MODELLO di ORGANIZZAZIONE, GESTIONE e CONTROLLO

D. Lgs. 8 giugno 2001 n. 231

Edizione 13 del 23 ottobre 2026

Sommario

1.	**Definizioni**	**3**
2.	**Introduzione**	**7**
3.	**Sintesi del Decreto e Normativa Rilevante**	**8**
4.	**Funzione e adozione del Modello Organizzativo**	**12**
5.	**Gruppo Sofinter**	**14**
5.1	**La Società e il Gruppo**	**14**
5.2	**Tipologia di business e di mercato/Clienti**	**14**
5.3	**Partecipazioni**	**14**
6.	**Il Sistema Organizzativo**	**15**
6.1	**Il Sistema Organizzativo**	**15**
6.2	**Deleghe di poteri: principi ordinatori e finalità**	**15**
6.3	**Organigramma**	**16**
6.4	**Organismo di Vigilanza (OdV)**	**17**
6.4.1	**Reporting dell'Organismo di Vigilanza**	**18**
6.4.2	**Flussi informativi verso l'Organismo di Vigilanza**	**18**
6.4.3	**Whistleblowing**	**19**
7.	**Utilizzo dei sistemi di intelligenza artificiale**	**21**
8.	**Governance di sostenibilità e presidio dei rischi ESG**	**21**
8.1	**Supply chain sostenibile e CBAM**	**21**
9.	**Sistema Disciplinare**	**22**
9.1	**Principi Generali**	**22**
9.2	**Sanzioni verso i lavoratori subordinati**	**22**
9.3	**Misure nei confronti dei Dirigenti**	**22**
9.4	**Misure nei confronti degli Amministratori e dei Sindaci**	**23**
9.5	**Misure nei confronti dei Consulenti e Partners**	**23**
9.6	**Misure applicabili ai destinatari delle segnalazioni ("Whistleblowing")**	**23**
10.	**Mappatura rischi potenziali dei reati presupposto**	**24**
11.	**Aggiornamento del Modello Organizzativo**	**25**
12.	**Documenti di riferimento per la predisposizione del Modello Organizzativo**	**25**
13.	**Allegati al Modello Organizzativo**	**25**
Appendice: Evoluzione del Modello Organizzativo		**26**

1. DEFINIZIONI

***Corporate Governance (CG)*:** La *Corporate Governance* o Sistema di controllo Interno è l'insieme di regole, di ogni livello (leggi, regolamenti, procedure aziendali, etc.) che disciplina la gestione dell'impresa stessa. La CG include anche le relazioni tra i vari soggetti coinvolti (gli *stakeholders*) e gli obiettivi per cui l'impresa è amministrata. Gli *attori* principali sono gli azionisti (*shareholders*), il management e il Consiglio di Amministrazione.

Attività Sensibile: Fase di un processo in cui sono state identificate attività a rischio di commissione reato.

Codice Etico (CE): Il CE è un codice di comportamento adottato nello svolgimento delle sue attività e del proprio business. Il Codice assume – come direttive di riferimento – le leggi, le normative e i protocolli interni della Società. Il CE pertanto stabilisce – per tutti i suoi dipendenti, amministratori, organi sociali, collaboratori, fornitori ecc. – le fondamentali regole di comportamento imperniate su principi etici di correttezza, lealtà, trasparenza, onestà e riservatezza e sul rispetto e la tutela dell'ambiente, nonché della salute e sicurezza dei lavoratori e della collettività nella quale l'Impresa si trova ad operare.

Codice di Condotta Fornitori: Costituisce gli standard documentati delle aziende per i membri dei loro ecosistemi di supply chain, nonché uno strumento utile a garantire che fornitori, subappaltatori e filiali condividano i propri valori in relazione agli standard di lavoro, alla salute e alla sicurezza, agli impatti ambientali e all'etica aziendale.

***Compliance*:** È la conformità delle attività aziendali alle disposizioni legislative, normative, ai regolamenti, alle procedure ed ai codici di condotta. La *Compliance aziendale* è quindi un'attività preventiva che si preoccupa di prevenire il rischio di non conformità dell'attività aziendale alle norme e alle leggi cogenti, suggerendo – ove si riscontrino disallineamenti – le correzioni più opportune.

