stato Islamico o ad altri gruppi terroristici.

6.3.5. Circostanze aggravanti -Art 452 octies c.p.

L'art. 452-octies è introdotto dall'articolo 1, comma 1 della legge n.68 del 22 maggio 2015 e viene applicato quando a commettere i reati di cui gli articoli precedenti, 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 (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 servizi in materia ambientale.

Esempio

Il caso sulla Cava di Paterno nel Mugello dove è acclarata la commistione tra camorra, banche, imprese, aziende dei rifiuti ed esponenti dei partiti. Dopo aver smaltito al Sud per vent'anni i rifiuti tossici prodotti al Nord, ora la camorra napoletana sta portando i rifiuti campani altrove, in primis in Toscana, nel Comune di Vaglia, dove la vecchia cava-fornace è stata per anni trasformata in una discarica clandestina di ogni genere di rifiuti.

6.3.6. Attività' organizzate per il traffico illecito di rifiuti (Art 452 quaterdecies c.p. inserito da D.lgs 21 del 1marzo 2018 in sostituzione dell'art.260 del D.Lgs 152/2006).

La norma punisce con la reclusione da uno a sei anni "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".

Se si tratta di rifiuti ad alta radioattività si applica la pena della reclusione da tre a otto anni.
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.

6.3.7. Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette Art. 727 bis c.p.

La norma punisce con l'arresto da uno a sei mesi o con l'ammenda fino a quattromila, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie: "Chiunque, fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie animale selvatica protetta".

Chiunque, fuori dai casi consentiti, distrugge, preleva o detiene esemplari appartenenti ad una specie vegetale selvatica protetta è punito con l'ammenda fino a quattromila euro, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie".

La fattispecie sanzionata dal nuovo articolo 727-bis del codice penale consiste nell'uccidere, catturare, prelevare e/o detenere esemplari appartenenti ad una specie animale selvatica protetta (primo comma), ovvero nel distruggere, prelevare o detenere esemplari appartenenti ad una specie vegetale selvatica protetta (secondo comma).

6.3.8. Distruzione o deterioramento di habitat all'interno di un sito protetto Art. 733 bis c.p.

"Chiunque, fuori dai casi consentiti, distrugge un habitat all'interno di un sito protetto o comunque lo deteriora compromettendone lo stato di conservazione, è punito con l'arresto fino a diciotto mesi e con l'ammenda non inferiore a tremila euro".

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.

Esempio:

La società deve eseguire le opportune verifiche in caso di acquisto terreni o siti per la costruzione di nuove strutture.

6.3.9. Commercio internazionale di flora e di fauna selvatiche Artt.1,2,3bis e 6 L. n. 150/1992

Le condotte di cui agli articoli 1,2,3bi e 6 della Legge n. 150/1992 disciplinano il commercio internazionale di flora e fauna selvatiche, con le relative disposizioni che non si applicano nei confronti dei giardini zoologici, delle aree protette, dei parchi nazionali, degli acquari e delfinari, dei circhi e delle mostre faunistiche permanenti o viaggianti, dichiarati idonei dalle autorità competenti

in materia di salute e incolumità pubblica, sulla base dei criteri generali fissati previamente dalla commissione scientifica, in funzione della corretta sopravvivenza degli stessi ,della salute e della incolumità pubblica.

6.3.10. Scarichi di acque reflue - Sanzioni penali Art. 137 D. Lgs. n. 152/2006

L'art. 137 del d. lgs. n. 152/2006 e smi punisce con l'arresto da due mesi a due anni o con l'ammenda da millecinquecento euro a diecimila euro "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". La pena è aumentata quando le condotte riguardano gli scarichi 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. E' ulteriormente aggravata ove quest'ultima condotta si verifichi senza osservare le prescrizioni dell'autorizzazione o le altre prescrizioni dell'autorità competente.

Le singole condotte sanzionate dal comma 1 dell'articolo 137, richiamate dal comma 2 dello stesso articolo 137, rilevano quattro comportamenti illeciti, consistenti:

- nell'apertura ovvero nell'effettuazione di nuovi scarichi di acque reflue industriali senza autorizzazione;
- nell'effettuazione ovvero nel mantenimento di scarichi di acque reflue industriali dopo che l'autorizzazione sia stata sospesa o revocata.

Le prime due condotte sanzionano, dunque, il comportamento sia di chi attiva fisicamente lo scarico, sia di chi subentra nella gestione di uno scarico aperto da altri, senza, in entrambi i casi, avere la prescritta autorizzazione. Ne discende che la norma in commento è volta a condannare una condizione di abusività degli scarichi, ovvero quegli scarichi privi ab origine del titolo abilitativo.
Le rimanenti due condotte sanzionano, invece, una condizione di abusività sopravvenuta, ovvero quei casi in cui l'illiceità dello scarico sopravviene ad un provvedimento amministrativo successivo all'autorizzazione che ne sospende o ne revoca l'efficacia.

La condotta di cui al comma 3 dell'articolo 137, Codice dell'Ambiente, sanziona la condotta consistente nello scarico di acque reflue industriali contenenti sostanze pericolose con violazione delle prescrizioni contenute nell'autorizzazione o di altre prescrizioni imposte dall'autorità competente, ai sensi degli articoli 107, comma 1 e 108, comma 4.

La condotta di cui al comma 5 dell'articolo 137, Codice dell'Ambiente, sanziona la condotta di chiunque effettui scarichi di acque reflue industriali, superando i valori limite fissati dalla tabella 3 o,

nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5 alla parte terza del D.Lgs. n.152/2006, ovvero i limiti più restrittivi fissati dalle Regioni o dalle Province autonome o dall'Autorità competente a norma dell'articolo 107, comma 1, in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5

La condotta di cui al comma 11 dell'articolo 137, Codice dell'Ambiente, sanziona l'inosservanza del divieto di scarico sul suolo e negli strati superficiali del sottosuolo, nonché di scarico diretto nelle acque sotterranee e nel sottosuolo sanciti, rispettivamente, dagli articoli 103 e 104, Codice dell'Ambiente, fatte salve le tassative eccezioni contenute negli stessi articoli 103 e 104.

La condotta di cui al comma 13 dell'articolo 137, Codice dell'Ambiente, sanziona penalmente lo scarico nelle acque del mare da parte di navi o aeromobili, che contenga sostanze o materiali per i quali vige il divieto assoluto di sversamento ai sensi delle disposizioni contenute nelle convenzioni internazionali ratificate dall'Italia (in primis, la Convenzione Marpol 73/78).

6.3.11. Attività di gestione di rifiuti non autorizzata - Art. 256 D. Lgs. n. 152/2006

La condotta di cui al comma 1 dell'articolo 256, Codice dell'Ambiente, disciplina una serie di condotte illecite di gestione dei rifiuti, accomunate dall'esercizio delle stesse in assenza dell'autorizzazione, iscrizione e comunicazione necessaria, ai sensi degli articoli 208, 209, 210, 211, 212, 214, 215 e 216 del Codice dell'Ambiente.

La condotta di cui al comma 3, primo e secondo periodo, dell'articolo 256, Codice dell'Ambiente, attribuisce rilevanza penale alle condotte di gestione e realizzazione di discariche non autorizzate. La condotta di cui al comma 5 dell'articolo 256, Codice dell'Ambiente sanziona la violazione del divieto di miscelazione di rifiuti pericolosi previsto dall'articolo 187, comma 1, Codice dell'Ambiente. La condotta di cui al comma 6, dell'articolo 256, Codice dell'Ambiente, punisce la condotta di chi effettua un deposito temporaneo di rifiuti sanitari pericolosi presso il luogo di produzione, in violazione delle disposizioni dell'articolo 227, comma 1, lettera b), Codice dell'Ambiente.

6.3.12. Bonifica dei siti Art. 257 D. Lgs. n. 152/2006

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 condotta di cui al comma 2, dell'articolo 257, Codice dell'Ambiente, prevede un'aggravante di pena per l'ipotesi in cui l'inquinamento sia provocato da sostanze pericolose.

6.3.13. Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari - Art. 258 D. Lgs. n. 152/2006

Si applica la pena di cui all'articolo 483 del codice penale (falsità ideologica commessa dal privato in atto pubblico) a chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto.

Chi invece pur essendo obbligato non ha aderito al sistema di controllo della tracciabilità dei rifiuti (SISTRI) di cui all'articolo 188-bis, comma 2, lett. a), e che ometta di tenere ovvero tenga in modo incompleto il registro di carico e scarico di cui al medesimo articolo, è punito con la sanzione amministrativa pecuniaria da duemilaseicento euro a quindicimilacinquecento euro.

(omissis)

Il comma 4, seconda parte, dell'articolo 258, Codice dell'Ambiente, punisce penalmente le due seguenti
condotte illecite:

1) la predisposizione di un certificato di analisi dei rifiuti contenente false indicazioni sulla natura, composizione e caratteristiche chimico-fisiche dei rifiuti stessi
2) l'uso di un certificato contenente indicazioni false durante il trasporto dei rifiuti

Tali fattispecie di reato rientrano nel novero dei reati propri, in quanto possono essere commesse solo da soggetti aventi una specifica posizione soggettiva. Nell'ipotesi di predisposizione di un certificato di analisi contenente indicazioni false, tale condotta illecita può essere realizzata solo dalle persone abilitate al rilascio di questi certificati; invece, nell'ipotesi di uso di un certificato di analisi contenente indicazioni false durante il trasporto dei rifiuti, tale condotta è riferibile al trasportatore. Con riferimento all'elemento soggettivo, le fattispecie di reato in esame sono punibili esclusivamente a titolo di dolo.

Nota: l'Art. 6 del D.Lgs 135 del 14 dicembre 2018 ha stabilito che dal 1° gennaio 2019 è soppresso il sistema di controllo della tracciabilità dei rifiuti di cui all'articolo 188-ter (Sistema di controllo della tracciabilità dei rifiuti-SISTRI- del decreto legislativo 3 aprile 2006, n. 152).

Dal 1° gennaio 2019, e fino alla definizione e alla piena operatività di un nuovo sistema di

tracciabilità dei rifiuti organizzato e gestito direttamente dal Ministero dell'ambiente e della tutela del territorio e del mare, i soggetti di cui agli articoli 188-bis e 188-ter del decreto legislativo n. 152 del 2006 garantiscono la tracciabilità dei rifiuti effettuando gli adempimenti di cui agli articoli 188, 189, 190 e 193 del medesimo decreto.

6.3.14. Traffico illecito di rifiuti Art. 259 D. Lgs. n. 152/2006

Chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 26 del regolamento (CEE) 1° febbraio 1993, n. 259, o effettua una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'articolo 1, comma 3, lettere a), b), c) e d), del regolamento stesso è punito con la pena dell'ammenda da millecinquecentocinquanta Euro a ventiseimila Euro e con l'arresto fino a due anni. La pena è aumentata in caso di spedizione di rifiuti pericolosi.
(omissis)

L'articolo 259, comma 1, Codice dell'Ambiente, sanziona due distinte condotte illecite, ovvero:

- il traffico illecito di rifiuti
- la spedizione di rifiuti destinati al recupero ed elencati nell'Allegato II (c.d. Lista Verde) del Regolamento, effettuata in violazione dell'articolo 1, comma 3, lettere a), b), c) e d) del Regolamento stesso.

In particolare, con riferimento alla prima delle sopra indicate condotte (traffico illecito di rifiuti), l'articolo 26 del Regolamento fornisce una definizione di «traffico illecito», penalmente rilevante, individuandolo in "qualsiasi spedizione di rifiuti effettuata in violazione di alcuni degli adempimenti previsti".

6.3.15. Sistema informatico di controllo della tracciabilità dei rifiuti – Art. 260-bis D. Lgs. n. 152/2006

Omissis

6. Si applica la pena di cui all'articolo 483 c.p. a colui che, nella predisposizione di un certificato di analisi di 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

7. (omissis) Si applica la pena di cui all'art. 483 del codice penale in caso di trasporto di rifiuti

pericolosi. Tale ultima pena si applica anche a colui che, durante il trasporto fa uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati

8. Il trasportatore che accompagna il trasporto di rifiuti con una copia cartacea della scheda SISTRI – AREA Movimentazione fraudolentemente alterata è punito con la pena prevista dal combinato disposto degli articoli 477 e 482 del codice penale. La pena è aumentata fino ad un terzo nel caso di rifiuti pericolosi

(omissis)

Il comma 6 dell'articolo 260-bis, Codice dell'Ambiente, sanziona due condotte illecite, ovvero:

- falsificazione, nell'ambito della predisposizione di un certificato di analisi di rifiuti, utilizzato per il sistema di controllo della tracciabilità dei rifiuti, delle indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti. A tale proposito, si precisa che per l'integrazione della fattispecie di reato occorre non solo la predisposizione del certificato analitico dei rifiuti falso, ma anche l'utilizzo dello stesso nell'ambito del sistema di controllo della tracciabilità dei rifiuti.
- Inserimento di un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti, nell'ambito del sistema di controllo della tracciabilità dei rifiuti. Con riferimento all'elemento soggettivo, entrambe le fattispecie di reato in esame sono/erano punibili esclusivamente a titolo di dolo.

Il secondo periodo del comma 7 dell'articolo 260-bis, Codice dell'Ambiente, sanziona penalmente la condotta del trasportatore che omette/avesse omesso di accompagnare il trasporto di rifiuti pericolosi (laddove la natura di «rifiuti pericolosi» è elemento caratterizzante rispetto al primo periodo dello stesso comma) con la copia cartacea della scheda SISTRI - AREA MOVIMENTAZIONE e - ove prescritto dalla normativa vigente - con la copia cartacea del certificato analitico che identifica le caratteristiche dei rifiuti pericolosi trasportati.

Il terzo periodo del comma 7 dell'articolo 260-bis, Codice dell'Ambiente, sanziona penalmente la condotta di chi, durante il trasporto di rifiuti, fa uso di un certificato di analisi contenenti false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati.

Con riferimento all'elemento soggettivo, entrambe le fattispecie di reato in esame sono punibili esclusivamente a titolo di dolo.

Il comma 8, dell'articolo 260-bis, Codice dell'Ambiente, sanziona penalmente la condotta illecita del trasportatore che accompagna i rifiuti (non pericolosi, per quanto attiene al primo periodo, e

pericolosi per il secondo) con una copia cartacea della scheda SISTRI - AREA MOVIMENTAZIONE fraudolentemente alterata- Il reato è punibile a titolo di dolo.

6.3.16. Sanzioni per superamento valori limite di emissione -Art. 279 D. Lgs. n. 152/2006

(omissis)

2. Chi, nell'esercizio di uno stabilimento, viola i valori limite di emissione o le prescrizioni stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla parte quinta del presente decreto, dai piani e dai programmi dalla normativa di cui all'articolo 271 o le prescrizioni altrimenti imposte dall'autorità competente ai sensi del presente titolo è punito con l'arresto fino ad un anno o con l'ammenda fino a 1.032 Euro. Se i valori limite le prescrizioni violati sono contenuti nell'autorizzazione integrata ambientale si applicano le sanzioni previste dalla normativa che disciplina tale autorizzazione
   (omissis)
5. Nei casi previsti dal comma 2 si applica sempre la pena dell'arresto fino ad un anno se il superamento dei valori limite di emissione determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa
   (omissis)

Il comma 2 dell'articolo 279, Codice dell'Ambiente, sanziona la condotta di colui che "nell'esercizio di uno stabilimento" violi i valori limite di emissione o le prescrizioni stabiliti:

- dall'autorizzazione
- dagli Allegati I, II, III o V alla parte quinta del Codice dell'Ambiente
- dai piani e dai programmi citati nell'articolo 271, Codice dell'Ambiente
- dalla normativa di cui all'articolo 271 del Codice dell'Ambiente
- dall'autorità competente
- dall'autorizzazione integrata ambientale

6.3.17. Inquinamento doloso provocato da navi Art.8 D. Lgs. n. 202/2007

1. Salvo che il fatto costituisca più grave reato, il Comandante di una nave, battente qualsiasi bandiera, nonché i membri dell'equipaggio, il proprietario e l'armatore della nave, nel caso in cui la violazione sia avvenuta con il loro concorso, che dolosamente violano le disposizioni dell'art. 4 sono puniti con l'arresto da sei mesi a due anni e con l'ammenda da euro 10.000 ad euro 50.000
2. Se la violazione di cui al comma 1 causa danni permanenti o, comunque, di particolare gravità, alla qualità delle acque, a specie animali o vegetali o a parti di queste, si applica l'arresto da uno a tre anni e l'ammenda da euro 10.000 ad euro 80.000

3. Il danno si considera di particolare gravità quando l'eliminazione delle sue conseguenze risulta di particolare complessità sotto il profilo tecnico, ovvero particolarmente onerosa o conseguibile solo con provvedimenti eccezionali

6.3.18. Inquinamento colposo provocato da navi Art.9 D. Lgs. n. 202/2007

1. Salvo che il fatto costituisca più grave reato, il Comandante di una nave, battente qualsiasi bandiera, nonché i membri dell'equipaggio, il proprietario e l'armatore della nave, nel caso in cui la violazione sia avvenuta con la loro cooperazione, che violano per colpa le disposizioni dell'art. 4, sono puniti con l'ammenda da euro 10.000 ad euro 30.000
2. Se la violazione di cui al comma 1 causa danni permanenti o, comunque, di particolare gravità, alla qualità delle acque, a specie animali o vegetali o a parti di queste, si applica l'arresto da sei mesi a due anni e l'ammenda da euro 10.000 ad euro 30.000
3. Il danno si considera di particolare gravità quando l'eliminazione delle sue conseguenze risulta di particolare complessità sotto il profilo tecnico, ovvero particolarmente onerosa o conseguibile solo con provvedimenti eccezionali.

Le fattispecie sanzionate dagli articoli 8 e 9 del D. Lgs. n. 202/2007 differiscono tra loro unicamente per quanto attiene all'elemento soggettivo della condotta ed alle sanzioni previste. Nel primo caso, infatti, è richiesto il dolo del soggetto agente, mentre nel secondo caso è sufficiente la colpa.

La condotta vietata consiste nel versare in mare o nel causare lo sversamento delle sostanze inquinanti inserite nell'Allegato I (idrocarburi) e nell'Allegato II (sostanze liquide nocive trasportate alla rinfusa) alla Convenzione Marpol 73/78, come richiamate nell'elenco di cui all'Allegato A alla Legge 31 dicembre 1982, n. 979, aggiornato dal Decreto del Ministro della Marina Mercantile 6 luglio 1983 (Sostanze nocive all'ambiente marino di cui è vietato lo scarico da parte del naviglio mercantile nel mare territoriale italiano.