Consulenti: Soggetti che agiscono in nome e/o per conto della Società, in forza di un contratto di collaborazione professionale.

Dipendenti: Personale dipendente della Società il cui rapporto è regolamentato da contratto di lavoro a tempo determinato o indeterminato.

D. Lgs. 231/2001: Il Decreto Legislativo 231 del 2001 istituisce la responsabilità amministrativa degli Enti per reati posti in essere da amministratori, dirigenti e/o dipendenti nell'interesse o a vantaggio degli Enti stessi.
È pertanto rivolto a: Enti forniti di personalità giuridica, società fornite di personalità giuridica e associazioni anche prive di personalità giuridica. Fanno eccezione lo Stato, gli Enti pubblici territoriali ed Enti con funzioni di rilievo costituzionale. È esclusa la responsabilità della società qualora la persona fisica abbia commesso il reato per esclusivo vantaggio proprio o di terzi. Il Decreto ha altresì previsto che ciascuna impresa possa non incorrere nell'illecito amministrativo, adottando e facendo rispettare alla propria organizzazione, un proprio "Modello di Organizzazione, Gestione e Controllo" (Modello Organizzativo) e istituendo un Organismo di Vigilanza che attui efficacemente i controlli sul rispetto del Modello.

Persona Giuridica: Si intende un complesso organizzato di persone e di beni al quale l'ordinamento giuridico attribuisce la capacità giuridica (attitudine di un soggetto ad essere titolare di diritti e doveri) facendone così un soggetto di diritto.

Ente: Identifica la Società Giuridica e anche le organizzazioni private che non hanno ottenuto il riconoscimento e quindi non sono, di fatto, persone giuridiche (i cosiddetti enti di fatto, come i partiti politici e i sindacati).
Lo stesso dicasi per le organizzazioni pubbliche prive di personalità giuridica ma parti di un Ente Pubblico più ampio, alle quali l'ordinamento riconosce una certa autonomia. Quando l'ordinamento attribuisce ad enti, pur privi di personalità giuridica, un certo grado di autonomia patrimoniale, essi, secondo una diffusa teoria, possono comunque essere considerati soggetti di diritto.

Fattispecie di reati: Tipologia di reati identificati dal D. Lgs. 231/2001 e successive integrazioni e/o modificazioni che "non si applicano allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale".

Insider Trading: Locuzione anglosassone indicante la pratica illecita di utilizzare informazioni riservate o non ancora divulgate al mercato al fine di compiere operazioni speculative in borsa e, quindi, fare profitti illecitamente nella compravendita di titoli. L'insider trading è vietato ed è disciplinato dalla legge 157/1992 e successivi integrazioni o aggiornamenti.

Linee Guida (LG): Le Linee Guida di Confindustria forniscono le Linee Guida che una Impresa può seguire per la costruzione del proprio Modello. Le LG sono preventivamente approvate dal Ministero di Giustizia. La prima edizione delle LG è del 7 marzo 2002.

Modello Organizzativo (MO): Il "Modello Organizzativo" prevede:
- un Codice Etico, quale codice comportamentale adottato dalla Società che, elencando i principi etici, funge da premessa al Modello;
- un organigramma aziendale con l'individuazione della Direzione e dei soggetti in posizione apicale, risultando gli altri sottoposti all'altrui direzione (dipendenti e collaboratori);
- un'analisi del rischio (mediante mappatura dei processi e analisi delle singole aree di rischio, con l'individuazione di cariche e funzioni che dirigono l'attività d'impresa);
- una formulazione di direttive aziendali vincolanti (procedure che individuano attività, responsabilità e relativi controlli);
- l'individuazione di un Organismo di Vigilanza (OdV) che vigila sull'applicazione del Modello;
- l'individuazione e pianificazione delle modalità di controllo preventivo (piani di audit);
- l'individuazione di un sistema disciplinare per le inosservanze del CE e del Modello.

OHSAS 18001: Norma che supporta le aziende a formulare obiettivi e politiche a favore della Sicurezza e della Salute dei Lavoratori (SSL), secondo quanto previsto dalle normative vigenti e in base ai pericoli ed ai rischi potenzialmente presenti sul posto di lavoro.

Organi sociali: Consiglio di Amministrazione, Collegio Sindacale.