6.3.19. Cessazione e riduzione dell'impiego delle sostanze lesive - Art.3 Legge n. 549/1993

1. La produzione, il consumo, l'importazione, l'esportazione, la detenzione e la commercializzazione delle sostanze lesive (sostanze che riducono lo strato di ozono) di cui alla tabella A allegata alla presente legge sono regolati dalle disposizioni di cui al regolamento (CE) n. 3093/94
2. A decorrere dalla data di entrata in vigore della presente legge è vietata l'autorizzazione di impianti che prevedano l'utilizzazione delle sostanze di cui alla tabella A allegata alla presente legge, fatto salvo quanto disposto dal regolamento (CE) n. 3093/94
3. Con decreto del Ministro dell'ambiente, di concerto con il Ministro dell'industria, del commercio

e dell'artigianato, sono stabiliti, in conformità alle disposizioni ed ai tempi del programma di eliminazione progressiva di cui al regolamento (CE) n. 3093/94, la data fino alla quale è consentito l'utilizzo di sostanze di cui alla tabella A, allegata alla presente legge, per la manutenzione e la ricarica di apparecchi e di impianti già venduti ed installati alla data di entrata in vigore della presente legge, ed i tempi e le modalità per la cessazione dell'utilizzazione delle sostanze di cui alla tabella B, allegata alla presente legge, e sono altresì individuati gli usi essenziali delle sostanze di cui alla tabella B, relativamente ai quali possono essere concesse deroghe a quanto previsto dal presente comma. La produzione, l'utilizzazione, la commercializzazione, l'importazione e l'esportazione delle sostanze di cui alle tabelle A e B allegate alla presente legge cessano il 31 dicembre 2008, fatte salve le sostanze, le lavorazioni e le produzioni non comprese nel campo di applicazione del regolamento (CE) n. 3093/94, secondo le definizioni ivi previste

4. L'adozione di termini diversi da quelli di cui al comma 3, derivati dalla revisione in atto del regolamento (CE) n. 3093/94, comporta la sostituzione dei termini indicati nella presente legge ed il contestuale adeguamento ai nuovi termini
5. Le imprese che intendono cessare la produzione e l'utilizzazione delle sostanze di cui alla tabella B, allegata alla presente legge, prima dei termini prescritti possono concludere appositi accordi di programma con i Ministeri dell'industria, del commercio e dell'artigianato e dell'ambiente, al fine di usufruire degli incentivi di cui all'articolo 10, con priorità correlata all'anticipo dei tempi di dismissione, secondo le modalità che saranno fissate con decreto del Ministro dell'industria, del commercio e dell'artigianato, d'intesa con il Ministro dell'ambiente
6. Chiunque viola le disposizioni di cui al presente articolo è punito con l'arresto fino a due anni e con l'ammenda fino al triplo del valore delle sostanze utilizzate per fini produttivi, importate o commercializzate. Nei casi più gravi, alla condanna consegue la revoca dell'autorizzazione o della licenza in base alla quale viene svolta l'attività costituente illecito

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.

6.4. Le attività sensibili relative ai reati ambientali

Con riferimento alle fattispecie disciplinate dall'art.25-undecies del D.Lgs. 231/01, sono state individuate le principali aree a rischio reato in cui l'azienda potrebbe essere coinvolta e le attività da ritenersi maggiormente "sensibili", ossia quelle attività il cui svolgimento espone la Società al rischio di commissione dei reati individuati nell'ambito della normativa di riferimento.

Di seguito si riportano le "aree a rischio reato" con riferimento alle fattispecie di cui all'art.25-undecies del D.Lgs.231/01 con una breve descrizione delle attività e caratteristiche aziendali:

1. **GESTIONE DI RACCOLTA E TRASPORTO RIFIUTI**
   BPR GROUP si configura come società di consulenza ed engeenering.
   Produce rifiuti assimilabili ai rifiuti urbani: carta e cartone, rifiuti organici, toner, plastica, barattolame, imballaggi plastici, sfalci del verde. In officina i rifiuti sono costituiti da ferro, alluminio e refrigerante esausto (CNC, frese manuali e tornio).
   Tutti i rifiuti suddetti sono rifiuti Non pericolosi.
   I rifiuti relativi all'attività d'ufficio sono raccolti in appositi contenitori forniti dal Servizio Pubblico di Raccolta e svuotati secondo un calendario predefinito o, in alternativa conferiti direttamente in cassonetti pubblici localizzati in apposita area o in Isola Ecologica.
   I rifiuti relativi all'officina sono gestiti mediante fornitore esterno, previo stoccaggio nel rispetto delle norme di sicurezza. Eventuali rifiuti derivanti da attività manutentive straordinarie legate alla struttura (es. neon, rifiuti ingombranti, ecc…) verranno gestiti direttamente dall'azienda che gestisce l'attività manutentiva o verranno conferiti all'Isola Ecologica di Moglia.
   Gli adempimenti in materia di rifiuti sono gestiti puntualmente.

2. **GESTIONE DEGLI ADEMPIMENTI E DELLE ATTIVITÀ CONNESSI ALLA NOTIFICA ED ALLA BONIFICA, A SEGUITO DI UN EVENTO CHE SIA POTENZIALMENTE IN GRADO DI CONTAMINARE IL SUOLO, IL SOTTOSUOLO, LE ACQUE SUPERFICIALI E/O LE ACQUE SOTTERRANEE**
   BPR GROUP ha identificato come eventi che astrattamente potrebbero contaminare il suolo, il sottosuolo e le acque l'utilizzo di estintore a polvere in caso di emergenza incendio e la gestione della vasca di contenimento di olio emulsionabile presente sotto i centri di lavoro.
   Per entrambe le situazioni il personale dedicato è formato e addestrato; sono effettuate verifiche periodiche di controllo.

3. **GESTIONE DEGLI IMPIANTI PER LA RACCOLTA, IL TRATTAMENTO E LO SMALTIMENTO DELLE ACQUE METEORICHE DI DILAVAMENTO RICADENTI SULLE AREE SOCIETARIE**
   BPR GROUP non presenta sulle aree esterne pertinenti, materiale che potrebbe contaminare le acque meteoriche, essendo le stesse destinata a parcheggio di mezzi.

L'analisi del rischio della commissione dei reati di cui alla presente Sezione in relazione alle aree ed attività sensibili sopra indicate e mappate riscontra un livello di rischio BASSO in considerazione della natura dell'attività svolta da BPR Group, delle procedure in essere costantemente attuate e verificate e della segregazione delle funzioni che assicura un puntuale controllo dei processi e la rilevazione di eventuali errori o anomalie.

6.5. Organi e funzioni aziendali coinvolte

In relazione alle descritte Attività Sensibili – tutte astrattamente ipotizzabili – si ritengono particolarmente coinvolti i seguenti organi e funzioni aziendali:

Amministratore Unico
È la funzione che si occupa della gestione della manutenzione di beni mobili/immobili e della definizione delle clausole contrattuali

RSPP/Ambiente-Ufficio Tecnico
È la funzione che presidia la gestione ambiente-rifiuti dal punto di vista tecnico e documentale.

Preposto
Gestione smaltimento e procedure amministrative relative alla produzione di rifiuti ferro e alluminio.

Responsabile amministrativo
Trasmissione di documentazione agli enti competenti

6.6. Principi e regole di comportamento

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, la politica e le procedure aziendali nonché le regole contenute nel Modello e nella presente parte speciale operando, in questo modo, in coerenza con i valori e i principi che sono alla base dell'attività d'impresa in azienda
In generale, il sistema di organizzazione, gestione e controllo della società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà, correttezza, trasparenza e tracciabilità degli atti
Nello svolgimento delle attività sopra descritte e, in generale, delle proprie funzioni, gli amministratori, gli organi sociali, i dipendenti, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, devono conoscere e rispettare:

- La normativa italiana applicabile alle attività svolte

- Il Codice Etico Aziendale
- Le disposizioni contenute nel presente Modello
- Regolamento aziendale
- Le procedure e le linee guida aziendali nonché tutta la documentazione attinente il sistema di organizzazione, gestione e controllo della Società

6.7. Principi e norme generali di comportamento

La presente Sezione è inerente alle condotte poste in essere dai soggetti destinatari del Modello che operano, in particolare, nelle aree a rischio reato e nello svolgimento delle attività sensibili.

Ciò posto e fermo restando quanto indicato nei successivi paragrafi della presente Parte Speciale, in linea generale e al fine di perseguire la prevenzione dei reati ambientali è fatto espresso divieto a tutti i soggetti destinatari del Modello di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, individualmente o collettivamente considerati, integrino, direttamente o indirettamente, le fattispecie di reato di cui all'art. 25-undecies del D.Lgs. 231/01, nonché di porre in essere comportamenti in violazione delle procedure aziendali e dei principi richiamati nella presente Sezione della Parte speciale.

È da considerarsi vietato qualsiasi comportamento che possa integrare una condotta rilevante di una qualsivoglia fattispecie di reato contemplata dall'art.25 -undecies del D.Lgs. 231/01.

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

- Previsione nel Codice Etico e relativa appendice applicativa di specifiche indicazioni volte a impedire la commissione dei reati previsti dall'art.25 -undecies del D.Lgs. 231/01;
- Previsione di un idoneo sistema di sanzioni disciplinari (o vincoli contrattuali nel caso di terze parti) a carico dei dipendenti (o altri destinatari del Modello) che violino i sistemi di controllo preventivi o le indicazioni comportamentali presenti nel Modello e in tutta la documentazione societaria esistente e ad esso afferente;
- Predisposizione di adeguati strumenti organizzativi e normativi atti a prevenire e/o impedire la realizzazione dei reati previsti dall'art. 25 - undecies del D.Lgs. 231/01 da parte dei dipendenti e in particolare di quelli appartenenti alle strutture della società ritenute più esposte al rischio;
- Predisposizione di programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti dalla commissione dei reati previsti dall'art. 25 - undecies del D.Lgs. 231/01.

Conseguentemente, gli organi sociali, gli amministratori, i dipendenti ed i procuratori aziendali nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nello svolgimento delle attività a rischio hanno l'espresso obbligo di perseguire i seguenti principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi di controllo specifici:

- **Gestione delle segnalazioni**
  Raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio per i reati ambientali rilevati da soggetti interni e esterni all'ente

- **Riporto all'OdV (Organismo di Vigilanza)**
  Riferire prontamente all'OdV eventuali situazioni di irregolarità

6.8. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili – salvaguardia ambientale

L'azienda è consapevole che l'impegno costante verso la compatibilità ambientale, al fine di prevenire, nel rispetto della legislazione, l'inquinamento, e una gestione razionale delle risorse naturali rappresentino un'opportunità di sviluppo per l'azienda, migliorandone l'immagine nel contesto sociale in cui opera e contribuendo alla soddisfazione dei clienti finali.

La società persegue l'obiettivo di coniugare le esigenze lavorative con la salvaguardia ambientale, definendo un piano per il miglioramento continuo della gestione ambientale, che tenga conto delle seguenti linee guida:

- Riduzione dei consumi energetici, utilizzando le risorse dove strettamente necessario;
- Utilizzo ridotto e limitato di plastica ad uso personale, privilegiando contenitori riutilizzabili, ove possibile;
- Utilizzo di carta riciclata ad uso interno;
- Riduzione delle stampe e fotocopie e, se necessario, preferire la stampa in bianco e nero.

6.9. Controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui alla presente Parte Speciale.

Tali controlli sono diretti a verificare la corretta applicazione dei principi e delle regole generali di

comportamento del presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

Inoltre, i compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati di cui alla presente Parte Speciale:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati ambientali;
- monitorare sul rispetto delle procedure interne per la prevenzione dei suddetti reati;
- monitoraggio specifico sulle attività sensibili dell'azienda che la espongono ai reati esaminati nella presente Parte Speciale;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente dell'azienda ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

6.10. Flussi informativi all'Organismo di vigilanza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace attuazione del Modello e di curarne l'aggiornamento dovranno essere assicurati i seguenti flussi informativi periodici:

Documenti	Periodicità	Soggetto tenuto
○ richieste di autorizzazioni ambientali ○ elenco aggiornato rifiuti prodotti e modalità di raccolta e smaltimento ○ copia documentazione amministrativa relativa allo smaltimento di rifiuti speciali	Annuale	RSPP/Ufficio tecnico

Tutti i destinatari della presente Parte speciale sono altresì tenuti ad effettuare segnalazioni all'Organismo di vigilanza qualora rilevino eventuali non conformità relative all'applicazione del flusso; al rispetto di procedure/regolamenti; al rispetto delle disposizioni del Modello di organizzazione, gestione e controllo, del Codice etico e in generale del d. lgs. n. 231/2001 e smi.

PARTE SPECIALE

SEZIONE 7 - REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME ANTIFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E SICUREZZA SUL LAVORO

INDICE

7.1	Il sistema tutela della sicurezza sul lavoro	3
7.2	Criteri per la definizione del reato di omicidio colposo e lesioni colpose commesse con violazione delle norme antinfortunistiche	7
7.3	Le fattispecie di reato richiamate dal D.Lgs. 231/01	7
7.3.1	Omicidio colposo – Art. 589 c.p.	7
7.3.2	Lesioni personali colpose gravi e gravissime – Art. 590, comma 3 c.p.	9
7.4	Le sanzioni previste dal Decreto - Art. 55 D.lgs 81/08	10
7.5	Le attività sensibili relative ai reati di omicidio colposo e lesioni colpose commesse	11
7.6	Organi e funzioni aziendali coinvolte	13
7.7	Principi e regole di comportamento	14
7.8	Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili	16
7.9	I controlli dell'Organismo di Vigilanza	31
7.10	Flussi informativi all'Organismo di vigilanza	32

7.1. Il sistema tutela della sicurezza sul lavoro

Il Decreto Legislativo n. 81/2008, noto come Testo Unico sulla Salute e Sicurezza sul Lavoro, ha lo scopo di garantire un ambiente di lavoro sicuro e salubre promuovendo la prevenzione degli infortuni e delle malattie professionali. Assume un approccio integrato alla gestione della sicurezza mediante una ripartizione intersoggettiva del generale obbligo di protezione e la previsione di un modello gestionale basato su prevenzione, programmazione e partecipazione. Il sistema sanzionatorio previsto dal Testo Unico è di tipo prevalentemente penale-contravvenzionale e si va ad integrare con l'apparato codicistico ed in particolare con i reati comuni di evento di omicidio colposo e di lesioni colpose di cui agli artt. 589 e 590 c.p. conseguenti alla violazione della normativa antinfortunistica.

Di seguito sono esplicitati i principali termini relativi alle norme per la salvaguardia della salute e sicurezza sul lavoro previsti dal d. lgs. n. 81/2008 e s.m.i.

ASPP o Addetti al Servizio di Prevenzione e Protezione
I soggetti in possesso delle capacità e dei requisiti professionali di cui all'art. 32 del Decreto Sicurezza designati per l'espletamento dei compiti rientranti nel Servizio di Prevenzione e Protezione.

Cantiere Temporaneo o Mobile o Cantiere
Qualunque luogo in cui si effettuano lavori edili o di ingegneria civile così come individuati nell'allegato X del Decreto Sicurezza, ovvero, lavori di costruzione, manutenzione, riparazione, demolizione, conservazione, risanamento, ristrutturazione, equipaggiamento, trasformazione, rinnovamento o smantellamento di opere fisse, permanenti o temporanee, comprese le linee elettriche e le parti strutturali degli impianti elettrici. Sono, inoltre, lavori di costruzione edile o di ingegneria civile gli scavi ed il montaggio e lo smontaggio di elementi prefabbricati utilizzati per i lavori edili o di ingegneria civile.

Committente
Il soggetto per conto del quale viene realizzata l'intera opera edile o di ingegneria civile, indipendentemente da eventuali frazionamenti della sua realizzazione secondo quanto disposto dagli artt. 88 e ss. del Decreto Sicurezza.

Coordinatore per l'Esecuzione dei Lavori
Il soggetto incaricato dal committente o dal responsabile dei lavori tra l'altro, di verificare, con opportune azioni di coordinamento e controllo, l'applicazione, da parte delle imprese esecutrici e dei lavoratori, anche autonomi, delle disposizioni loro pertinenti contenute nel piano di sicurezza e coordinamento e di verificare altresì l'idoneità del piano operativo di sicurezza, assicurandone la

coerenza con il primo.

Coordinatore per la Progettazione

Il soggetto, incaricato dal committente o dal responsabile dei Lavori, di redigere il piano di sicurezza e di coordinamento e di predisporre un fascicolo contenente le informazioni utili ai fini della prevenzione e della protezione dai rischi cui sono esposti i lavoratori.

Datore di Lavoro

Il soggetto titolare del rapporto di lavoro o, comunque, il soggetto che, secondo il tipo e l'organizzazione dell'impresa, ha la responsabilità dell'impresa stessa ovvero dell'unità produttiva in quanto titolare dei poteri decisionali e di spesa. È responsabile di provvedere all'attuazione di tutti gli obblighi fissati dal D.Lgs. 81/08 s.m.i. Gli obblighi non delegabili sono i seguenti:

- *La valutazione di tutti i rischi e la conseguente elaborazione del documento (Art. 28 Del D.Lgs. 81/08)*
- *La designazione del responsabile del servizio di prevenzione e protezione dei rischi*

Decreto Sicurezza "T.U.S." Testo Unico sulla Sicurezza

Il Decreto Legislativo 9 Aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e sicurezza nei luoghi di lavoro".

Dirigente

Il soggetto che, in ragione delle competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando sulla stessa.

DUVRI o Documento Unico di Valutazione dei Rischi per le Interferenze

Il documento redatto dal datore di lavoro committente contenente una valutazione dei rischi che indichi le misure per eliminare o, ove ciò non risulti possibile, ridurre al minimo i rischi da interferenze nei contratti di appalto, d'opera o di somministrazione ai sensi dell'art. 26 del Decreto Sicurezza.

DVR o Documento di Valutazione dei Rischi

Il documento redatto dal datore di lavoro contenente una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro ed i criteri per la suddetta valutazione, l'indicazione delle misure di prevenzione e protezione e dei dispositivi di protezione individuale conseguente a tale valutazione, il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, l'indicazione del nominativo del RSPP, del RLS e del medico competente che abbia partecipato alla valutazione del

rischio, nonché l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione.