Organismo di Vigilanza (OdV): Organismo di una società, nominato dal CdA, e dotato di poteri di iniziativa e controllo, a cui viene affidato il compito di vigilare sul funzionamento e l'osservanza del CE e del Modello e di curarne l'aggiornamento e la diffusione (ex D. Lgs. 231/2001 e LG).

Parte Speciale: Guida di approfondimento, facente parte del Modello Organizzativo, sui reati previsti dal D. Lgs. 231/2001 e sulle aree aziendali a rischio potenziale.

Personale: I Dipendenti, i membri del Consiglio di Amministrazione, i componenti del Collegio Sindacale, i componenti dell'OdV.

Procuratori: Persone a cui la Società ha conferito poteri ai fini gestionali; contraggono impegni per la Società con terze parti.

Pubblica Amministrazione (PA): La P.A. costituita da enti pubblici, privati concessionari di servizi pubblici, imprese pubbliche e organismi di diritto pubblico che sono chiamati ad operare, in relazione all'ambito di attività considerato, nell'esercizio di una pubblica funzione.

Pubblico ufficiale (art. 357 c.p.): sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autorizzativi, e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autorizzativi o certificativi. In senso estensivo si include nella nozione di Ente Pubblico e di Pubblico Ufficiale anche enti (e conseguentemente le persone che ne fanno parte) che svolgono servizi di pubblica utilità (Enel, Telecom, Aziende Municipalizzate, ecc.), ancorché regolate da norme di diritto privato.

Reati: Tipologia di reati contemplati nel D. Lgs. 231/2001 e successive integrazioni.

Reg. CE 761/01 EMAS: È l'acronimo di *Environmental Management and Audit Scheme*, ovvero "Sistema di Eco-Gestione ed Eco-Audit ambientale".

Rischio/i: La combinazione della probabilità di un evento e delle sue conseguenze. I processi d'impresa sono finalizzati a gestire in modo integrato i rischi e la loro analisi deve essere, per quanto possibile, riferita ad un modello generale dei rischi d'impresa che deve essere dettagliato e personalizzato sulla specifica realtà aziendale. In generale, i rischi più ricorrenti possono essere classificati in rischi gestionali (impegni contrattuali, ecc.), rischi strategici (struttura organizzativa, joint ventures, alleanze, ecc.), rischi finanziari (gestione fiscale, riciclaggio, pagamenti, ecc.) e rischi esterni (leggi e regolamenti, concorrenza, ecc.).

SA 8000: La norma SA 8000 (*Social Accountability* – Responsabilità Sociale d'Impresa) è uno standard internazionale, elaborato nel 1997 dall'ente americano SAI, che contiene i requisiti sociali di quelle organizzazioni che volontariamente forniscono garanzia di eticità della propria 'filiera produttiva' e del proprio ciclo produttivo. SA 8000 è basata sulle convenzioni dell'ILO, sulla Dichiarazione Universale dei Diritti Umani, sulle Convenzioni delle Nazioni Unite.

Soggetti Apicali: Soggetti che rivestono funzione di rappresentanza, di amministrazione e di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione ed il controllo della stessa.

***Stakeholders*:** Sono tutti quei soggetti "portatori di interessi" che operano di concerto con la Società. Tra questi si individuano i Soci, i Dipendenti e Collaboratori, i Clienti, i Fornitori, i Partners, i Finanziatori, i Concorrenti, lo Stato con le sue Pubbliche Amministrazioni e la collettività in senso lato.

UNI EN ISO 14001: La norma è uno strumento internazionale che specifica i requisiti di un sistema di gestione ambientale. Viene rilasciata da un organismo indipendente accreditato che verifica l'impegno concreto nel minimizzare l'impatto ambientale dei processi, prodotti e servizi, attestando con il marchio ISO 14001 l'affidabilità del SGA (Sistema di Gestione Ambientale) applicato.