Fascicolo dell'Opera

Il fascicolo predisposto a cura del coordinatore per la progettazione, eventualmente modificato nella fase esecutiva in funzione dell'evoluzione dei lavori ed aggiornato a cura del committente a seguito delle modifiche intervenute in un'opera nel corso della sua esistenza, contenente le informazioni utili ai fini della prevenzione e della protezione dei rischi cui sono esposti i lavoratori.

Lavoratori

Soggetti che svolgono un'attività lavorativa nell'ambito della struttura organizzativa della società e contribuiscono, insieme al datore di lavoro, ai dirigenti ed ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro.

Medico Competente

Il medico preposto all'attività di sorveglianza sanitaria. Il medico deve inoltre possedere uno dei titoli e dei requisiti formali e professionali indicati nel decreto sicurezza che collabora con il datore di lavoro, secondo quanto previsto all'Art.29 del D.Lgs.81/08 e s.m.i, ai fini della valutazione dei rischi e al fine di effettuare la sorveglianza sanitaria (di cui all'Art. 41 del D.Lgs 81/08 e s.m.i.) ed adempiere tutti gli altri compiti di cui al decreto sicurezza.

Preposto

Il soggetto che in ragione delle competenze professionali e nei limiti dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende all'attività lavorativa e garantisce l'attuazione delle direttive ricevute secondo quanto previsto dal D. lgs. n. 81/2008 e s.m.i., controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa.

Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro

I reati di cui all'Art. 25-septies del D.Lgs. 231/2001, ovvero l'omicidio colposo (Art. 589 c.p.) e le lesioni personali colpose gravi o gravissime (Art. 590 terzo comma c.p.) commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

RLS o Rappresentante dei Lavoratori per la Sicurezza

Soggetto eletto o designato per rappresentare i lavoratori in relazione agli aspetti della salute e sicurezza sul lavoro.

RSPP o Responsabile del Servizio di Prevenzione e Protezione

Il soggetto responsabile del servizio di prevenzione e protezione nominato dal datore di lavoro a cui risponde secondo quanto previsto dall'Art. 33 del D.Lgs. 81/08 e s.m.i.

Responsabile dei Lavori
Il soggetto che può essere incaricato dal committente ai fini della progettazione, dell'esecuzione o del controllo dell'esecuzione dell'opera o di una parte della procedura.

Sorveglianza Sanitaria
L'insieme degli atti medici finalizzati alla tutela dello stato di salute e sicurezza dei lavoratori in relazione all'ambiente di lavoro, ai fattori di rischio professionali, ed alle modalità di svolgimento dell'attività lavorativa.

SPP o Servizio di Prevenzione e Protezione
L'insieme delle persone, sistemi e mezzi esterni o interni alla società finalizzati all'attività di prevenzione e protezione dei rischi professionali.

SLL
Salute e sicurezza dei lavoratori

Addetto al Primo Soccorso e addetto alla prevenzione incendi
Soggetti 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.

Referente Tecnico
Soggetto incaricato di assicurare la corretta realizzazione, in conformità alle norme e specifiche tecniche di progetto o del capitolato speciale, delle opere e dei servizi commissionati ad appaltatori/fornitori.

7.2. Criteri per la definizione del reato di omicidio colposo e lesioni colpose commesse con violazione delle norme antinfortunistiche

I reati contro la persona sono ipotesi aggravate dei delitti di omicidio colposo e lesioni personali colpose.

Tale aggravante consiste nella violazione delle norme per la prevenzione degli infortuni sul lavoro, sussiste non soltanto quando sia contestata la violazione di specifiche norme per la prevenzione degli infortuni sul lavoro, ma anche quando la contestazione ha per oggetto l'omissione dell'adozione di misure e/o accorgimenti per la più efficace tutela dell'integrità fisica dei lavoratori

e, più in generale, la violazione di tutte le norme che, direttamente o indirettamente, tendono a garantire la sicurezza del lavoro in relazione all'ambiente in cui deve svolgersi.

7.3. Le fattispecie di reato richiamate dal D.Lgs. 231/01

Si provvede qui di seguito a fornire una breve descrizione dei reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro indicati all'Art. 25-septies del Decreto.

Tale articolo, originariamente introdotto dalla Legge 3 Agosto 2007 n. 123, e successivamente sostituito ai sensi dell'art. 300 del Decreto Sicurezza, prevede l'applicazione di sanzioni pecuniarie ed interdittive agli Enti i cui esponenti commettano i reati di cui agli art. 589 (omicidio colposo) e 590 terzo comma (lesioni personali colpose gravi o gravissime) del codice penale, in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

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

Il Consiglio dei Ministri in data 1 Aprile 2008 ha approvato il D.Lgs. 81/08 attuativo della delega di cui all'Art. 1 della L. 3 Agosto 2007 n. 123 in materia della salute e sicurezza nei luoghi di lavoro modificato dal D.Lgs. 3 Agosto 2009 n. 106 "Disposizioni integrative e correttive del D.Lgs 81/08".

7.3.1. Omicidio Colposo (Art. 589 c.p.)

Tale ipotesi di reato si configura nei confronti di "Chiunque cagiona per colpa la morte di una persona".
I soggetti che possono rispondere del reato sono tutti i soggetti tenuti ad osservare o far osservare le norme di prevenzione o protezione, vale a dire i datori di lavoro, i dirigenti, i preposti, i soggetti destinatari delle deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro nonché i medesimi lavoratori.

La colpa, nel caso che ci interessa, consiste nell'avere il soggetto agito in violazione delle norme sulla prevenzione degli infortuni sul lavoro o meglio nella mancata adozione delle misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili alla luce dell'esperienza e delle più avanzate conoscenze tecnico scientifiche.

Se il reato in oggetto è commesso con violazione delle norme per la prevenzione degli infortuni sul

lavoro, la pena è della reclusione da due a sette anni.

Le misure di sicurezza vanno intese sia in senso statico vale a dire quale obbligo di adottare le misure di protezione e sicurezza oggettiva, sia in senso dinamico da intendersi come obbligo di formare ed informare i lavoratori circa i rischi propri dell'attività lavorativa nonché sulle misure idonee per evitare i rischi o ridurli al minimo.

La colpa per violazione delle norme per la prevenzione degli infortuni sul lavoro, pertanto, può essere ravvisata non solo in caso di violazione delle specifiche norme per la prevenzione degli infortuni sul lavoro ma anche nel caso in cui l'evento (che in caso di omicidio consiste nella morte) dipenda dall'omessa adozione di quelle misure ed accorgimenti imposti all'imprenditore ai fini della tutela dell'integrità fisica e della personalità del lavoratore da differenziare a seconda della tipologia di lavoro e tenendo conto della tecnica e dell'esperienza (art. 2087 del codice civile).

L'ente risponde, ai sensi del D.Lgs. 231/2001, qualora abbia tratto un vantaggio dall'evento dannoso che può consistere, ad esempio, in un risparmio di costi o di tempi per non aver adottato le misure di prevenzione degli infortuni sul lavoro.

Il datore di lavoro risponde, ad esempio, di omicidio colposo nel caso in cui la morte sia derivata dall'inosservanza delle norme sulla prevenzione degli infortuni sul lavoro qualora l'evento della morte si sia verificato nei confronti di un dipendente oppure di un soggetto estraneo all'ambiente di lavoro purché la presenza sul luogo di lavoro non sia eccezionale o atipica.

7.3.2. Lesioni personali colpose gravi e gravissime (Art. 590, comma 3 c.p.)

Tale ipotesi di reato si configura nei confronti di "Chiunque cagiona per colpa una lesione personale".

La colpa richiesta dall'art. 25-septies del D.Lgs. 231/2001, consiste nella violazione delle norme per la prevenzione degli infortuni sul lavoro e di igiene e sicurezza. L'ente, risponde ai sensi del D.Lgs. 231/2001 sia per le ipotesi di lesioni gravi che per i casi di lesioni gravissime qualora abbia tratto un vantaggio concreto da intendersi, ad esempio, come già si è detto, quale una riduzione dei costi per approntare le misure di sicurezza richieste dalla normativa vigente o, comunque, dovute in considerazione delle nuove acquisizioni tecnologiche.

Il delitto, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli

infortuni sul lavoro o relativi all'igiene del lavoro o che abbiamo determinato una malattia professionale, è perseguibile d'ufficio.

Se il reato è commesso 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 500 Euro a 2.000 Euro e la pena per le lesioni gravissime è della reclusione da uno a tre anni.

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

Ai sensi del comma 1 dell'art. 583 cod. penale, la lesione è considerata **grave** 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.

Ai sensi del comma 2 dell'art. 583 cod. penale, la lesione è considerata invece **gravissima** se dal fatto deriva:
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.

Esclusione della responsabilità amministrativa della società

Come già indicato nella Parte Generale del Modello, il D.Lgs. n. 81/2008, all'art. 30, ha indicato le caratteristiche e i requisiti che deve un modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al Decreto.

Pertanto nella predisposizione del Modello e nella definizione degli standard di controllo la società ha tenuto conto:
- delle previsioni del Decreto
- della vigente disciplina legislativa della prevenzione dei rischi lavorativi
- della ISO 45001:2018
- delle Linee Guida Confindustria

- dell'art. 30 del D.Lgs. 81/2008

7.4. Le sanzioni previste dal Decreto (art.55 D.Lgs 81/08)

Per entrambe le fattispecie delittuose sopra indicate - ossia omicidio colposo e lesioni personali colpose gravi o gravissime - gli enti sono soggetti ad una sanzione pecuniaria fino a 1000 quote (si consideri a tal riguardo che il valore di ogni quota può essere determinato, sulla base delle condizioni economiche e patrimoniali dell'ente, tra un minimo di 258 e un massimo di 1549 euro).

Perché si venga a configurare la responsabilità amministrativa della società ai sensi del Decreto Legislativo 8 giugno 2001, n. 231, l'art. 5 del Decreto medesimo esige però che i reati siano stati commessi nel suo interesse o a suo vantaggio (ad esempio in termini di risparmi di costi per la salute e sicurezza sul lavoro) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità' organizzativa dotata di autonomia finanziaria e funzionale nonchè da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso.

L'ente non risponde se le persone hanno agito nell'interesse esclusivo proprio o di terzi.

Nel caso di condanna per uno dei reati sopra indicati, la società potrebbe essere assoggettata anche ad una sanzione interdittiva per una durata non inferiore a tre mesi e non superiore ad un anno.
Tali sanzioni interdittive possono consistere in:

- Interdizione dall'esercizio dell'attività
- Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito
- Divieto di contrattare con la pubblica amministrazione salvo che per ottenere le prestazioni di un pubblico servizio
- Esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi
- Divieto di pubblicizzare beni o servizi

7.5. Le attività sensibili relative ai reati di omicidio colposo e lesioni colpose commesse

Le principali aree aziendali a potenziale rischio reato relativamente alle fattispecie di cui all'art.25-septies del D.Lgs. 231/01 sono identificate e valutate nell'ambito dei documenti aziendali di valutazione dei rischi, predisposti ai sensi della normativa di riferimento e costantemente aggiornati in relazione all'evoluzione delle caratteristiche dell'attività produttiva.

Tuttavia, come precisato dalle Linee Guida di Confindustria per la costruzione dei Modelli di organizzazione, gestione e controllo ex D.Lgs. 231/01, non è possibile individuare e limitare a priori alcun ambito di attività, dal momento che tale casistica di reati può, di fatto, investire la totalità delle componenti aziendali.

In altri termini l'oggetto della presente Parte Speciale potrebbero astrattamente essere commessi in tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni in materia di salute e sicurezza sul lavoro.

Poiché la valutazione dei rischi rappresenta l'adempimento cardine per la garanzia della salute e della sicurezza dei lavoratori e poiché costituisce il principale strumento per procedere all'individuazione delle misure di tutela, siano esse la riduzione o l'eliminazione del rischio, l'operazione di individuazione e di rilevazione dei rischi deve essere effettuata con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza.

Il Modello, pertanto, prevede un costante aggiornamento del Documento di Valutazione dei Rischi (DVR), fornendo così evidenza del suo continuo adeguamento e della sua completezza.

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella parte speciale del presente Modello.

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree di operatività ritenute più specificamente a rischio per la società risultano essere, ai fini della presente Parte Speciale del Modello, le seguenti:

- Attività di ufficio svolta dal personale dipendente, in particolare per ciò che concerne l'utilizzo di videoterminali
- attività di engineering svolta dal personale dipendente in officina
- Attività svolta da personale esterno presso la sede della società, quali fornitori di servizi in base a contratti di appalto, d'opera o di somministrazione (di cui all'art. 26 del Decreto Sicurezza).
- Attività di consulenza esterna alla sede e presso terzi (clienti) in molteplici e variegati contesti produttivi e di cantiere
- Attività di trasferimento, viaggi o trasferte fuori sede
- Attività di addestramento (parti pratiche) nei diversi percorsi formativi erogati
- Attività di audit nei pressi di macchine ed impianti non completi o difformi
- Lavoro solitario o in orari inusuali

Nell'ambito delle suddette aree di operatività, in virtù della probabilità che in tali contesti

l'inosservanza delle norme poste a tutela della salute e sicurezza sul lavoro possa determinare uno degli eventi dannosi di cui all'art. 25 septies, sono state individuate le seguenti attività sensibili:

- Determinazione delle procedure interne in tema di salute e sicurezza sul lavoro volte a definire i compiti e le responsabilità in materia di sicurezza e a garantire una corretta gestione di tutti gli adempimenti posti in capo a ciascun destinatario così come disposti dal Decreto Sicurezza e dalla normativa primaria e secondaria ad esso collegata
- Attribuzione di responsabilità in materia di salute e sicurezza sul lavoro, con particolare riferimento a:
  - Attribuzioni di compiti e doveri in capo a ciascun Destinatario
  - Attività del Servizio Prevenzione e Protezione e del Medico Competente

- Individuazione dei pericoli all'interno della sede dell'azienda e valutazione dei rischi, con particolare riferimento a:
  - Stesura del Documento di Valutazione dei Rischi (DVR)
  - Valutazione dei rischi delle interferenze
  - Gestione dei contratti di appalto
- Sensibilizzazione di tutti i soggetti che, a diversi livelli, operano nell'ambito della struttura aziendale attraverso un'adeguata attività di informazione e la programmazione di piani di formazione in tema di salute e sicurezza nei luoghi di lavoro

- Attuazione di adeguate attività di monitoraggio, verifica ed ispezione, in particolare per ciò che concerne:
  - L'aggiornamento delle misure in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fine della salute e sicurezza sul lavoro
  - La gestione, rettifica ed inibizione dei comportamenti posti in violazione delle norme, attraverso l'eventuale irrogazione di provvedimenti disciplinari

L'analisi del rischio della commissione dei reati di cui alla presente Sezione in relazione alle aree ed attività sensibili sopra indicate e mappate riscontra un livello BASSO, pur considerata l'attività svolta in officina che presenta maggiori probabilità del verificarsi di incidenti/infortuni, che non evidenziano allo stato significatività, rispetto all'attività d'ufficio prevalente. BPR GROUP ha infatti adottato un Sistema di gestione della Sicurezza (SGS) conforme alla norma UNI-INAIL la cui attuazione è puntualmente verificata dall' RSPP che provvede altresì ad aggiornamenti e piani di miglioramento.

7.6. Organi e funzioni aziendali coinvolte

In relazione alle descritte attività sensibili, si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali

Responsabile risorse umane

- In relazione all'attività di gestione dei dipendenti relativamente ad eventuali provvedimenti disciplinari ed agli adempimenti infortunistici
- Per la programmazione di piani di formazione in tema di salute e sicurezza nei luoghi di lavoro
- Per la gestione della sorveglianza sanitaria

RSPP

- In quanto incaricato dal datore di lavoro in relazione all'adempimento di tutti i compiti connessi alla gestione della sicurezza negli ambienti di lavoro.
- Acquisti DPI

Preposto

- In quanto incaricato delle attività di controllo ambienti di lavoro, macchine, impianti e attività di lavoro nel rispetto delle norme antinfortunistiche

Amministratore Unico

Con riferimento all'approvazione del budget annuale di spesa in particolare per ciò che concerne i costi per la sicurezza.

- In qualità di Datore di Lavoro della società secondo la definizione di cui al Decreto Sicurezza, in relazione all'adempimento di tutti i compiti non delegabili a lui attribuiti dal suddetto decreto (e dunque, a titolo esemplificativo, attività di valutazione dei rischi e predisposizione del relativo Documento di Valutazione dei Rischi o valutazione dei rischi delle interferenze), nonché in merito all'inibizione dei comportamenti posti in violazione delle norme a tutela della salute e sicurezza dei Lavoratori attraverso l'adozione di eventuali provvedimenti disciplinari.

Lavoratori

In particolare con riferimento ai soggetti incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei luoghi di lavoro in caso di pericolo, di salvataggio, di primo soccorso e di gestione delle emergenze e, in generale, con riferimento a tutti (compresi i consulenti e formatori esterni nel cui contratto è richiamato l'impegno alla sicurezza), in merito all'osservanza delle norme poste a tutela dell'incolumità propria e altrui.

7.7. Principi e norme generali di comportamento

La presente Parte Speciale si riferisce a comportamenti posti in essere dai Soggetti Apicali o in Posizione Apicale, dipendenti, collaboratori, fornitori della società nonché, nella misura in cui non rientrino in queste definizioni, dalle figure rilevanti di cui al successivo paragrafo (destinatari).

Obiettivo della presente Parte Speciale è che tutti i destinatari si attengano – in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti della società – a regole di condotta conformi a quanto prescritto nella medesima Parte Speciale al fine di prevenire e impedire il verificarsi dei Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Al fine di consentire l'attuazione dei principi finalizzati alla protezione della salute e della sicurezza dei Lavoratori, così come individuati dal Decreto Sicurezza, si prevede quanto segue:

- La tutela della salute e sicurezza sul lavoro (SSL) costituisce parte integrante della politica e gestione aziendale;
- La società adotta un sistema di gestione della salute e sicurezza sul lavoro (SGSL) conforme alle linee guida Inail e all'art. 30 del D.Lgs 81/2008.

Nel sistema di gestione della salute e sicurezza sul lavoro SGSL vengono definite le modalità per individuare, all'interno della struttura organizzativa aziendale, le responsabilità, le procedure, i processi e le risorse per la realizzazione della politica aziendale di prevenzione, nel rispetto delle norme vigenti sulla salute e sicurezza dei lavoratori.

Esso integra obiettivi e politiche per la salute e sicurezza, nella gestione di sistemi di lavoro.