2. INTRODUZIONE

Nel 2004 Sofinter S.p.A. ha aderito volontariamente a quanto stabilito dal Decreto Legislativo 231 dell'8 giugno 2001 adottando il Codice Etico ed il Modello Organizzativo di Gestione e Controllo.
Nel 2008 il Modello è stato ampiamente rivisto sia per recepire quanto ulteriormente legiferato, sia per essere adeguato alle evoluzioni organizzative di Sofinter, perseguendo anche l'obiettivo di rafforzare incisivamente il sistema di *governance*, sottoponendo preventivamente ad attenta verifica l'individuazione delle aree a rischio potenziale.
Nel corso degli anni il Modello è stato aggiornato con l'introduzione dei nuovi reati previsti dalla normativa 231 e con le modifiche della struttura organizzativa aziendale adottate dalla Società.
Il Modello Organizzativo è composto da una Parte Generale, nella quale si definiscono i criteri e le linee di metodo sviluppate successivamente nella Parte Speciale per tipologia di reato e nei relativi Protocolli, diretti a regolamentare lo svolgimento delle attività a rischio, nonché le regole dirette a programmare la formazione delle decisioni in relazione ai singoli reati da prevenire.

Sofinter si impegna al tempestivo aggiornamento del Modello nel caso in cui si dovessero evidenziare inadeguatezze – anche solo parziali – tali da pregiudicare un'efficace prevenzione dei rischi, o qualora intervenissero apprezzabili mutamenti o modifiche al sistema normativo e regolamentare di riferimento, alla struttura societaria e all'organizzazione della Società.

Il compito di vigilare sul funzionamento e l'osservanza del predetto Modello e di curarne l'aggiornamento è stato affidato ad un Organismo di Vigilanza, nominato dal Consiglio di Amministrazione, la cui composizione viene puntualmente comunicata successivamente alla nomina.

L'Amministratore Delegato

3. SINTESI DEL DECRETO E NORMATIVA RILEVANTE

Il Decreto Legislativo n. 231 dell'8 giugno 2001 ha introdotto nell'ordinamento italiano un regime di responsabilità amministrativa (equiparabile sostanzialmente alla responsabilità penale) a carico delle persone giuridiche che va ad aggiungersi alla responsabilità della persona fisica che ha realizzato materialmente i reati e che mira a coinvolgere nelle sanzioni le persone giuridiche (Società ed Enti).
La responsabilità amministrativa dell'Ente per la commissione di uno dei Reati previsti dal Decreto si aggiunge, e non si sostituisce, a quella (penale o amministrativa) della persona fisica che è l'autore dell'illecito. La responsabilità dell'Ente sussiste anche se l'autore del reato non è stato identificato oppure il reato medesimo sia estinto nei confronti del reo per una causa diversa dall'amnistia.
L'Ente non può essere chiamato a rispondere della realizzazione di qualsiasi fatto costituente reato, ma solo della commissione di reati e di illeciti amministrativi tassativamente previsti dal decreto, nella formulazione risultante dal suo testo originario e dalle successive integrazioni, nonché dalle leggi che espressamente lo richiamano.
La responsabilità dell'Ente sorge qualora il fatto illecito sia stato commesso nell'interesse dell'Ente ovvero per favorire l'Ente, senza che sia in alcun modo necessario il conseguimento effettivo e concreto dell'obiettivo.
L'illecito deve inoltre essere stato realizzato da uno o più soggetti qualificati, appartenenti a una delle seguenti categorie:

- i c.d. *"Apicali",* 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, quali, ad esempio, il legale rappresentante, l'amministratore, il direttore generale o il direttore di una sede o filiale;
- i c.d. "*Subalterni*", persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali che, si segnala, possono anche non coincidere con il personale dipendente.

Per i reati commessi da soggetti in posizione «apicale», è stabilita una presunzione relativa di responsabilità dell'Ente, dal momento che si prevede l'esclusione della sua responsabilità solo se esso dimostra che – prima della commissione del reato – abbia adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo e una serie di provvedimenti specifici idonei a prevenire la commissione di reati della specie di quello che è stato realizzato.
Per i reati commessi da soggetti in posizione «subordinata», l'Ente può essere chiamato a rispondere solo qualora si accerti che «la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza».

I reati presupposto contemplati dal Decreto, sono i seguenti:
Art. 24: *"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"* [articolo modificato dalla L. 161/2017 e dal D. Lgs. n. 75/2020];
Art. 24-bis: *"Delitti informatici e trattamento illecito di dati"* [articolo aggiunto dalla L. n. 48/2008; modificato dal D. Lgs. n. 7 e 8/2016, dal D.L. n. 105/2019 e dalla L. n. 90 del 28 giugno 2024];
Art. 24-ter: *"Delitti di criminalità organizzata"* [articolo aggiunto dalla L. n. 94/2009 e modificato dalla L. 69/2015];
Art. 25: *"Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione"* [modificato dalla L. n. 190/2012, dalla L. 3/2019 e dal D. Lgs. n. 75/2020. Rubrica modificata, unitamente al testo, dalla legge di conversione n. 112 dell'8 agosto 2024];
Art. 25-bis: *"Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni*

di riconoscimento" [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];
Art. 25-bis-1: *"Delitti contro l'industria e il commercio"* [articolo aggiunto dalla L. n. 99/2009];
Art. 25-ter: *"Reati societari"* [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 del 2 marzo 2023];
Art. 25-quater: *"Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali"* [articolo aggiunto dalla L. n. 7/2003];
Art. 25-quater-1: *"Pratiche di mutilazione degli organi genitali femminili"* [articolo aggiunto dalla L. n. 7/2006];
Art. 25-quinquies: *"Delitti contro la personalità individuale"* [articolo aggiunto dalla L. n. 228/2003; modificato dalla L. n. 199/2016];
Art. 25-sexies: *"Reati di Abusi di mercato"* [articolo aggiunto dalla L. n. 62/2005];
"Altre fattispecie in materia di abusi di mercato" (Art. 187-quinquies TUF) [articolo modificato dal D. Lgs. n. 107/2018];
Art. 25-septies: *"Omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro"* [articolo aggiunto dalla L. n. 123/2007; modificato L. n. 3/2018];
Art. 25-octies: *"Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio"* [articolo aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014 e dal D. Lgs. n. 195 dell'8 novembre 2021];
Art. 25-octies 1: *"Illeciti in materia di mezzi di pagamento diversi dai contanti e trasferimento fraudolento di valori"* [articolo aggiunto dal D. Lgs. 184/2021 e modificato dal D.L. 10 agosto 2023 n. 105];
Art. 25-octies 2: *"Reati in materia di violazione di misure restrittive dell'Unione Europea"* [articolo aggiunto da D. Lgs. n. 211 del 30 dicembre 2025];
Art. 25-novies: *"Delitti in materia di violazione del diritto d'autore"* [articolo aggiunto dalla L. n. 99/2009];
Art. 25-decies: *"Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria"* [articolo aggiunto dalla L. n. 116/2009];
Art. 25-undecies: *"Reati Ambientali"* [articolo aggiunto dal D. Lgs. n. 121/2011, modificato dalla L. n. 68/2015, modificato dal D. Lgs. n. 21/2018];
Art. 25-duodecies: *"Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare*" [articolo aggiunto dal D. Lgs. n. 109/2012, modificato dalla Legge 17 ottobre 2017 n. 161];
Art. 25-terdecies: *"Razzismo e xenofobia"* [articolo aggiunto dalla Legge 20 novembre 2017 n. 167, modificato dal D. Lgs. n. 21/2018];
Art. 25-quaterdecies: *"Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati"* [articolo aggiunto dalla L. n. 39/2019];
Art. 25-quinquiesdecies: *"Reati tributari"* [articolo aggiunto dalla L. n. 157/2019, dal D. Lgs. n. 75/2020 e dal D. Lgs. 156/22];
Art. 25-sexiesdecies: *"Contrabbando"* [articolo aggiunto dal D. Lgs. n. 75/2020 e modificato nel testo dal D. Lgs. 141/24];
Art. 25-septiesdecies: *"Delitti contro il patrimonio culturale"* [Legge 9 marzo 2022 n. 22];
Art. 25-duodevicies: *"Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici"* [Legge 9 marzo 2022 n. 22];
Art. 25-undevicies: *"Disposizioni in materia di Delitti contro gli animali"* – [Articolo aggiunto da L. n. 82 del 06 giugno 2025];
Art. 25-vicies: *"Reati commessi con l'uso di intelligenza artificiale"* – [Articolo aggiunto dal D. Lgs.

n. 160 del 9 settembre 2026];
Art. 26: *"Delitti tentati"*;
L. n. 9 del 2013, art. 12 *"Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato"* [Costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva];
Legge 16 marzo 2006 n. 146 *"Reati transnazionali"* [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale].