Adottando il SGSL, la Società si propone di:

- Contribuire a migliorare i livelli di salute e sicurezza sul lavoro
- Ridurre incidenti ed infortuni, prevenire le potenziali malattie correlate al lavoro ed i rischi cui possono essere esposti i lavoratori o i terzi (clienti, fornitori, visitatori, etc.,)
- Aumentare la propria efficienza e le proprie prestazioni.

Tutte le attività sensibili devono essere svolte seguendo le leggi vigenti, i valori, le politiche e le procedure aziendali nonché le regole contenute nel Modello e nella presente parte speciale del Modello.

In generale, il sistema di organizzazione, gestione e controllo della Società deve rispettare i principi di attribuzione di responsabilità e di rappresentanza, di separazione di ruoli e compiti e di lealtà,

correttezza, trasparenza e tracciabilità degli atti.

Nello svolgimento delle attività e in generale, delle proprie funzioni, gli amministratori, gli organi sociali, i lavoratori, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, devono conoscere e rispettare:

- Leggi e regolamenti in tema di salute e sicurezza negli ambienti di lavoro
- Il Codice Etico
- Il presente Modello
- Le procedure/linee guida aziendali, la documentazione e le disposizioni inerenti la struttura organizzativa e il sistema di gestione della salute e sicurezza sul lavoro (SGSL).

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

- Conoscibilità all'interno della società
- Delimitazione dei ruoli, con una descrizione dei compiti di ciascuna funzione e dei relativi poteri
- Descrizione delle linee di riporto
- Procedure specifiche per contesti specifici (Istruzioni Operative).

Nello specifico, la società, è dotata di una struttura organizzativa in conformità a quella prevista dalla normativa prevenzionistica vigente.

In coerenza con lo schema organizzativo e funzionale dell'azienda sono stati definiti i compiti e le responsabilità in materia di SSL a partire dal Datore di Lavoro fino al lavoratore.

La società ha, inoltre, individuato il Responsabile Sistema di Gestione (RSGSL), avente la responsabilità di mantenere operativo e far applicare il SGSL, riferendo direttamente al Datore di lavoro in merito alle prestazioni del sistema.

La società, come previsto dal D.Lgs.81/08 e s.m.i, deve garantire il rispetto delle normative in tema di tutela della SSL, di tutela dell'ambiente nonché assicurare in generale un ambiente di lavoro sicuro, sano e idoneo allo svolgimento dell'attività, anche attraverso:

- Una continua analisi del rischio e della criticità dei processi e delle risorse da proteggere in evoluzione con l'attività sempre varia
- La programmazione della prevenzione, mirando ad un complesso che integri in modo coerente nella prevenzione e condizioni lavorative e organizzative dell'azienda nonché l'influenza dei fattori dell'ambiente di lavoro
- Il rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro
- L'eliminazione/riduzione al minimo dei rischi in relazione alle conoscenze acquisite in base al progresso tecnico, privilegiando gli interventi alla fonte

- La sostituzione di ciò che è pericoloso con ciò che non è pericoloso o che è meno pericoloso
- Il controllo e l'aggiornamento delle metodologie di lavoro
- Il controllo sanitario dei lavoratori, con particolare riguardo ai rischi specifici
- Attività di informazione, formazione, consultazione e partecipazione dei lavoratori ovvero dei loro rappresentanti, dei dirigenti e dei preposti sulle questioni riguardanti la sicurezza e la salute sul luogo di lavoro
- La partecipazione e consultazione dei lavoratori e dei loro rappresentanti
- La programmazione delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione del Codice Etico e di buone prassi
- La formalizzazione di istruzioni adeguate ai lavoratori
- L'uso di segnali di avvertimento e sicurezza
- La regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti
- La definizione di adeguate misure di emergenza da attuare in caso di pronto soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato

Le misure relative alla SSL non devono in nessun caso comportare oneri finanziari per i lavoratori.

Nella scelta dei fornitori di beni o servizi, ivi inclusi in materia di SSL, devono essere privilegiati l'affidabilità del fornitore e la sua capacità di assolvere correttamente alle obbligazioni assunte, oltre al rapporto qualità/prezzo del bene o della prestazione offerta.

È fatto espresso divieto di:

- Modificare o disattivare, senza autorizzazione i dispositivi di protezione individuali o collettivi
- Modificare o togliere, senza autorizzazione, i dispositivi di sicurezza o di segnalazione o di controllo
- Fabbricare, acquistare, noleggiare e utilizzare impianti, macchine, attrezzature o altri mezzi tecnici, inclusi dispositivi di protezione individuali e collettivi, non adeguati o non rispondenti alle disposizioni vigenti in materia di sicurezza
- Accedere ad aree di lavoro a cui non si è autorizzati
- Svolgere di propria iniziativa operazioni che non siano di competenza o che possano compromettere la sicurezza propria o di altri lavoratori

7.8. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole definite nel Modello e nei suoi protocolli (sistema procuratorio, Codice Etico, etc.,) gli amministratori, gli organi sociali, i lavoratori, i procuratori aziendali nonché i collaboratori e le controparti contrattuali che operano in nome e per conto della società, nello svolgimento delle attività sono tenuti, al fine di prevenire e impedire il

verificarsi dei reati di cui all'art. 25 septies, al rispetto della normativa vigente, delle regole e procedure aziendali emesse a regolamentazione delle attività a rischio.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale i dipendenti sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei seguenti documenti:

- Organigramma aziendale
- Documento di Valutazione dei Rischi con i relativi documenti integrativi
- Procedure interne di selezione, qualificazione e monitoraggio dei fornitori di servizi
- Procedure interne finalizzate a garantire il mantenimento di elevati standard di sicurezza nei lavori appaltati a terzi a tutela sia del personale dell'azienda che di quello delle ditte appaltatrici presso la sede aziendale
- Procedure interne per l'informazione e la formazione del personale in materia di tutela della salute e della sicurezza sul lavoro
- Codice Etico.

La regolamentazione specifica delle attività a rischi è contenuta ulteriormente in una struttura documentale articolata in:

- Manuale del SGSL
- Documenti del SGSL (Politica, Obiettivi e Programma di Miglioramento, Organigramma, etc.,)
- Procedure del SGSL
- Istruzioni di lavoro
- Registrazioni relative agli aspetti inerenti la SSL tra le quali i registri di dati specifici
- La formazione, i risultati dei monitoraggi ed i risultati dei riesami
- Altri documenti (legislazione, norme tecniche, etc.,).

Il manuale del SGSL, in particolare, ha lo scopo di illustrare gli elementi fondamentali del sistema di gestione della sicurezza sul lavoro dell'azienda.

In particolare intende descrivere le interazioni della Politica e degli obiettivi in materia di sicurezza sul lavoro fornendo anche un orientamento in merito alla documentazione del sistema stesso.

La Società, nella predisposizione del manuale e delle procedure in materia di SSL, rivolge particolare attenzione all'esigenza di garantire il rispetto dei seguenti principi:

- Devono essere formalmente identificate e documentate le responsabilità in materia di SSL, attraverso disposizioni organizzative e deleghe specifiche rilasciate da parte dei soggetti competenti e comunicate ai terzi interessati
- Deve essere nominato il Medico Competente, devono, altresì, essere definiti appositi ed adeguati

flussi informativi verso il Medico Competente in relazione ai processi ed ai rischi connessi all'attività produttiva

- Devono essere tempestivamente identificati e valutati dal Datore di Lavoro i rischi per la SSL ivi compresi quelli riguardanti i lavoratori esposti a rischi particolari, deve, inoltre, essere tenuta in adeguata considerazione la struttura aziendale, la natura dell'attività, l'ubicazione dei locali e delle aree di lavoro, l'organizzazione del personale, i macchinari, le attrezzature e gli impianti impiegati nelle attività e nei relativi cicli di protezione. La valutazione dei rischi deve essere documentata attraverso l'elaborazione, ai sensi della normativa prevenzionistica vigente, di un DVR che contenga quanto prescritto all'Art. 28 del D.Lgs. 81/08 e succ. mod.
- Il DVR deve essere elaborato dal DDL in collaborazione con il RSPP e il medico competente. Il DVR deve essere custodito presso il sito di riferimento ed aggiornato periodicamente e comunque in occasione di modifiche dell'organizzazione del lavoro significative ai fini della salute e sicurezza dei lavoratori, o in relazione al grado di evoluzione della tecnica, della prevenzione o della protezione o a seguito di infortuni significativi o quando i risultati della sorveglianza sanitaria ne evidenzino la necessità. A seguito di tale rielaborazione, le misure di prevenzione debbono essere aggiornate
- La valutazione del rischio deve essere condotta sviluppando il criterio di analisi dei rischi per singola fonte, identificata dalle norme di legge o ragionevolmente prevedibile, individuando nel documento di metodica le modalità di esecuzione. Il documento di metodica è quindi il punto di riferimento per la rappresentazione della metodologica di tutti i rischi, a cui fanno riferimento:
  - Le schede di valutazione del rischio specifica per mansione, sulla base del processo lavorativo e dell'organizzazione presente, atte ad evidenziare i rischi presenti per singole fasi o gruppi di fasi lavorative, e le misure tecniche, organizzative e formative messe in atto per la loro prevenzione
  - Le relazioni tecniche, redatte a supporto dei rischi di mansione, atte a valutare o i rischi presenti nei vari ambienti riferibili alla generalità dei presenti (ad es. rischio incidente rilevante, etc.,) o rischi specifici e ben definiti ma relativi ad un esiguo numero di mansioni.

- Ai fini della gestione delle emergenze, della prevenzione degli incendi e dell'evacuazione dei lavoratori, nonché per il caso di pericolo grave e immediato, devono essere adottate adeguate misure, che prevedano:
  - Lo svolgimento e la documentazione di periodiche prove di evacuazione ossia delle simulazioni ove vengono provate le interazioni fra le varie strutture aziendali preposte, le modalità di evacuazione, le modalità di comunicazione, etc.,
  - La definizione e adozione di adeguate misure per il controllo di situazioni di rischio in caso di emergenza, con particolare riferimento all'elaborazione e periodico aggiornamento, a cura del Servizio di Protezione e Prevenzione, del Piano di sicurezza e di gestione dell'emergenza, testato periodicamente
  - L'identificazione di lavoratori incaricati dell'attuazione delle misure di primo soccorso,

gestione delle emergenze e antincendio che intervengono in funzione dell'area oggetto dell'emergenza
  - La programmazione delle verifiche e delle manutenzioni relative alle apparecchiature antincendio e la regolare tenuta Registro dell'Antincendio

- Devono essere organizzati i necessari rapporti con i servizi pubblici competenti in materia di pronto soccorso, salvataggio, lotta antincendio e gestione delle emergenze

- A seguito della valutazione dei rischi e secondo il programma di sorveglianza sanitaria devono essere individuate, in collaborazione con il medico competente e SPP, le mansioni che necessitano di sorveglianza sanitaria periodica, con riferimento ai requisiti espressamente stabiliti dalla legge, ovvero risultanti da altri criteri/metodologie disponibili

- Gli infortuni sul lavoro che comportano un'assenza di almeno un giorno devono essere tempestivamente, accuratamente e cronologicamente annotati in apposito registro, redatto conformemente al modello approvato con Decreto del Ministero del Lavoro

- Devono essere predisposte apposite procedure interne volte a definire le modalità ed i termini per l'acquisizione e la trasmissione dei dati informativi relativi agli infortuni sul lavoro
- Deve essere definito, documentato, monitorato e periodicamente aggiornato, un programma di informazione dei lavoratori in materia di salute e sicurezza sul lavoro. Gli argomenti dell'informazione sono definiti anche in base alle risultanze della valutazione dei rischi e riguardano almeno:
  - I rischi per la salute e sicurezza connessi all'attività dell'impresa in generale
  - Le misure e le attività di protezione e prevenzione adottate
  - I rischi specifici cui il lavoratore è esposto in relazione all'attività svolta, le normative di sicurezza e le disposizioni aziendali in materia
  - Le procedure che riguardano il pronto soccorso, la lotta antincendio, l'evacuazione dei lavoratori
  - I nominativi del responsabile del servizio di prevenzione e protezione e del medico competente
  - I nominativi dei lavoratori incaricati di applicare le misure lotta all'incendio, evacuazione dei lavoratori e pronto soccorso

A ciascun lavoratore è inoltre fornita, per quanto di competenza, l'informazione specifica per quanto riguarda:
  - Uso delle attrezzature di lavoro
  - Uso dei dispositivi di protezione individuale
  - Movimentazione manuale dei carichi

- Utilizzo di VDT
- Segnaletica visuale, gestuale, vocale, luminosa e sonora
- Ogni altro fattore di rischio e argomento rilevante ai fini della SSL individuato e definito nel programma di informazione

- Deve essere redatto, documentato, implementato, monitorato ed aggiornato un programma di formazione ed addestramento periodico, con particolare riguardo ai lavoratori neo-assunti, per i quali è necessaria una particolare qualificazione in materia di SSL. La formazione e l'addestramento devono essere differenziati in base al posto di lavoro e alle mansioni affidate ai lavoratori, nonché erogati anche in occasione dell'assunzione, del trasferimento o del cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro o di nuove tecnologie. Devono essere monitorati ed adeguatamente documentati il regolare svolgimento e la partecipazione ai corsi di in materia di SSL

- Deve essere attuato il coinvolgimento di tutti i lavoratori sui temi della SSL con continuità e periodicità

- L'efficacia e l'adeguatezza delle misure di prevenzione e protezione devono essere periodicamente monitorate. Tali misure devono essere sostituite, modificate o aggiornate qualora ne sia riscontrata l'inefficacia e/o l'inadeguatezza, ovvero in relazione ad eventuali mutamenti organizzativi e dei rischi. È necessario predisporre un piano di esecuzione delle verifiche, che indichi anche le modalità di esecuzione delle stesse, nonché le modalità di segnalazione di eventuali difformità

- Il corretto utilizzo, da parte dei lavoratori, dei dispositivi di protezione individuale per lo svolgimento delle mansioni loro attribuite deve essere costantemente monitorato

- Il DDL e il RSPP con la partecipazione del Medico competente, devono programmare ed effettuate apposite riunioni con i RLS, volte ad approfondire le questioni connesse alla prevenzione ed alla protezione dai rischi. Le riunioni devono essere adeguatamente formalizzate mediante la redazione di apposito verbale, il quale dovrà essere inviato all'Organismo di Vigilanza (ODV)

- Il divieto di fumare in tutti gli ambienti di lavoro deve essere formalizzato ed adeguatamente pubblicizzato

- Deve essere garantita la manutenzione ordinaria e straordinaria dei dispositivi di sicurezza aziendale (ad esempio, porte tagliafuoco, lampade di emergenza, estintori, etc.,). Manutenzioni ordinarie programmate devono essere effettuate sugli ambienti, gli impianti, i macchinari e le

attrezzature generiche e specifiche in conformità alle indicazioni dei fabbricanti

- Deve essere predisposto ed implementato un sistema di controllo interno idoneo a garantire la costante registrazione, anche attraverso l'eventuale redazione di apposita documentazione, delle verifiche svolte dalla Società in materia di SSL. In tale ambito, la Società deve prevedere che l'ODV effettui un'attività di monitoraggio periodica della funzionalità del complessivo sistema preventivo adottato. A tal fine deve essere inviata all'ODV copia della reportistica periodica in materia di SSL, del verbale della riunione periodica di cui all'art. 35 del D.Lgs. 81/08 e succ. mod, nonché tutti i dati relativi agli infortuni sul lavoro occorsi nei siti della Società

- Devono essere previste nel sistema disciplinare e meccanismo sanzionatorio adottato dalla Società, nel rispetto di quanto previsto dalla legge e dalla contrattazione collettiva, apposite sanzioni per la violazione del Modello in materia di SSL.

La Società ha facoltà di integrare, in qualsiasi momento, i principi elencati nel presente paragrafo così come le procedure aziendali vigenti, qualora ritenuto opportuno al fine di garantire la SSL .

Tali procedure e i documenti devono essere considerati come parte integrante delle strutture di organizzazione gestione e controllo necessarie per il corretto funzionamento ed efficacia del Modello 231 e sono aggiornati dalle funzioni aziendali e dagli Organi Sociali competenti.

Si riportano qui di seguito gli adempimenti che, in attuazione dei principi sopra descritti e della normativa applicabile, sono posti a carico delle figure rilevanti, salvo l'obbligo in capo a tutti i destinatari di segnalare all'Organismo di Vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente Parte Speciale sia stato commesso o possa essere commesso.

Il Datore di Lavoro

Al datore di lavoro sono attribuiti tutti gli obblighi in materia di salute e sicurezza sul lavoro, tra cui i seguenti compiti non delegabili:

- Valutare tutti i rischi per la sicurezza e per la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari (es. rischi connessi alla differenza di genere, alla provenienza da altri Paesi, etc.,) anche nella scelta delle attrezzature di lavoro, nonché nella sistemazione dei luoghi di lavoro; a tal riguardo, nelle scelte operate il Datore di Lavoro dovrà garantire il rispetto degli standard tecnico-strutturali previsti dalla legge

- Elaborare, all'esito di tale valutazione, un Documento di Valutazione dei Rischi con data certa

contenente:

- Una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro, nella quale siano specificati i criteri adottati per la valutazione stessa
- L'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuale adottati, a seguito della suddetta valutazione dei rischi
- Il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza
- L'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere
- L'indicazione del nominativo del RSPP, degli RLS e del medico competente che abbiano partecipato alla valutazione del rischio
- L'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

L'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con il RSPP e con il medico competente. La valutazione dei rischi è oggetto di consultazione preventiva con il RLS, e va nuovamente effettuata in occasione di modifiche del processo produttivo significative ai fini della sicurezza e della salute dei Lavoratori, o in relazione al grado di evoluzione della tecnica, della prevenzione e della protezione, a seguito di infortuni significativi o quando i risultati della Sorveglianza Sanitaria ne evidenzino la necessità.
Nell'ambito della riunione annuale ai fini della sicurezza a cui partecipano il Datore di Lavoro, il RSPP, il Medico Competente, gli RLS viene riesaminato, tra gli altri documenti, anche il Documento di Valutazione dei Rischi.

- Designare il Responsabile del Servizio di Prevenzione e Protezione sia esso interno o esterno all'azienda

Al Datore di Lavoro sono attribuiti i seguenti altri compiti dallo stesso delegabili a soggetti qualificati.