Le ipotesi di reato di cui sopra sono state riprese nella Parte Speciale che è parte integrante del Modello.
L'Ente può essere considerato responsabile, in Italia, per la commissione all'estero di taluni reati, purché nei suoi confronti non procedano le Autorità dello Stato del luogo in cui è stato commesso il fatto.
Il legislatore al fine di assicurare uno strumento sanzionatorio "effettivo, proporzionato e dissuasivo" ha stabilito due tipologie principali di sanzioni: pecuniarie ed interdittive.
La sanzione pecuniaria è determinata dal giudice attraverso un sistema basato su «quote». Ogni illecito prevede un minimo ed un massimo di quote in base alla gravità del fatto, il cui valore monetario è poi determinato dal giudice, tenuto conto delle condizioni «economiche e patrimoniali dell'ente», in termini tali da assicurare efficacia alla sanzione.
Il sistema delle quote rimane il meccanismo tradizionale, ma dal 2026 è stato introdotto un innovativo metodo di calcolo basato su percentuali del fatturato globale dell'ente per alcune tipologie di reati.
Il metodo proporzionale (1%–5% del fatturato globale) è stato introdotto dal D. Lgs. 211/2025 per i reati legati alle violazioni delle misure restrittive UE.
Le sanzioni interdittive si applicano **in aggiunta** alle sanzioni pecuniarie. Sono applicate nei casi più gravi e possono compromettere la continuità operativa dell'ente.
Possono durare da tre mesi a due anni, salvo aggravanti specifiche, possono essere applicate anche in via cautelare e possono prevedere:
1. l'interdizione, temporanea o definitiva, dall'esercizio dell'attività;
2. la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
3. il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
4. l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
5. il divieto, temporaneo o definitivo, di pubblicizzare beni o servizi.

Oltre alle sanzioni pecuniarie e alle sanzioni interdittive, sono previste altre due sanzioni:
- la confisca, che consiste nell'acquisizione da parte dello Stato del prezzo o del profitto del reato;
- la pubblicazione della sentenza di condanna a spese dell'Ente.

La Società può essere esonerata dalla responsabilità amministrativa (articoli 6 e 7 del Decreto) se:
- il soggetto ha agito nell'esclusivo interesse proprio o di terzi (quindi non nell'interesse della Società)

oppure
1. l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire il compimento dei reati;
2. il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un Organismo di Vigilanza nominato dalla Società, dotato di autonomi poteri di iniziativa e di controllo;
3. le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione,

gestione e controllo; non vi è stata omessa (o insufficiente) vigilanza da parte dell'Organismo di Vigilanza.

La Società dovrà quindi aver adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione degli illeciti.

Tali modelli, per essere idonei a prevenire il rischio della realizzazione degli illeciti, devono rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito possono essere commessi i reati;
- prevedere specifici protocolli, ovvero elementi organizzativo - procedurali, diretti a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire (sistema di poteri e deleghe, iter autorizzativi, procedure operative);
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- provvedere agli obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- adottare un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure adottate dal Modello di organizzazione, gestione e controllo.

L'ambito di applicazione dell'impianto sanzionatorio previsto dal D. Lgs. 231/2001 opera anche nel caso in cui il reato sia rimasto a livello di tentativo (art. 26 del Decreto). Infatti, la responsabilità dell'impresa può ricorrere anche se il delitto presupposto si configura nella forma del tentativo, vale a dire quando il soggetto agente compie atti idonei in modo non equivoco a commettere il delitto e l'azione non si compie o l'evento non si verifica (art. 56 c.p.).

In tal caso le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà. Inoltre, l'ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento.

4. FUNZIONE E ADOZIONE DEL MODELLO ORGANIZZATIVO

La Società intende operare secondo principi etici diretti ad improntare lo svolgimento dell'attività, il perseguimento dello scopo sociale e la crescita della Società e del Gruppo nel rispetto delle leggi vigenti.
A tal fine si è dotata di un Codice Etico di Gruppo, volto a definire i principi di deontologia aziendale che la Società riconosce come propri e dei quali esige l'osservanza, e di un Codice di Condotta Fornitori, che delinea le aspettative di base per la condotta commerciale dei fornitori in relazione al lavoro e ai diritti umani, alla salute e alla sicurezza, alla tutela dell'ambiente, alle leggi e all'etica. La Società è, inoltre, sensibile alle aspettative dei propri azionisti in tema di correttezza e trasparenza nella conduzione degli affari ed è consapevole, al fine di assicurare tali condizioni, dell'opportunità di integrare nel proprio sistema di controllo interno, un Modello di organizzazione, gestione e controllo per la prevenzione dei reati, tenendo presenti le prescrizioni del Decreto e le Linee Guida elaborate da Confindustria.
Tale iniziativa, unitamente all'adozione del Codice Etico e del Codice di Condotta Fornitori, è stata assunta nella convinzione che possa costituire un valido strumento di sensibilizzazione nei confronti di tutti i dipendenti della Società e di tutti gli altri soggetti alla stessa cointeressati (Clienti, Fornitori, Partner, collaboratori esterni, ecc.), affinché vengano seguiti comportamenti corretti e lineari tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.
Mediante il Modello Organizzativo la Società si propone di perseguire le seguenti principali finalità:

1. prevenire il rischio di commissione dei reati;
2. sensibilizzare coloro che operano in nome e per conto della Società affinché ogni attività sia caratterizzata da principi di trasparenza, correttezza e rispetto delle procedure (controllo interno);
3. diffondere la consapevolezza del rischio di incorrere, in caso di violazione delle disposizioni ivi riportate, in infrazioni disciplinari adeguatamente sanzionate;
4. ribadire che la Società considera inammissibile qualsiasi comportamento contrario a disposizioni di legge e ai principi etici a cui la Società si ispira.

I punti cardine del Modello Organizzativo sono:

- l'individuazione delle aree/processi di rischio potenziale di commissione reati nell'attività aziendale;
- la definizione di un sistema normativo interno diretto a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai rischi/reati da prevenire tramite:
  - un Codice Etico, che fissa i principi e i valori della Società;
  - un Codice di Condotta Fornitori, che aiuta la Società a garantire che fornitori, subappaltatori e filiali condividano i propri valori in relazione agli standard di lavoro, alla salute e alla sicurezza, agli impatti ambientali e all'etica aziendale;
  - un sistema di deleghe di funzioni e di procure per la firma di atti aziendali che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;
- la determinazione di una struttura organizzativa coerente volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara e organica attribuzione dei compiti e applicando una giusta segregazione delle funzioni;
- l'individuazione dei processi di gestione e controllo delle risorse finanziarie nelle attività a rischio di reato;
- l'attribuzione all'OdV del compito di vigilare sul funzionamento e sull'osservanza del Modello Organizzativo e di proporne l'aggiornamento;

- ai sensi del Decreto – art 6 e 7 – la costruzione di un Sistema Disciplinare per la violazione delle regole di condotta del Codice Etico e del Modello a prescindere dal giudizio penale.

La Società ha scelto di strutturare il proprio Modello Organizzativo con una prima parte ove sono richiamati i riferimenti legislativi, una seconda parte che identifica la Società in termini di struttura societaria ed organizzazione adottata, una terza parte ove vengono illustrate le componenti essenziali del Modello Organizzativo con particolare riferimento all'Organismo di Vigilanza, la formazione del personale e la diffusione del Modello Organizzativo nel contesto aziendale, il sistema disciplinare nonché le aree di rischio identificate ed infine un'ultima parte dove vengono analizzati i possibili reati commissibili in azienda.

Al Modello Organizzativo sono associati i protocolli che definiscono norme, procedure o prescrizioni operative adottate per ogni singola tipologia di ipotesi di reato.