Tali compiti, previsti dal Decreto Sicurezza, riguardano, tra l'altro, il potere di:

- Nominare il medico competente per l'effettuazione della sorveglianza sanitaria
- 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 ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione delle emergenze
- Fornire ai Lavoratori i necessari ed idonei dispositivi di protezione individuale, sentito il RSPP ed il medico competente
- Adottare 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
- Adempiere agli obblighi di informazione e formazione di cui ai successivi paragrafi
- Comunicare all'Inail, a fini statistici e informativi, i dati relativi agli infortuni sul lavoro che comportino un'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, le informazioni relative agli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni
- Convocare la riunione periodica di cui all'art. 35 del Decreto Sicurezza;
- 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
- Prevedere un adeguato sistema di vigilanza sul rispetto delle procedure e delle misure di sicurezza da parte dei lavoratori, individuando specifiche figure a ciò deputate
- Adottare provvedimenti disciplinari, in conformità alle disposizioni contrattuali e legislative, nei confronti dei lavoratori che non osservino le misure di prevenzione e le procedure di sicurezza mettendo in pericolo, attuale o potenziale, la propria o altrui sicurezza.

In relazione a tali compiti, ed a ogni altro compito affidato al datore di lavoro che possa essere da questo delegato ai sensi del Decreto Sicurezza, la suddetta delega, cui deve essere data adeguata e tempestiva pubblicità, è ammessa con i seguenti limiti e condizioni:
- Che essa risulti da atto scritto recante data certa
- Che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate
- Che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate
- Che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate
- Che la delega sia accettata dal delegato per iscritto

Al fine di garantire l'attuazione di un modello di sicurezza aziendale sinergico e compartecipativo, il datore di lavoro fornisce al Servizio di Prevenzione e Protezione e al Medico Competente informazioni in merito a:
- La natura dei rischi
- L'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive
- La descrizione degli impianti e dei processi produttivi
- I dati relativi agli infortuni e quelli relativi alle malattie professionali

Il Servizio di Prevenzione e Protezione (SPP)

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro organizza il Servizio di Prevenzione e Protezione all'interno dell'azienda o incarica persone o servizi esterni assicurandosi che gli ASPP ed i RSPP, da questi nominati, siano in possesso delle capacità e dei requisiti professionali di cui all'Art. 32 del Decreto Sicurezza (es. possesso di un titolo di studio di istruzione secondaria superiore, nonché di un attestato di frequenza, con verifica di apprendimento, a specifici corsi di formazione adeguati alla natura dei rischi presenti sul luogo di lavoro, etc.,)…

Il SPP provvede a:

- Individuare i fattori di rischio, valutare i rischi e individuare le misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente e sulla base della specifica conoscenza dell'organizzazione aziendale
- Elaborare, per quanto di competenza, le misure preventive e protettive di cui all'art. 28 del Decreto Sicurezza e dei sistemi di controllo di tali misure
- Elaborare procedure di sicurezza per le varie attività aziendali
- Proporre programmi di informazione e formazione dei lavoratori
- Partecipare, attraverso il RSPP, alla "riunione periodica di prevenzione e protezione dai rischi" di cui all'art. 35 del Decreto Sicurezza
- Partecipare alle consultazioni in materia di tutela della salute e della sicurezza
- Informare i lavoratori, a nome e per conto del Datore di Lavoro, sulle tematiche di cui all'art. 36 del Decreto Sicurezza come indicato nel dettaglio al successivo paragrafo
- Segnalare all'Organismo di Vigilanza la sussistenza di eventuali criticità nell'attuazione delle azioni di recupero prescritte dal Datore di Lavoro

L'eventuale sostituzione del RSPP deve essere comunicata all'Organismo di Vigilanza con l'espressa indicazione delle motivazioni a supporto di tale decisione.

Il Medico Competente

Il Medico Competente deve essere in possesso di uno dei titoli di cui all' art. 38 del Decreto Sicurezza e, precisamente:

- Specializzazione in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica
- Docenza in medicina del lavoro o in medicina preventiva dei lavoratori e psicotecnica, o in tossicologia industriale, o in igiene industriale, o in fisiologia ed igiene del lavoro o in clinica del lavoro
- Autorizzazione di cui all'articolo 55 del D.Lgs. 277/91 e successive modifiche che prevede una comprovata esperienza professionale di almeno 4 anni

Il Medico Competente provvede a:

- Collaborare con il Datore di Lavoro e con il Servizio di Prevenzione e Protezione alla predisposizione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori
- Effettuare le visite mediche preventive e periodiche previste dalla legge e da programmi di prevenzione opportunamente stabiliti
- Fornire informazioni ai lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informarli sui risultati
- Esprimere il giudizio di idoneità specifica alla mansione
- Istituire ed aggiornare, per ogni lavoratore sottoposto a sorveglianza sanitaria, le cartelle sanitarie e di rischio, con salvaguardia del segreto professionale
- Visitare gli ambienti di lavoro, congiuntamente al RSPP, redigendo specifico verbale e partecipare alla programmazione del controllo dell'esposizione dei lavoratori
- Comunicare, in occasione della "riunione periodica di prevenzione e protezione dai rischi" di cui all'art. 35 del Decreto Sicurezza, i risultati anonimi collettivi degli accertamenti sanitari, fornendo le informazioni necessarie
- Collaborare all'attività di informazione e formazione dei lavoratori
- Collaborare con il Datore di Lavoro alla predisposizione del servizio di pronto soccorso

Il Medico Competente può avvalersi, per accertamenti diagnostici, della collaborazione di medici specialisti scelti in accordo con il Datore di Lavoro che ne sopporta gli oneri.

Il Datore di Lavoro assicura al Medico Competente le condizioni necessarie per lo svolgimento di tutti i suoi compiti garantendone la piena autonomia.

I Rappresentanti dei Lavoratori per la Sicurezza (RLS)

Sono i soggetti eletti o designati, in conformità a quanto previsto dagli accordi sindacali in materia, per rappresentare i lavoratori per gli aspetti di salute e sicurezza sui luoghi di lavoro.

Gli RLS:

- Accedono ai luoghi di lavoro
- Sono consultati preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive
- Sono consultati sulla designazione del RSPP, degli ASPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso
- Sono consultati in merito all'organizzazione delle attività formative

- Promuovono l'elaborazione, l'individuazione a l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei Lavoratori
- Partecipano alla "riunione periodica di prevenzione e protezione dai rischi" di cui all'art. 35 del Decreto Sicurezza
- Ricevono informazioni e la documentazione aziendale inerenti alla valutazione dei rischi e le misure di prevenzione relative, nonché quelli inerenti alle sostanze e ai preparati pericolosi, alle macchine, agli impianti, all'organizzazione e agli ambienti di lavoro, agli infortuni ed alle malattie professionali; ricevono altresì, su loro richiesta e per l'espletamento delle loro funzioni, copia del Documento di Valutazione dei Rischi
- Ricevono informazioni provenienti dai servizi di vigilanza
- Ricevono un'informazione adeguata e comunque non inferiore a quella prevista per i lavoratori ai sensi dell'art. 37 del Decreto Sicurezza
- Formulano osservazioni in occasione di visite e verifiche effettuate dalle autorità competenti dalle quali siano sentiti
- Avvertono il Datore di Lavoro dei rischi individuati nel corso della loro attività
- Possono far ricorso alle autorità competenti qualora ritengano che le misure di prevenzione e protezione dai rischi adottate dal Datore di Lavoro o dai dirigenti ed i mezzi impiegati per attuarle non siano idonei a garantire la sicurezza e la salute durante il lavoro.

Gli RLS dispongono del tempo necessario allo svolgimento dell'incarico, senza perdita di retribuzione, nonché dei mezzi e degli spazi necessari per l'esercizio delle funzioni e delle facoltà loro riconosciute; non possono subire pregiudizio alcuno a causa dello svolgimento della propria attività e nei loro confronti si applicano le stesse tutele previste dalla legge per le rappresentanze sindacali.

I Lavoratori

È cura di ciascun lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite.

I lavoratori devono:

- 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, i mezzi di trasporto e le altre attrezzature di lavoro, nonché gli eventuali dispositivi di sicurezza
- Segnalare immediatamente al Datore di Lavoro, al Dirigente o al Preposto le deficienze dei mezzi e dispositivi dei punti precedenti, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e

possibilità, per eliminare o ridurre tali deficienze o pericoli, dandone notizia al Rappresentante dei Lavoratori per la Sicurezza
- Non rimuovere né modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo
- Non compiere di propria iniziativa operazioni né manovre che non siano di loro competenza ovvero che possano compromettere la sicurezza propria o di altri lavoratori
- Sottoporsi ai controlli sanitari previsti nei loro confronti
- Contribuire, insieme al Datore di Lavoro, ai Dirigenti e ai Preposti, all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro

Attività di formazione ed informazione

ATTIVITÀ DI INFORMAZIONE

L'azienda è tenuta a fornire adeguata informazione ai dipendenti e nuovi assunti, ai lavoratori, agli stagisti circa:
- I rischi specifici dell'impresa
- Le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle prescrizioni di legge e di autoregolamentazione di cui l'azienda si è dotata
- Il ruolo e responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità delle prescrizioni di cui sopra
- Le misure di prevenzione e protezione adottate nonché sulle conseguenze che il mancato rispetto di tali misure può provocare anche ai sensi del D.Lgs. 231/2001.

Tale informazione deve essere facilmente comprensibile per ciascun lavoratore, consentendo a ciascuno di acquisire le necessarie conoscenze e deve essere preceduta, qualora riguardi lavoratori immigrati, dalla verifica della comprensione della lingua utilizzata nel percorso formativo.
Ciò premesso, l'azienda, in considerazione dei diversi ruoli, responsabilità, capacità e dei rischi cui è esposto ciascun dipendente, fornisce tra l'altro, adeguata informazione ai lavoratori sulle seguenti tematiche:
- Sui rischi per la salute e sicurezza sul lavoro, connessi all'attività dell'impresa in generale e su quelli specifici cui ciascun lavoratore è esposto in relazione all'attività svolta
- Sulle misure di prevenzione e protezione adottate
- Sulle procedure che riguardano il primo soccorso, la lotta antincendio, l'evacuazione dei luoghi di lavoro
- Sui nominativi dei lavoratori incaricati delle misure di emergenza e di pronto soccorso, nonché del Medico Competente

Si precisa infine che nei confronti dei dipendenti distaccati se esistenti, in capo ai quali permangono

gli obblighi in materia di prevenzione e protezione, la società destina adeguata informativa circa i rischi generalmente connessi alle mansioni per le quali i dipendenti vengono distaccati.

Con l'obiettivo di rafforzare l'efficacia del sistema organizzativo adottato dalla società per la gestione della salute e sicurezza dei Lavoratori e quindi per la prevenzione degli infortuni, la società si organizza per assicurare un adeguato livello di circolazione e condivisione delle informazioni tra tutti i lavoratori.

In primo luogo, la società mette a disposizione un apposito sistema di comunicazione aziendale attraverso cui ciascun Lavoratore ha la possibilità di conoscere le procedure aziendali in tema di sicurezza e portare a conoscenza del proprio superiore gerarchico le proprie osservazioni, proposte ed esigenze di miglioramento relative alla gestione della salute e sicurezza in ambito aziendale.

In secondo luogo, la società garantisce a tutti i lavoratori un'adeguata e costante informativa attraverso la predisposizione di comunicati e l'organizzazione di incontri periodici, cui l'Organismo di Vigilanza ha la facoltà di partecipare, che abbiano ad oggetto:

- Eventuali nuovi rischi in materia di salute e sicurezza
- Modifiche nella struttura organizzativa per la gestione della salute e sicurezza nei luoghi di lavoro
- Predisposizione di nuove procedure o aggiornamento in merito a quelle esistenti per la gestione della salute e sicurezza sul lavoro
- Ogni altro aspetto inerente la salute e sicurezza dei lavoratori

Di tutta l'attività di informazione sopra descritta deve essere data evidenza su base documentale, eventualmente anche mediante apposita verbalizzazione. A tali fini la società deve mettere a disposizione dei destinatari una bacheca che conterrà i vari riferimenti in tema di sicurezza, la normativa, la descrizione della struttura, le circolari interne ed i nominativi degli RLS.

ATTIVITÀ DI FORMAZIONE

La società deve fornire adeguata formazione a tutti i lavoratori in materia di sicurezza sul lavoro e il contenuto della stessa deve essere facilmente comprensibile e consentire di acquisire le conoscenze e competenze necessarie.

A tal riguardo si specifica che:

- Il RSPP e il medico competente debbono partecipare alla stesura del piano di formazione
- La formazione erogata deve prevedere questionari di valutazione dell'apprendimento
- La formazione deve essere adeguata ai rischi della mansione cui il lavoratore è in concreto assegnato
- I lavoratori che cambiano mansione e quelli trasferiti devono fruire di formazione specifica,

preventiva e/o aggiuntiva, ove necessario, per il nuovo incarico

- Ciascun lavoratore deve essere sottoposto a tutte quelle azioni formative rese obbligatorie dalla legge, tra le quali, ad esempio:
  - L'uso delle attrezzature di lavoro
  - La movimentazione manuale carichi
  - L'uso dei videoterminali
  - La segnaletica visuale, gestuale, vocale, luminosa e sonora

- Gli addetti a specifici compiti in materia di emergenza devono ricevere specifica formazione
- L'azienda deve effettuare periodiche esercitazioni di emergenza di cui deve essere data evidenza (attraverso, ad esempio, la verbalizzazione dell'avvenuta esercitazione con riferimento alle modalità di svolgimento e alle risultanze)
- I neo assunti - in assenza di pregressa esperienza professionale/lavorativa e di adeguata qualificazione - non possono essere adibiti in autonomia ad attività operativa ritenuta più a rischio infortuni se non dopo l'acquisizione di un grado di professionalità idoneo allo svolgimento della stessa mediante adeguata formazione non inferiore ad almeno tre mesi dall'assunzione, salvo periodi più ampi per l'acquisizione di qualifiche specifiche.

Di tutta l'attività di formazione sopra descritta deve essere data evidenza su base documentale, eventualmente anche mediante apposita verbalizzazione.

Conservazione della documentazione rilevante

La società garantisce che vengano adeguatamente conservati su supporto cartaceo ed informatico, e aggiornati i seguenti documenti:

- La cartella sanitaria, ove prevista, deve essere istituita e aggiornata dal medico competente e custodita dal Datore di Lavoro
- Il registro infortuni
- Verbalizzazione delle visite dei luoghi di lavoro effettuate congiuntamente dal RSPP e dal medico competente
- Documenti che registrano gli adempimenti espletati in materia di sicurezza e salute sul lavoro
- Documento di Valutazione dei Rischi
- Documento di Valutazione dei Rischi integrato ("DUVRI")
- Nomina formale del Responsabile e degli Addetti al Servizio di Prevenzione e Protezione (RSPP e ASPP), del Medico Competente, degli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, nonché degli eventuali Dirigenti e Preposti
- Documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti alla realtà aziendale
- Documentazione inerente a regolamenti ed accordi aziendali

- Manuali di istruzione per l'uso di macchine e attrezzature forniti da fabbricanti e/o fornitori
- Ogni procedura adottata dall'azienda per la gestione della salute e sicurezza sui luoghi di lavoro
- Tutta la documentazione relativa alle attività di cui a "Informazione" e "Formazione", che deve essere conservata a cura del RSPP e messa a disposizione dell'Organismo di Vigilanza.

Contratto di appalto

La società predispone e mantiene aggiornato l'elenco delle aziende che operano all'interno dei propri siti con contratto d'appalto.

Le modalità di gestione e di coordinamento dei lavori in appalto vengono formalizzate in contratti scritti nei quali siano presenti espressi riferimenti agli adempimenti in capo al Datore di Lavoro di cui all'art. 26 del Decreto Sicurezza, tra cui, in via esemplificativa:

- Verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori da affidare in appalto attraverso:
  - Acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato
  - Acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale ai sensi dell'articolo 4 del Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445
- Fornire informazioni dettagliate agli appaltatori circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività
- Cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto
- Coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori
- Predisporre un unico DUVRI che indichi le misure adottate al fine di eliminare, o quanto meno ridurre al minimo, i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva; tale documento deve allegarsi al contratto di appalto o d'opera
- Verificare in fase di gestione del contratto ed esecuzione dei lavori il rispetto delle misure previste di prevenzione e protezione e il rispetto degli adempimenti di legge verso il personale di cui al punto precedente
- Assicurarsi che il personale dell'impresa appaltatrice o subappaltatrice esponga, in presenza dello specifico obbligo di legge, la tessera di riconoscimento con fotografia, dati anagrafici e indicazione del Datore di Lavoro

Nei contratti di somministrazione, di appalto e di subappalto, vengono specificamente indicati i costi relativi alla sicurezza del lavoro.

A tali dati possono accedere, su richiesta, gli RLS e le organizzazioni sindacali dei lavoratori.

Infine, nei contratti di appalto viene chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

Clausole contrattuali

La società inserisce, nei contratti con i Collaboratori esterni e con i Partner, un'apposita dichiarazione dei medesimi con cui afferma:

- Di essere a conoscenza della normativa di cui al Decreto e delle sue implicazioni per la società, nonché dell'adozione da parte della stessa del Modello e del Codice Etico
- Di non essere mai stati implicati in procedimenti giudiziari relativi ai reati contemplati nel Decreto
- Di impegnarsi al rispetto delle prescrizioni contenute nel Decreto, nonché dei principi contenuti nel Modello, nel Codice Etico.

Inoltre, nei contratti con i collaboratori esterni e con i partner, viene inserita un'apposita clausola che regola le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto nonché dei principi di cui al Modello (ad es. clausole risolutive espresse, penali).

7.13. I controlli dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai compiti e doveri dell'Organismo di Vigilanza ed al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei destinatari, nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo.

Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate in tema di sicurezza sul lavoro, la documentazione prevista dal Decreto Sicurezza, il rispetto delle relative formalità, nonché l'adeguatezza dei sistemi dei controlli interni adottati in tale ambito.

In particolare l'Organismo di Vigilanza dovrà esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.
Al fine di svolgere i propri compiti, l'Organismo di Vigilanza può:

- partecipare agli incontri organizzati dalla società tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;
- accedere a tutta la documentazione di cui al precedente paragrafo.

L'azienda istituisce altresì a favore dell'Organismo di Vigilanza flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

L'Organismo di Vigilanza, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse competenti in azienda. L'Organismo di Vigilanza si incontra regolarmente ed almeno semestralmente con il RSPP per una disamina complessiva degli aspetti relativi alle tematiche sulla sicurezza sul lavoro.

7.14. Flussi informativi all'Organismo di vigilanza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace attuazione del Modello e di curarne l'aggiornamento dovranno essere assicurati i seguenti flussi informativi periodici:

Documenti	Periodicità	Soggetto tenuto
○ Modifica organigramma sicurezza ○ Modifiche SSL ○ Conferimento delega di funzioni ○ Aggiornamenti Dvr e procedure di emergenza ○ Verbale di riunione periodica ○ Contratti di appalto/DUVRI ○ Segnalazione di mancati infortuni ○ Denunce di infortuni ○ Sanzioni disciplinari comminate a dipendenti per violazione della normativa antinfortunistica ○ Verbali ispettivi	Al verificarsi della condizione	Amministratore unico RSPP

Tutti i destinatari della presente Parte speciale sono altresì tenuti ad effettuare segnalazioni all'Organismo di vigilanza qualora rilevino eventuali non conformità relative all'applicazione del flusso; al rispetto di procedure/regolamenti; al rispetto delle disposizioni del Modello di organizzazione, gestione e controllo, del Codice etico e in generale del d. lgs. n. 231/2001 e smi.

PARTE SPECIALE

SEZIONE 8 - DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

INDICE

8.1	Introduzione e funzione della parte speciale dedicata ai reati in violazione del diritto d'autore	3
8.2	Criteri per la definizione di diritto d'autore	3
8.3	Le fattispecie di reato richiamate dal D.Lgs. 231/2001 aggiornate dal D.L n.8 del 15 gennaio 2016	3
8.3.1	Messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa - Art. 171, L. 633/1941 comma 1 lett a) bis	4
8.3.2	Reati commessi su opera altri non destinata alla pubblicazione qualora ne risulti offeso l'onore/reput. - Art. 171, L. 633/1941 comma 3	4
8.3.3	Abusiva duplicazione contenuta in supporti non contrassegnati dalla SIAE - Art. 171-bis L. 633/1941 comma 1	4
8.3.4	Riproduzione, trasferimento su altro supporto del contenuto di una banca dati - Art. 171-bis L. 633/1941 comma 2	4
8.3.5	Abusiva duplicazione di opere dell'ingegno destinate al circuito televisivo, cinematografico, etc., - Art. 171-ter L. 633/1941	5
8.3.6	Mancata comunicazione alla SIAE dei dati di identificazione dei supporti - Art. 171-septies L. 633/1941	5
8.3.7	Fraudolenta produzione, vendita o importazione di apparati di decodifica - Art. 171-octies L. 633/1941	5
8.4	Le attività sensibili relative ai reati in violazione del diritto d'autore	5
8.5	Organi e funzioni coinvolte	6
8.6	Principi e norme generali di comportamento	6
8.7	Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili	8
8.8	I controlli dell'Organismo di Vigilanza	9
8.9	Flussi informativi all'Organismo di Vigilanza	10

8.1. Introduzione e funzione della parte speciale dei reati in violazione del diritto d'autore

L'art. 25-novies del d.lgs. 231/2001, introdotto dall'art. 15 della L. 99/2009, prevede la punibilità della Società con riferimento alla commissione dei reati di violazione del diritto di autore, sempre che siano stati commessi nell'interesse o a vantaggio della medesima.

Allo scopo di evitare e prevenire la realizzazione dei reati previsti dall'art. 25-novies del d.lgs. 231/2001 ed in conformità con le politiche aziendali, nonché in attuazione dei principi di trasparenza, efficienza e buon governo, i Destinatari del Modello dovranno rispettare e uniformarsi alle prescrizioni di seguito riportate.

8.2. Criteri per la definizione di diritto d'autore

Il **diritto d'autore** è la posizione giuridica soggettiva dell'autore di un'opera dell'ingegno a cui i diversi ordinamenti nazionali e varie convenzioni internazionali (quale la Convenzione di Berna) riconoscono la facoltà originaria esclusiva di diffusione e sfruttamento.

8.3. Le fattispecie di reato richiamate dal D.Lgs. 231/01

Si riporta di seguito il testo integrale dell'art. 25 novies del D. Lgs.231/2001:

Delitti in materia di violazione del diritto d'autore

1. In relazione alla commissione dei delitti previsti dagli articoli 171, primo comma, lettera a-bis), e terzo comma, 171-bis, 171-ter, 171-septies e 171-octies della legge 22 aprile 1941, n. 633, si applica all'ente la sanzione pecuniaria fino a cinquecento quote.

2. Nel caso 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 superiore ad un anno. Resta fermo quanto previsto dall'articolo 174-quinquies della citata legge n. 633 del 1941".

Con questo articolo vengono estese le fattispecie di reato presupposto L'art. 25 novies prevede, pertanto, che la Società possa essere sanzionata in relazione ai delitti in materia di violazione del diritto d'autore, così come disciplinati dalla legge 633/1941 "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" (legge sul diritto d'autore o "l.d.a.").

Il D.L. n.8 del 15 gennaio 2016 aggiunge:

È sempre ordinata la confisca degli strumenti e dei materiali serviti o destinati a commettere i reati di cui agli articoli 171-bis, 171-ter e l'illecito amministrativo di cui all'articolo 171-quater nonché delle

videocassette, degli altri supporti audiovisivi o fonografici o informatici o multimediali abusivamente duplicati, riprodotti, ceduti, commerciati, detenuti o introdotti sul territorio nazionale, ovvero non provvisti di contrassegno SIAE, ove richiesto, o provvisti di contrassegno SIAE contraffatto o alterato, o destinato ad opera diversa.

8.3.1. Messa a disposizione del pubblico di un'opera dell'ingegno protetta o di parte di essa - Art. 171, L. 633/1941 comma 1 lett a) bis

Salvo quanto disposto dall'art. 171-bis e dall'articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa.

8.3.2. Reati commessi su opera altri non destinata alla pubblicazione qualora ne risulti offeso l'onore/reputazione - Art. 171, L. 633/1941 comma 3

La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati sono commessi sopra una opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

8.3.3. Abusiva duplicazione contenuta in supporti non contrassegnati dalla SIAE - Art. 171-bis L. 633/1941 comma 1

Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

8.3.4. Riproduzione, trasferimento su altro supporto del contenuto di una banca dati - Art. 171-bis L. 633/1941 comma 2

Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante

gravità.

8.3.5. Abusiva duplicazione di opere dell'ingegno destinate al circuito televisivo, cinematografico, etc. - Art. 171-ter L. 633/1941

È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento

8.3.6. Mancata comunicazione alla SIAE dei dati di identificazione dei supporti - Art. 171-septies L. 633/1941

La pena di cui all'articolo 171-ter, comma 1, si applica anche ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

Salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

8.3.7. Fraudolenta produzione, vendita o importazione di apparati di decodifica - Art. 171-octies-L. 633/1941

Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

8.4. Le attività sensibili relative ai reati in violazione del diritto d'autore

Nell'ambito delle attività sociali che possono comportare la commissione di uno dei delitti in materia di diritto d'autore di cui all'art. 25 - novies del D.Lgs. 231/01 sono state individuate le attività sensibili che si vanno ad indicare:

1) Gestione della documentazione di proprietà delle Società Clienti

2) Gestione dei software ad uso interno
3) Gestione di immagini, musica, video per presentazioni della propria Società

La società ritiene opportuno regolamentare l'utilizzo delle proprie risorse informatiche per assicurare che in tale ambito non vengano poste in essere condotte in violazione delle norme sul diritto d'autore. Talvolta, accade che l'azienda a scopo promozionale organizzi convention o eventi, o che utilizzi per proprie pubblicazioni (ad es. pubblicità, promozioni, gadeget,…) fotografie e immagini. Anche in questi casi, è ravvisata la necessità di adottare principi e norme che assicurino la legittimità di tali attività sotto il profilo del diritto d'autore.

L'analisi del rischio della commissione dei reati di cui alla presente Sezione in relazione alle aree ed attività sensibili sopra indicate e mappate riscontra un livello di rischio BASSO in considerazione delle procedure di sicurezza informatica adottate e delle procedure in essere per la gestione delle attività promozionali/pubblicitarie, procedure attuate e verificate. La segregazione delle funzioni in essere assicura un puntuale controllo dei processi e la rilevazione di eventuali errori o anomalie.

8.5. Organi e funzioni coinvolte

Per quanto riguarda le aree sensibili riferibili all'utilizzo delle risorse informatiche, si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali

- **IT - Responsabile Informatico**
  Effettua gli ordini relativi all'acquisto ed alla sottoscrizione di nuove licenze

- **Responsabile Marketing**
  È l 'ufficio cui spetta l'organizzazione di iniziative aziendali rivolte al pubblico, gestendone gli aspetti logistici e organizzativi e in genere le attività promozionali/pubblicitarie.

8.6. Principi e norme generali di comportamento

Per ciascuna delle attività sensibili di cui alla presente Parte Speciale sono previste norme comportamentali in forza delle quali siano garantiti i seguenti requisiti:

- I software e le banche dati installati sui sistemi informativi dell'azienda siano sempre muniti di valida licenza di utilizzo
- La rete informatica aziendale ed i dati presenti nella stessa siano preservati da accessi ed utilizzi impropri;
- Sia fornito accesso da e verso l'esterno a mezzo di connessione internet esclusivamente ai sistemi informatici dei soggetti che ne abbiano effettiva necessità ai fini lavorativi;

- Sia accertato da parte della funzione competente che tutte le opere dell'ingegno utilizzate dall'azienda sotto qualsiasi forma (eventi aperti al pubblico, pubblicazioni proprie, corsi di e-learning etc.,) siano sempre utilizzate in conformità alle disposizioni in materia di diritto d'autore;
- Il personale ritenuto esposto al rischio di commissione dei reati in materia di diritto d'autore sia sempre adeguatamente formato e sensibilizzato a tenere comportamenti corretti.

Sulla base di tali principi, la presente Parte Speciale prevede l'espresso divieto a carico di tutti i destinatari 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 - novies del D.Lgs. 231/2001);
- Mettere a disposizione di terzi, riprodurre, divulgare, trasmettere o diffondere, in tutto o in parte, opere dell'ingegno tutelate dal diritto d'autore e dai diritti connessi;
- Violare i principi e le procedure aziendali previste nella presente Parte Speciale.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

- Installare sui sistemi informativi aziendali programmi per elaboratore non assistiti da valida licenza d'utilizzo;
- Scaricare sui personal computer aziendali programmi prelevati da internet o da sistemi peer to peer, anche qualora trattasi di software gratuiti (freeware) o shareware, salvo espressa autorizzazione del Responsabile informatico.

I Destinatari debbono pertanto:

- Utilizzare esclusivamente i software, le applicazioni, i files e le apparecchiature informatiche fornite dall'azienda e farlo esclusivamente per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
- Osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici ed ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'azienda;
- Rispettare le policy interne in merito ai dispositivi antintrusione e antivirus;
- Custodire le password di accesso alla rete aziendale ed alle diverse applicazioni e le chiavi/codici personali secondo criteri idonei a impedirne una facile individuazione ed un uso improprio;
- Non prestare o permettere a terzi l'uso delle apparecchiature informatiche aziendali o dell'archivio informatico della stessa, senza la preventiva autorizzazione del Responsabile informatico;
- Astenersi dall'effettuare copie non specificamente autorizzate dal Responsabile informatico di dati e di software di proprietà dell'azienda;
- Evitare di trasferire all'esterno dell'azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà interna, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;

- Qualora per la connessione alla rete internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni all'azienda, possano illecitamente collegarsi alla rete internet tramite i router della stessa e compiere illeciti ascrivibili ai dipendenti;
- Utilizzare opere dell'ingegno senza l'autorizzazione del soggetto che legittimamente ne detiene i diritti, ovvero senza aver stipulato un valido contratto di licenza.

Per ciascuna delle operazioni di carattere significativo individuate nella presente Parte Speciale sono previste specifici principi di riferimento, in forza dei quali:

- Sia previsto (compatibilmente con la normativa vigente in materia di diritto del lavoro e di diritto alla privacy) il costante monitoraggio della rete informatica interna;
- Siano adottati adeguati programmi di formazione del personale ritenuto esposto al rischio relativo ai reati di cui alla presente Parte Speciale e sia attuata una politica di sensibilizzazione di tutti gli utenti alla sicurezza informatica;
- La rete informatica dell'azienda sia dotata di adeguate protezioni, così da evitare la non corretta duplicazione, riproduzione, trasmissione o divulgazione di opere dell'ingegno protette, ed in particolare delle opere letterarie nella disponibilità dell'azienda;
- Sia prevista l'attuazione di un tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici contenuti nel sistema informativo dell'azienda;
- Sia assicurato che tutti i supporti informatici alienati o smaltiti (personal computer, floppy disc, CD o DVD, USB) siano resi illeggibili prima della loro vendita o distruzione, così da evitare l'involontaria diffusione di programmi e/o contenuti protetti;
- Sia previsto che la funzione competente, prima di utilizzare per l'attività dell'azienda un'opera coperta da diritto d'autore, si accerti di averne pieno titolo;
- Nel caso di collaborazione con agenzie di comunicazione, di pubblicità etc., sia con le stesse contrattualizzato che tutti gli adempimenti concernenti il diritto d'autore relativi all'oggetto della prestazione sono stati adempiuti da tali soggetti, che si impegnano a tenere indenne la società da qualsiasi pretesa che venisse alla stessa rivolta a tale riguardo;
- In caso di evento aperto al pubblico, sia corrisposto in favore della SIAE il compenso di legge, ove lo stesso risulti dovuto.

8.7. Principi di riferimento specifici relativi alla regolamentazione delle attività sensibili

Installazione ed utilizzo dei programmi per computer

- L'azienda assicura che su tutti i sistemi informativi in uso vengano installati esclusivamente programmi muniti di valida licenza di utilizzo ed approvati dalla società;
- Sia previsto un sistema di privilegi tale per cui l'installazione di nuovi software o applicazioni sia riservata; esclusivamente ai soggetti individuati dall'azienda;

- Sia redatta una policy relativa all'utilizzo degli strumenti informatici a cui gli amministratori di sistema dovranno attenersi;
- L'attività posta in essere dagli amministratori di sistema sia tracciabile;
- Siano utilizzati dall'azienda sistemi antivirus e firewall che blocchino il download dal web di software ed applicazioni non autorizzate;
- L'azienda verifichi con cadenza puntuale e periodica la corrispondenza delle licenze in essere con il numero di terminali nella sua disponibilità.

Acquisto di nuove licenze

- La funzione aziendale che rileva la necessità di acquistare un nuovo software o applicativo predispone un progetto esplicativo e ne chiede l'approvazione
- Il progetto viene sottoposto all'approvazione dell'amministratore unico o del responsabile informatico, a seconda dell'oggetto, del livello di spesa e della durata dell'impegno;
- L'amministratore unico concede l'autorizzazione, abilitando il servizio di spesa;
- L'installazione dei nuovi software o applicativi viene effettuata dagli amministratori di sistema del settore di competenza.

Utilizzo da parte dell'azienda di opere coperte da diritto d'autore

- La funzione competente, prima di utilizzare per l'attività dell'azienda un'opera o parte di essa coperta da diritto d'autore, si accerta di averne pieno titolo;
- La funzione competente tiene traccia scritta dell'attività di verifica di cui al punto che precede e delle sue risultanze, conservando l'eventuale documentazione rilevante;
- Nel caso di utilizzo da parte dell'azienda di agenzie di comunicazione, di pubblicità etc., per attività che coinvolgono opere protette da diritto d'autore, sia con le stesse contrattualizzato che tutti gli adempimenti concernenti il diritto d'autore relativi all'oggetto della prestazione sono stati adempiuti da tali soggetti, i quali si impegnano a tenere indenne la società da qualsiasi pretesa che venisse alla stessa rivolta a tale riguardo da terzi;
- Nel caso di intervento di professionisti esterni alle iniziative organizzate dall'azienda, sia ottenuta la loro autorizzazione scritta alla trasmissione dell'evento (ove prevista) e siano contrattualizzati con i medesimi le modalità della loro prestazione, gli eventuali limiti allo sfruttamento dell'immagine ed i relativi diritti economici.

8.8. I controlli dell'Organismo di Vigilanza

Fermo restando il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati in violazione del diritto d'autore, commessi nell'interesse o a vantaggio della società, diretti a verificare la corretta esplicazione delle stesse in

relazione alle regole di cui al presente Modello.

Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle eventuali procedure interne adottate, il rispetto delle stesse da parte di tutti i destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

L'Organismo di Vigilanza dovrà, inoltre, esaminare eventuali segnalazioni specifiche provenienti dagli organi sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

8.9. Flussi informativi all'Organismo di vigilanza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace attuazione del Modello e di curarne l'aggiornamento dovranno essere assicurati i seguenti flussi informativi periodici:

Documenti	Periodicità	Soggetto tenuto
○ Nuovi software acquistati e relative licenze	Al verificarsi della condizione	Responsabile informatico
○ Autorizzazioni utilizzo immagini/loghi aziendali per eventi e social media		Responsabile Marketing

Tutti i destinatari della presente Parte speciale sono altresì tenuti ad effettuare segnalazioni all'Organismo di vigilanza qualora rilevino eventuali non conformità relative all'applicazione del flusso; al rispetto di procedure/regolamenti; al rispetto delle disposizioni del Modello di organizzazione, gestione e controllo, del Codice etico e in generale del d. lgs. n. 231/2001 e smi.

PARTE SPECIALE

SEZIONE 9 - REATI TRIBUTARI

INDICE

9.1	La tipologia dei reati tributari (art. 25 quinquesdecies del d.lgs231/2001)	3
9.2	Principali aree di attività a rischio	7
9.3	Destinatari della parte speciale	8
9.4	Principi generali di comportamento	9
9.5	Misure specifiche di comportamento	10
9.6	Flussi informativi all'Organismo di Vigilanza	12

9.1. La tipologia dei reati tributari (art. 25 quinquesdecies del d.lgs 231/2001)

Il Decreto Legge 26 ottobre 2019, n. 124 recante "Disposizioni urgenti in materia fiscale e per esigenze indifferibili", convertito con modificazioni dalla Legge 19 dicembre 2019, n. 157 (entrata in vigore il 25 dicembre 2019) ha introdotto nel D.Lgs.n. 231/2001 l'art. 25-quinquiesdecies "Reati tributari".

Le fattispecie previste dal D. Lgs. 10 marzo 2000, n. 74 espressamente richiamate all'interno dell'art. 25-quinquiesdecies sono ascrivibili a due macrocategorie: i delitti in materia di dichiarazione e i delitti in materia di documenti e pagamento di imposte.

Nella prima categoria rientrano i seguenti reati:

1) **Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000)**

Il reato di dichiarazione fraudolenta mediante l'uso di fatture o di altri documenti per operazioni inesistenti è previsto e punito dall'art. 2, D.lgs. n. 74/2000, che punisce 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 annuali relative a dette imposte elementi passivi fittizi. In tal caso, 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.

Per dette ipotesi, la fattispecie criminosa potrebbe configurarsi nel caso in cui la Società riceva "fatture o altri documenti" a fronte di operazioni di acquisto di beni e servizi inesistenti, fatture che poi provvede a registrare nelle scritture contabili o comunque a detenere ai fini di prova nei confronti dell'Amministrazione finanziaria. In tal caso, il reato si consuma nel momento in cui la Società indica detti elementi passivi fittizi nella dichiarazione annuale.

La nozione di operazione inesistente include:

a) le operazioni mai effettuate (cosiddetta inesistenza oggettiva): che si verifica nel caso in cui la Società riceva una fattura di acquisto di un servizio o di un bene, che in realtà non ho mai acquistato;

b) le operazioni effettuate, ma per le quali è stato indicato in fattura un importo diverso, generalmente superiore (cosiddetta sovrafatturazione);

c) le operazioni effettuate ma tra parti diverse (cosiddetta inesistenza soggettiva): che si verifica nel caso in cui la Società abbia realmente effettuato l'acquisto, ma il reale fornitore risulti diverso da quello indicato nella fattura.

2) Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)

L'art. 3 del 3 del D.Lgs. n. 74/2000, punisce chi, fuori dai casi previsti dall'art. 2 (ossia dall'impiego in dichiarazione di fatture false), 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 a 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 30.000 euro;

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al 5% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a 1.500.000 euro, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al 5% dell'ammontare dell'imposta medesima o comunque a 30.000 euro.

3) Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000)

L'art. 4 del D.Lgs. n. 74/2000, punisce la condotta del soggetto che, fuori dai casi precedentemente descritti dagli artt. 2 e 3 e pertanto non con frode ma comunque volontariamente, al fine di evadere le imposte dirette o l'Iva, indica in una delle dichiarazioni annuali relative a queste imposte elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi quando congiuntamente:

a) l'imposta evasa è superiore a 100.000 euro con riferimento a ciascuna delle singole imposte;

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione anche mediante indicazione di elementi passivi fittizi è superiore al 10% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o, comunque, è superiore a 2 milioni di euro.

E' esclusa la somma dell'evasione concernente imposte diverse; il superamento del limite va verificato in relazione a ciascuna imposta considerata.

Il reato si consuma dunque attraverso la presentazione di una dichiarazione annuale relativa alle imposte dirette e IVA, indicando in essa elementi attivi divergenti da quelli reali ovvero elementi passivi fittizi, determinando un'evasione d'imposta nei limiti sopra indicati.

4) Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000)

L'art. 5 del D. lgs. n. 74/2020 punisce l'omessa dichiarazione che si può manifestare con due distinte fattispecie:

- la prima prevista dal comma 1 riguarda la condotta del soggetto che al fine di evadere le imposte sui redditi o sul valore aggiunto non presenta la dichiarazione ai fini delle imposte sul reddito o dell'Iva, pur essendovi tenuto, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila;

- la seconda prevista dal comma 1-bis la condotta del soggetto che non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

Non integrano il reato:

- la presentazione delle dichiarazioni intervenute entro 90 giorni dalla scadenza;
- la presentazione di dichiarazioni non sottoscritte da persona legittimata o non redatte su stampati conformi a quelli ministeriali prescritti.

Rientrano nella seconda tipologia, i seguenti delitti:

1) Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000)

L'art. 8 del D. lgs. n. 74/2000 punisce chiunque emette o rilascia fatture o altri documenti per operazioni inesistenti, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto.

La pena prevista è la reclusione da quattro a otto anni. Si applica la reclusione da un anno e sei mesi a sei anni se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila.

Ai fini della norma, 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) Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000)

L'art. 10 del D. lgs. n. 73/2020 punisce 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.

La condotta sanzionata è solo quella, espressamente contemplata dalla norma, di occultamento o distruzione, anche solo parziale, delle scritture contabili obbligatorie e non anche quella della loro mancata tenuta sanzionata in via amministrativa dall'art. 9 del d.lgs. n. 471 del 1997.

Il reato è integrato in tutti i casi in cui la distruzione o l'occultamento della documentazione contabile dell'impresa non consenta o renda difficoltosa la ricostruzione delle operazioni. Non si configura pertanto quando il reddito e il volume d'affari possano essere accertati tramite la documentazione restante che venga esibita o rintracciata presso la sede del contribuente oppure presso il suo domicilio ovvero grazie alle comunicazioni fiscali dello stesso contribuente stesso (dichiarazioni, bilanci depositati).

3) Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)

L'art. 11, comma 1, del D.Lgs. n. 73/2020 punisce 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.

Il comma 2 prevede un'ulteriore fattispecie delittuosa punendo chiunque, al fine di ottenere per sé 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.

La condotta penalmente rilevante può, dunque, consistere, rispettivamente:

a) nell'alienare simulatamente o nel compiere altri atti fraudolenti sui propri o su altrui beni (quindi un'attività di materiale sottrazione di disponibilità (comma 1);

b) nell'indicare, nella documentazione presentata ai fini della procedura di transazione fiscale, elementi attivi o passivi diversi da quelli reali falsificando la consistenza patrimoniale (comma 2).

In entrambi i casi si tratta di reati istantanei.

4) Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000)

L'art. 10-quater del D. Lgs. n. 74/2020 punisce 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 cinquantamila euro.

La pena è aumentata con la reclusione da un anno e sei mesi a sei anni nel caso vengano posti in compensazione crediti inesistenti per un importo annuo superiore ai cinquantamila euro.

La punibilità è esclusa quando, anche per la natura tecnica delle valutazioni, sussistono condizioni di obiettiva incertezza in ordine agli specifici elementi o alle particolari qualità che fondano la spettanza del credito.

Per il perfezionamento dei reati non basta il mancato versamento dell'imposta, ma è necessario che lo stessi risulti giustificato dalla compensazione tra i debiti ed i crediti verso l'Erario, allorché i crediti non spettino o non esistano. La compensazione è dunque l'elemento di differenziazione del reato ex art. 10-quater quater rispetto alle distinte fattispecie di omesso versamento di imposte e/o ritenute.

La fattispecie si perfeziona nel momento in cui viene presentato il modello F24 e non invece il termine entro cui presentare la dichiarazione dei redditi.

9.2. Principali aree di attività a rischio

In relazione alle tipologie di reati sopra descritte, pur dandosi atto dell'esistenza nell'organizzazione interna di BPR Group che assicura un elevato livello di presidio e una rischiosità valutata BASSA, le aree/processi ed attività aziendali ritenuti potenzialmente a rischio sono ritenuti i seguenti:

Area/Processi	Attività sensibili
OPERATION Acquisti	- Gestione del sistema di qualificazione dei fornitori - Raccolta e controllo delle richieste di acquisto - Richieste di offerte/preventivi, valutazione delle offerte,selezione dei fornitori e negoziazione - Emissione degli ordini di acquisto e stipulazione dei contratti - Verifica delle prestazioni/beni acquistati - Gestione degli acquisti urgenti e gestione dei conferimenti di incarichi a consulenti / professionisti esterni - Selezione degli appaltatori e subappaltatori e gestione dei relativi rapporti
AMMINISTRAZIONE Gestione fornitori	- Gestione anagrafica fornitori - Registrazione delle fatture e delle note di credito - Liquidazione delle fatture - Monitoraggio delle fatture da ricevere e in scadenza - Gestione delle attività di contabilizzazione degli accontipagati ai fornitori - Archiviazione della documentazione a supporto delle fatture
AMMINISTRAZIONE Gestione clienti	- Gestione anagrafica clienti - Emissione delle fatture attive - Registrazione delle fatture attive e delle note di credito - Archiviazione della documentazione a supporto delle fatture emesse

	- Registrazioni di carico e scarico merci da magazzino
AMMINISTRAZIONE Contabilità/tesoreria	- Apertura / Chiusura di conti correnti - Registrazione degli incassi e dei pagamenti in contabilità generale - Riconciliazione degli estratti conto bancari e delle operazioni - Gestione programma contabilità, archiviazione dei documenti aziendali, delle scritture contabili e dei registri fiscali obbligatori - Fatturazione elettronica
CONSULENTE ESTERNO (commercialista) Rapporti con l'Amministrazione finanziaria e altri enti di vigilanza e controllo	- Effettuazione del calcolo delle imposte dirette e indirette, esecuzione dei versamenti relativi, predisposizione e trasmissione delle relative dichiarazioni - Attività che prevedono una interazione diretta con l'Amministrazione finanziaria (svolgimento di verifiche tributarie, presentazione di interpelli, avvio di contenzioso tributario, ecc.) - Gestione dei rapporti con enti pubblici ed Autorità di Vigilanza per gli adempimenti di competenza e gestione delle eventuali verifiche / accertamenti che ne derivano.
RISORSE UMANE Gestione personale dipendente e collaboratori	- Selezione e assunzione del personale; - Gestione delle consulenze e delle prestazioni professionali (inclusa la fase di selezione e qualifica dei consulenti e di gestione dei rapporti con gli stessi); - Gestione delle missioni / trasferte - Gestione, controllo e autorizzazione delle note spese
GOVERNANCE Operazioni straordinarie	- Operazioni straordinarie - Prelievi e disposizioni dai conti correnti bancari

9.3. Destinatari della parte speciale

Le funzioni coinvolte nella gestione delle aree e processi sensibili, destinatari della presente Sezione della Parte Speciale sono:

- l'Amministratore unico
- il CFO
- il Business Developer
- il Responsabile consulenza strategica
- il Responsabile amministrativo

- il Responsabile operations
- il Responsabile engineering
- il Responsabile risorse umane
- il Consulente esterno (commercialista)
- gli incaricati alla funzione acquisti
- il Responsabile sistemi informativi, in relazione al corretto funzionamento dei presidi di sicurezza informatica,

nonché i dipendenti soggetti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio.

Tutte le funzioni coinvolte nello svolgimento delle attività a rischio individuate sono tenute ad osservare le disposizioni di legge esistenti in materia, le prescrizioni previste dal D.Lgs. 231/2001, nonché quanto previsto dal Modello di organizzazione, gestione e controllo e dal Codice Etico.

9.4. Principi generali di comportamento

I destinatari della presente Parte Speciale sono tenuti a:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge in materia tributaria e delle procedure aziendali interne, in tutte le attività finalizzate alla contabilizzazione delle fatture attive e passive, rispettivamente, emesse e ricevute dalla Società, al calcolo ed al relativo pagamento delle imposte e/o comunque riconducibili alle attività sensibili alla commissione dei reati tributari sopra individuate;
- osservare rigorosamente tutte le norme poste dalla legge in materia tributaria e di agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano;
- assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;
- osservare le regole che presiedono all'autorizzazione di operazione straordinarie e di quelle dirette a disciplinare le ipotesi di dismissione di cespiti, evitando rigorosamente di porre in essere comportamenti idonei a provocarne una diminuzione del patrimonio sociale funzionale e/o, comunque, idonea a costituire il presupposto della fattispecie penale della sottrazione fraudolenta al pagamento delle imposte;
- effettuare con tempestività, correttezza e buona fede tutti gli adempimenti tributari previsti dalla legge.

Si richiamano espressamente, per la stretta correlazione con la materia tributaria, le prescrizioni già contenute nella Sezione 3 Reati Societari.

E' fatto inoltre espressamente divieto di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione nelle dichiarazioni fiscali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà;
- porre in essere che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque costituiscano ostacolo allo svolgimento all'esercizio delle funzioni di vigilanza dell'Amministrazione finanziaria o di altre autorità di controllo;
- effettuare operazioni che, anche solo potenzialmente, siano idonee a provocarne una diminuzione del patrimonio sociale funzionale e/o, comunque, idonea a costituire il presupposto della fattispecie penale della sottrazione fraudolenta al pagamento delle imposte;
- omettere di effettuare, con la dovuta completezza e trasparenza, tutti gli adempimenti tributari previsti a carico della Società dalla normativa vigente e a collaborare, ove previsto, con l'Amministrazione finanziaria;
- esporre nelle predette dichiarazioni fiscali e trasmette all'Amministrazione finanziaria fatti non rispondenti al vero, ovvero occultare fatti rilevanti.

9.5. Misure specifiche di comportamento

CFO e Responsabile amministrativo, in collaborazione con il commercialista esterno, sono tenuti a:

- gestire puntualmente l'anagrafica clienti e fornitori;
- raccogliere i documenti fiscali predisposti dal fornitore e verificare la corrispondenza tra fattura, merce o servizio ricevuto ed ordine inviato;
- effettuare le necessarie registrazioni dei documenti fiscali ricevuti dai fornitori per le operazioni di acquisto e/o emessi per le operazioni di vendita;
- gestione delle attività di contabilizzazione degli incassi e dei pagamenti;
- effettuare periodicamente la riconciliazione degli estratti conto bancari e delle operazioni di cassa; monitorare l'utilizzo delle carte di credito che prevedono l'addebito su conto corrente aziendale;
- nell'ambito delle attività di predisposizione, approvazione e pubblicazione del bilancio, pianificare le attività necessarie alla chiusura della contabilità e alla redazione della prima bozza di bilancio da presentare all'Amministratore unico, elaborando uno scadenziario che indichi ulteriormente le attività funzionali all'accantonamento delle relative imposte;
- provvedere alla predisposizione di uno specifico documento contenente il calcolo dell'accantonato delle imposte dovute per l'anno di riferimento da presentare, unitamente alla prima bozza di bilancio di esercizio costituito da stato patrimoniale, conto economico e nota integrativa, all'approvazione dell'Amministratore Unico;

- provvedere alla valutazione della fattibilità finanziaria delle operazioni straordinarie prospettate dall'Amministratore Unico, valutando con il supporto del consulente esterno gli aspetti fiscali delle medesime;
- provvedere alla verifica della corretta identificazione, nella dichiarazione fiscale, del soggetto firmatario;
- verificare la conformità della dichiarazione effettivamente presentata con la copia cartacea conservata agli atti della società;

E' compito del Responsabile risorse umane ricevere le note spese di cui il dipendente richiede il rimborso, verificare la congruità delle spese, il rispetto delle procedure operative aziendali, l'esistenza dei documenti giustificativi e la loro corrispondenza con le spese autorizzate. Le note spese rimborsate e i relativi giustificativi sono archiviati dal Responsabile risorse umane.

Compete al Business developer ricevere le note spese di cui i collaboratori esterni richiedono il rimborso, verificare la congruità delle spese, il rispetto delle procedure operative aziendali, l'esistenza dei documenti giustificativi e la loro corrispondenza con le spese autorizzate. Le note spese rimborsate e i relativi giustificativi sono archiviati dal Business Developer.

Il Responsabile Operation, il Responsabile consulenza strategica, il Business developer e il Responsabile engineering in relazione alle attività di natura strategica e commerciale, in collaborazione con il Responsabile Amministrativo sono tenuti a:

- definire le proposte commerciali da sottoporre ai clienti;
- raccogliere e verificare la documentazione predisposta dal cliente;
- controllare che quantità e qualità dei servizi erogati corrispondano a quelli richiesti dal cliente,
- assicurare la corretta archiviazione della documentazione in collaborazione con il responsabile sistemi informativi.

Il Responsabile Consulenza strategica, il Responsabile Operation, il personale incaricato acquisti e il Responsabile qualità:

- definire le attività per le quali si rende necessaria attività di consulenza;
- definire i fabbisogni e gestire le richieste d'acquisto di beni e servizi;
- gestire e monitorare il processo di selezione e valutazione tecnico-economica dei fornitori;
- definire il corrispettivo per la fornitura dei beni o servizi richiesti nel rispetto delle procedure aziendali;
- emettere ordini di acquisto, con il supporto del responsabile amministrativo, nel rispetto delle procedure aziendali;
- conservare e archiviare, anche in collaborazione con il responsabile IT, tutta la documentazione prodotta.

È compito dell'Amministratore Unico, in collaborazione, per competenza, con il CFO, il Responsabile amministrativo, Risorse umane e Operation:

- sottoscrivere i contratti di acquisto con i fornitori;
- sottoscrivere i contratti di servizio/consulenza con i clienti;
- formalizzare e motivare la decisione della Società di concedere contributi, liberalità e sponsorizzazioni (P.A., società, non profit);
- verificare che i contratti e le proposte commerciali siano sottoscritte soltanto da soggetti aziendali formalmente autorizzati in tal senso mediante appropriata delega di funzioni o procura;
- proporre eventuali operazioni straordinarie all'Assemblea dei soci;
- autorizzare il pagamento delle note spese presentate;
- eseguire il monitoraggio delle spese di trasferta;
- firmare la copia cartacea della dichiarazione fiscale conservata agli atti della Società.
- approvare la bozza del calcolo dell'accantonato delle imposte e del bilancio di esercizio costituita da stato patrimoniale, conto economico e nota integrativa, presentate dal Responsabile Amministrativo e predisporre il progetto di bilancio da presentare all'approvazione dell'Assemblea dei Soci;
- attribuire, all'interno dell'organizzazione aziendale, eventuali poteri di firma dei contratti;
- verificare che i contratti e le proposte commerciali siano sottoscritte soltanto da soggetti aziendali formalmente autorizzati in tal senso mediante appropriata delega di funzioni o procura.

Il commercialista incaricato, in raccordo con il Responsabile amministrativo, sarà tenuto a:
- monitorare, nel corso dell'annualità, il regolare adempimento di ogni onere dichiarativo e/o versamento in materia tributaria;
- analizzare il progetto di bilancio di esercizio approvato dall'Amministratore unico da presentare all'Assemblea dei Soci;
- verificare l'adeguatezza dell'accantonamento delle imposte indicate nel progetto di bilancio.

Si rinvia espressamente ai Protocolli speciali di prevenzione allegati al presente Modello di organizzazione, gestione e controllo.

9.6. Flussi informativi all'Organismo di vigilanza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace attuazione del Modello e di curarne l'aggiornamento dovranno essere assicurati i seguenti flussi informativi periodici:

Documenti	Periodicità	Soggetto tenuto
○ Schema di bilancio in via preventiva; ○ Documento contenente il calcolo dell'accantonato delle imposte dovute per l'anno di riferimento presentato all'approvazione dell'Amministratore unico; ○ Bilancio CEE approvato e documentazione collegata; ○ Copia delle dichiarazioni fiscali presentate nel periodo di riferimento; ○ Copia degli F24 presentate nell'anno utilizzando in compensazione crediti fiscali; ○ Relazione sintetica sulle attività svolte nel periodo di riferimento con relativi controlli e segnalazioni effettuati.	Annuale	Responsabile Amministrativo

Tutti i destinatari della presente Parte speciale sono altresì tenuti ad effettuare segnalazioni all'Organismo di vigilanza qualora rilevino eventuali non conformità relative all'applicazione del flusso; al rispetto di procedure/regolamenti; al rispetto delle disposizioni del Modello di organizzazione, gestione e controllo, del Codice etico e in generale del d. lgs. n. 231/2001 e smi.

PARTE SPECIALE

SEZIONE 10 - RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, AUTORICICLAGGIO E DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

INDICE

10.1	Le fattispecie di reato	3
10.2	Aree a rischio e attività sensibili	9
10.3	Destinatari della parte speciale	10
10.4	Principi generali di comportamento	11
10.5	Compiti dell'Organismo di Vigilanza	12
10.6	Flussi informativi verso l'Organismo di Vigilanza	12

10.1. Le fattispecie di reato

Il d. lgs. 21 novembre 2007, n. 231 è intervenuto inserendo l'art. 25-octies, disposizione che estende il regime della responsabilità amministrativa delle persone giuridiche alle ipotesi di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (artt. 648, 648-bis e 648-ter del codice penale).

In particolare, al comma 1 dell'art. 25-octies è previsto che si applica all'ente la sanzione pecuniaria da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote.

Il comma 2 prevede inoltre che "nei casi di condanna per uno dei delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore a due anni".

Tra i reati presupposto l'art. 3 della legge 15 dicembre 2014, n. 186 ha inserito in reato di autoriciclaggio di cui al nuovo art. 648-ter-1 c.p.

Di seguito la breve descrizione delle fattispecie.

- Ricettazione (Art. 648 c.p.)

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

- Riciclaggio (art. 648-bis c.p.)

Oggetto della presente fattispecie è il comportamento di chi sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

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

La fattispecie sanziona la condotta di chi impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

- **Autoriciclaggio**

Il reato di autoriciclaggio è previsto dall'art. 648-ter-1 c.p. - norma introdotta dall'art. 3 della legge 15 dicembre 2014, n. 186 - e richiamato dall'art. 25-octies del d. lgs. n. 231/01, quale nuovo reato presupposto.

La norma recita:

"*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 non colposo, 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.*

Si applica la pena della reclusione da uno a quattro anni e della multa da euro 2.500 a euro 12.500 se il denaro, i beni o le altre utilità provengono dalla commissione di un delitto non colposo punito con la reclusione inferiore nel massimo a cinque anni.

Si applicano comunque le pene previste dal primo comma se il denaro, i beni o le altre utilità provengono da un delitto commesso con le condizioni o le finalità di cui all'articolo 7 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203, e successive modificazioni.

Fuori dei casi di cui ai commi precedenti, non sono punibili le condotte per cui il denaro, i beni o le altre utilità vengono destinate alla mera utilizzazione o al godimento personale.

La pena e' aumentata quando i fatti sono commessi nell'esercizio di un'attività bancaria o finanziaria o di altra attività professionale.

La pena e' diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto. Si applica l'ultimo comma dell'articolo 648".

L'autoriciclaggio è il riciclaggio di denaro di provenienza illecita, compiuto dalla stessa persona che ha ottenuto tale denaro in maniera illecita. L'autore del delitto presupposto incorre nel delitto se impiega il danaro in attività economiche, finanziarie, imprenditoriali, speculative. Non è punito, se destina tali beni alla mera utilizzazione o al godimento personale.

La normativa vigente in tema di prevenzione dei reati di riciclaggio prevede i seguenti strumenti di contrasto:

- la previsione di un divieto di trasferimento di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore in Euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione è pari o superiore al limite previsto dalla normativa vigente. Il trasferimento può tuttavia essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.a.;
- l'obbligo di adeguata verifica della clientela da parte di alcuni soggetti destinatari del d. lgs. n.

231/2007 (elencati agli artt. 11, 12, 13 e 14) in relazione ai rapporti e alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale degli stessi;

- l'obbligo degli stessi soggetti di conservare, nei limiti previsti dall'art. 36 del decreto, i documenti o le copie degli stessi e registrare le informazioni che hanno acquisito per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dall'UIF o da qualsiasi altra autorità competente;
- l'obbligo di segnalazione da parte di alcuni soggetti (elencati agli artt. 10, comma 2, 11, 12, 13 e 14 del d. lgs. n. 231/2007) all'UIF, di tutte quelle operazioni, poste in essere dalla clientela, ritenute "sospette" o quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo.

I soggetti sottoposti agli obblighi di cui ai n. 2., 3., 4., sono:
1) gli intermediari finanziari e gli altri soggetti esercenti attività finanziaria. Tra tali soggetti figurano, ad esempio:
• banche;
• poste italiane;
• società di intermediazione mobiliare (SIM);
• società di gestione del risparmio (SGR);
• società di investimento a capitale variabile (SICAV).
2) I professionisti, tra i quali si indicano:
• i soggetti iscritti nell'albo dei ragionieri e periti commerciali;
• i notai e gli avvocati quando, in nome e per conto dei loro clienti, compiono qualsiasi operazione di natura finanziaria o immobiliare e quando assistono i loro clienti in determinate operazioni.
3) I revisori contabili.
4) Altri soggetti, intesi quali operatori che svolgono alcune attività il cui esercizio resta subordinato al possesso delle licenze, autorizzazioni, iscrizioni in albi o registri, ovvero alla preventiva dichiarazione di inizio di attività richieste dalle norme. Tra le attività si indicano:
• recupero di crediti per conto terzi;
• trasporto di denaro contante;
• gestione di case da gioco;
• offerta, attraverso internet, di giochi, scommesse o concorsi pronostici con vincite in denaro.

Come emerge dall'elencazione appena riportata, BPR Group non figura tra i destinatari del d. lgs. n. 231/2007; tuttavia, gli esponenti aziendali, al pari di qualsiasi soggetto giuridico, possono

astrattamente commettere uno dei reati di riciclaggio, così come i professionisti di cui la Società di avvale.

Con il D. Lgs. 184/2021 è stato inserito nel catalogo dei reati del D. Lgs. 231/2001 l'articolo 25 octies. 1, rubricato "**Delitti in materia di strumenti di pagamento diversi dai contanti**".
Le novità legislative così introdotte - recante l'"attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio" - sono entrate in vigore il 14 dicembre 2021. Il suddetto decreto legislativo, in linea con quanto previsto nella citata Direttiva 2019/713 si pone lo scopo di contrastare le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti intervenendo sul noto e sempre più allarmante fenomeno delle azioni/attività a carattere manipolativo riguardanti gli strumenti di pagamento e i flussi monetari digitali (bancomat, carte di credito, carte ricaricabili, POS, internet banking, etc.).

Incorre nei reati contemplati dall'Art.25-octies.1, per la tutela del patrimonio oltre che per la corretta circolazione del credito:
- Chi utilizza carta di credito non essendone titolare avendola sottratta
- Chi utilizza carta di credito non essendone titolare anche avendola solo trovata
- Chi falsifica carte di credito
- Chi cede carte di credito falsificate
- Chi mette in circolazione carte di credito falsificate
- Chi procura a sé o ad altri un ingiusto profitto alterando il funzionamento di un sistema informatico.

Il reato si consuma al momento dell'utilizzo delle carte o di programmi informatici indipendentemente se c'è stato o meno il conseguimento di un profitto.

Con il D.l. 105/2023 che ha introdotto l'art. 512 bis c.p., il legislatore ha inteso sanzionare anche la condotta fraudolenta di chi trasferisce fittiziamente ad altri denaro o altri beni al fine di eludere l'applicazione della confisca e degli altri mezzi di prevenzione patrimoniale ovvero al fine di agevolare la commissione dei delitti di ricettazione, riciclaggio e autoriciclaggio. L'oggetto materiale della condotta è costituito da: - carte di credito o di pagamento o ogni alto strumento di pagamento diverso dal denaro in contanti; - apparecchiature, dispositivi o programmi informatici costruite o progettate principalmente per la commissione reati riguardanti strumenti di pagamento diversi dai contanti.

I reati contemplati nell'Art.25-octies.1 D.Lgs. n. 184 dell'8 Novembre 2021 sono i seguenti:

1) **Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493 ter c.p.)**

La norma punisce con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro "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."

Alla stessa pena soggiace "chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi".

L'art. 493 ter c.p. precisa che la falsificazione punibile riguarda non solo le "carte di credito" ma anche qualsiasi strumento di pagamento lato sensu "digitale" e diverso dal contante, di cui l'art. 1 del d. lgs. n. 184/2021 fornisce una definizione includendovi "ogni dispositivo, oggetto o record protetto, materiale o immateriale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali".

L'ampliamento dell'oggetto sembra dunque muoversi in due direzioni: da un lato, il fatto di ricomprendere i mezzi di pagamento immateriali consente di sanzionare anche le condotte aventi ad oggetto account di mezzi di pagamento digitali aventi una diffusione sempre più ampia, come Satispay o Paypal, a prescindere dall'esistenza di un documento fisico; dall'altro, lo stesso art. 1 del d. lgs. n. 184/2021, nel definire i "mezzi di scambio digitali", ricomprende anche la "valuta digitale".

Il reato si consuma nel momento in cui vengono utilizzate le carte e, rispettivamente, chi le falsifica o le cede a terzi. Non è quindi richiesta l'effettivo conseguimento di un profitto, purché venga accertato il dolo specifico. Nonostante tale anticipazione di tutela penale, il tentativo appare comunque configurabile.

Esempio

La fattispecie potrebbe venire in rilievo laddove un dipendente della Società utilizzi app di pagamento o carte di credito intestate a terzi non facenti parte dell'organizzazione aziendale, nell'interesse o vantaggio della Società stessa

2. Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493 quater c.p.)

La norma punisce con la reclusione sino a due anni e la multa sino a 1000 euro. "chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento

diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri e apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

La norma è stata introdotta per sanzionare quelle condotte "preparatorie" alla successiva utilizzazione fraudolenta dei mezzi di pagamento diversi dal contante e, quindi, i reati per i quali assume rilevanza penale la condotta tipizzata dall'art. 493 quater c.p. non possono che essere quelli di indebita utilizzazione di cui all'art. 493 ter c.p.

Le condotte punibili in particolare sono la produzione, l'importazione, l'esportazione, la vendita, il trasporto e la distribuzione di apparecchiature, dispositivi o programmi informatici per la commissione di reati riguardanti strumenti di pagamento diversi dai contanti.

Esempio
Messa a disposizione, all'interno dell'azienda, di strumenti (apparecchiature, dispositivi o programmi informatici) funzionali alla realizzazione di frodi e falsificazioni di mezzi di pagamento diversi dai contanti.

3. Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.)

Il delitto di frode informatica è stato introdotto dal D.lgs 184/2021 nel testo dell'art. 25 octies 1 quale reato presupposto, ma solo ed esclusivamente se la condotta fraudolenta risulti aggravata, a norma del comma 2 dell'art. 640 ter c.p. e, quindi, produca un trasferimento di denaro, di valore monetario o di valuta virtuale.

L'art. 640-ter c.p. punisce con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno".
La pena è aggravata se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.

3. **Trasferimento fraudolento di valori (art. 512-bis) [articolo introdotto dalla L. n. 137/2023 e modificato dal D.L. 19/2024]**

La norma punisce con la reclusione da due a sei anni

- "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".
- "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".

Esempio

Possono rientrare nella sfera di punibilità prevista dalla disposizione, ad esempio, la nomina fittizia di un prestanome come amministratore di una società, al quale sia attribuita la titolarità del conto corrente bancario della società, con potere di disporre delle risorse della medesima, ovvero, la costituzione di una nuova attività d'impresa esercitata in forma societaria con la medesima finalità richiamata dalla norma.

10.2 Aree a rischio e attività sensibili

L'attività di risk assessment ha consentito di individuare tra le attività nel cui ambito potrebbero astrattamente essere commesse le fattispecie di reato sopra richiamate le seguenti aree sensibili.

Area/Processi	Attività sensibili
AMMINISTRAZIONE	- gestione risorse finanziarie e dei flussi finanziari attivi e passivi, ivi compresa la fatturazione - tesoreria - sponsorizzazioni e liberalità - transazioni finanziarie con controparti - Utilizzo di carte di credito o carte prepagate
RISORSE UMANE Gestione personale dipendente e collaboratori	- Gestione del personale (progressioni, retribuzione, rimborsi spesa, formazione, contribuzioni obbligatorie, ecc.) - Utilizzo di carte prepagate
OPERATION Acquisti	- Acquisti - Affidamento di opere, servizi e manutenzioni

	- Conferimento di incarichi di collaborazione, incarichi professionali, consulenze
OPERATION	- Acquisizione e gestione clienti
MARKETING	- Attività promozionali/pubblicitarie
SISTEMI INFORMATIVI	- Trasferimento di denaro mediante il Sistema informativo aziendale

L'analisi del rischio della commissione dei reati di cui alla presente Sezione della Parte speciale in relazione alle aree ed attività sensibili sopra indicate e mappate riscontra un livello di rischio BASSO in considerazione dei seguenti elementi di sintesi.
BPR Group non ammette e non riceve pagamenti in contanti di alcun importo; tutti i pagamenti avvengono con sistemi tracciati. Le carte di credito e le carte prepagate in uso sono verificate dal Responsabile amministrativo. Non sono utilizzati pagamenti mediante valute digitali. La segregazione delle funzioni assicura un controllo costante dei processi interessati e delle procedure aziendali. Nella storia aziendale non si riscontrano contenziosi di natura fiscale né procedimenti giudiziari per i reati di cui trattasi.

10.3. Destinatari della parte speciale

Destinatari della presente Parte Speciale sono:
- Amministratore unico
- Responsabile amministrativo
- Responsabile risorse umane
- Responsabile marketing
- Responsabile operation
- Responsabile sistemi informativi

Tutte le funzioni coinvolte nello svolgimento delle attività a rischio individuate sono tenute ad osservare le disposizioni di legge esistenti in materia, le prescrizioni previste dal D.Lgs. 231/2001, nonché quanto previsto dal Modello di organizzazione, gestione e controllo e dal Codice Etico.

10.4. Principi generali di comportamento

I destinatari della presente Parte speciale sono tenuti a:

- rispettare il Codice Etico e le disposizioni del presente Modello di organizzazione e gestione;
- rispettare le procedure del sistema Qualità ai fini della selezione e valutazione dei fornitori, dei processi di vendita e della selezione e formazione del personale;
- assicurare lo sviluppo e la gestione operativa degli strumenti utilizzati nelle attività di contrasto al riciclaggio;
- verificare e garantire l'aggiornamento, la manutenzione e la diffusione delle liste interne di soggetti/Paesi/merci interessati da provvedimenti restrittivi;
- verificare l'attendibilità commerciale e professionale dei Fornitori, Consulenti e Partner commerciali/finanziari e, ove consentito dalla normativa vigente, scambiare le informazioni finalizzate alla completa ed adeguata conoscenza;
- garantire trasparenza e tracciabilità degli eventuali accordi/joint venture con altre imprese per la realizzazione di investimenti;
- verificare la congruità economica degli investimenti effettuati in joint venture (rispetto dei prezzi medi di mercato, utilizzo di professionisti di fiducia per le operazioni di due diligence, ecc.);
- procedere all'identificazione e registrazione dei dati delle persone fisiche e giuridiche con cui la Società pone in essere rapporti giuridici o negoziali, anche all'estero, e verificare che tali soggetti non abbiano sede o residenza ovvero qualsiasi collegamento con paesi interessati da provvedimenti restrittivi. In caso contrario, le decisioni relative devono essere assunte previa autorizzazione del Presidente, sentito l'Organismo di vigilanza;
- effettuare controlli formali e sostanziali dei flussi finanziari aziendali in entrata; tali controlli devono tener conto della sede legale della società controparte (es. paradisi fiscali, paesi a rischio terrorismo ecc.), degli Istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie;
- non accettare denaro e titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) per importi complessivamente superiori al limite previsto dalla normativa vigente, se non tramite intermediari a ciò abilitati, quali banche, istituti di moneta elettronica e Poste Italiane S.p.A.;
- mantenere evidenza, in apposite registrazioni su archivi informatici, delle transazioni effettuate su conti correnti aperti presso stati in cui permangono regole di trasparenza meno restrittive per importi superiori, complessivamente, al limite previsto dalla normativa vigente.

I destinatari della presente parte speciale sono inoltre tenuti:
- al rispetto delle procedure aziendali in ordine agli strumenti di pagamento diversi dai contanti;
- al rispetto delle deleghe e dei poteri conferiti (segregazione) in ordine ai pagamenti;

- al monitoraggio dei pagamenti effettuati mediante carte di credito e altri strumenti diversi dai contanti.

Si rinvia espressamente ai Protocolli speciali di prevenzione allegati al presente Modello di organizzazione, gestione e controllo.

10.5. Compiti dell'Organismo di Vigilanza

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della società.

I compiti dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

- proporre che vengano costantemente redatte o aggiornate le eventuali procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;
- monitorare sul rispetto delle eventuali procedure interne per la prevenzione dei reati societari. L'Organismo di Vigilanza è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

10.6. Flussi informativi verso l'Organismo di vigilanza

Al fine di consentire all'Organismo di Vigilanza di vigilare sull'efficace attuazione del Modello e di curarne l'aggiornamento dovranno essere assicurati i seguenti flussi informativi periodici:

Documenti	Periodicità	Soggetto tenuto
Oltre ai flussi informativi già previsti nelle Sezioni Reati PA e Reati Societari: ○ Aggiornamento nuove carte di credito in possesso di amministratori/responsabili/personale ○ Situazioni particolarmente rilevanti, relativamente ad eventuali uscite economiche sospette od utilizzo di strumenti di pagamento anomali; ○ Comunicazione introduzione nuovi sistemi di pagamento ○ Ogni irregolarità riscontrata nella contabilità;	Al verificarsi della condizione	Responsabile amministrativo

Tutti i destinatari della presente Parte speciale sono altresì tenuti ad effettuare segnalazioni all'Organismo di vigilanza qualora rilevino eventuali non conformità relative all'applicazione del flusso; al rispetto di procedure/regolamenti; al rispetto delle disposizioni del Modello di organizzazione, gestione e controllo, del Codice etico e in generale del d. lgs. n. 231/2001 e smi.