5. GRUPPO SOFINTER

5.1 La Società e il Gruppo

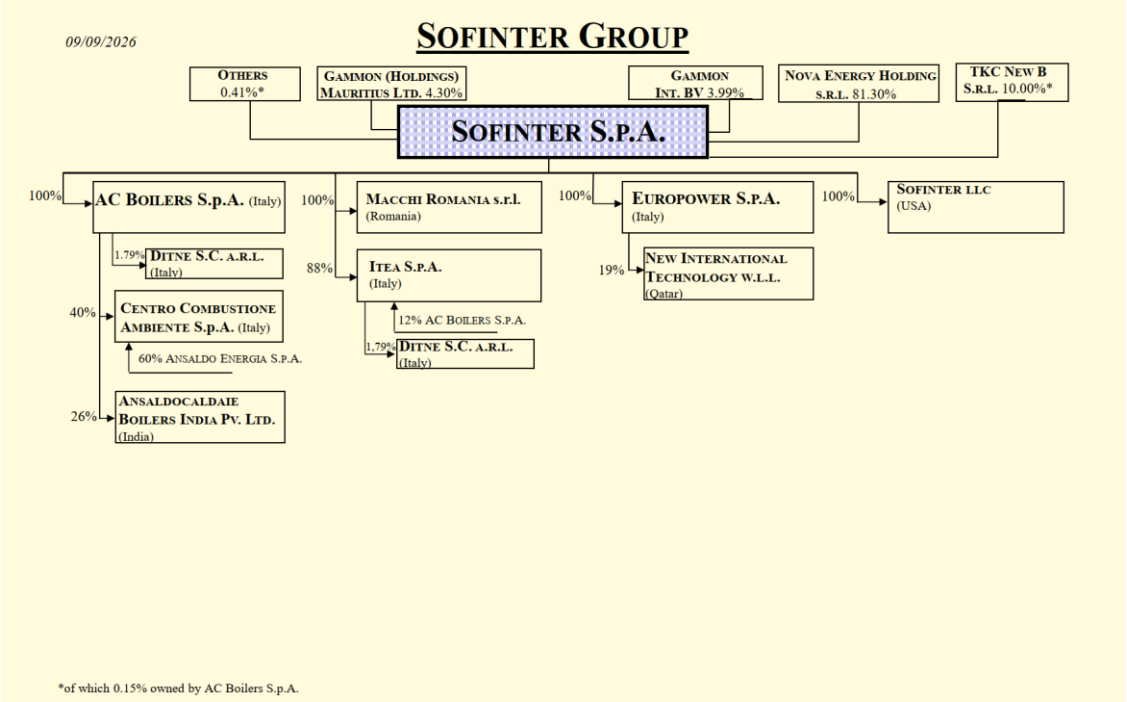
Sofinter e le società del Gruppo operano direttamente, attraverso controllate e collegate e attraverso partnership, nei mercati di riferimento. I rispettivi statuti delle singole società elencano dettagliatamente le attività che costituiscono l'oggetto sociale, il tutto in osservanza delle prescrizioni, limitazioni e divieti previsti e stabiliti dalle disposizioni legislative ed attuative di tempo in tempo vigenti. Essa inoltre può operare nei confronti dei propri Clienti tramite Raggruppamenti Temporanei di Impresa, Joint Venture, Accordi di Collaborazione, Consorzi e altre forme di partnership. Per quanto di sua competenza la Società si impegna ad applicare a tali Enti il presente Modello e a comunicarlo ai propri Partner. Essa, inoltre, si impegna a promuovere l'adozione di analoghi modelli organizzativi nei confronti delle società controllate.
La composizione del Gruppo Sofinter è rappresentata nello schema sotto riportato.

5.2 Tipologia di business e di mercato/Clienti

I *prodotti* della Società sono principalmente: caldaie industriali, caldaie a recupero su turbine a gas, caldaie a recupero su processo, service e ricambi e impianti di trattamento acque.
I *mercati* sono principalmente: Italia ed Europa, Sud America, Nord America, Nord Africa e Medio/Estremo Oriente.
I *Clienti* sono principalmente: società petrolifere, società EPC (Engineering Procurement Construction), società IPP (Independent Power Producers), enti pubblici, municipalizzate e aziende statali, *plant manufacturers*.

5.3 Partecipazioni

Non vengono rappresentati i RTI, le JV e gli altri accordi di collaborazione in quanto legati all'esecuzione di singole commesse o progetti, ovvero in quanto temporanei e/o privi di personalità giuridica; non vengono altresì rappresentate le *branches*, le stabili organizzazioni e le rappresentanze fiscali in quanto diretta emanazione della Società e/o privi di personalità giuridica.



6. IL SISTEMA ORGANIZZATIVO

6.1 Il Sistema Organizzativo

Il sistema organizzativo aziendale individua e definisce le cariche, le mansioni e le responsabilità delle funzioni aziendali, stabilendo le attribuzioni di responsabilità e le linee di raccordo gerarchico e funzionale (ove necessario) tra ogni settore e ogni livello della Società.
Il sistema organizzativo aziendale è rappresentato dall'organigramma aziendale di seguito riportato la cui descrizione viene riportata nel Sistema Qualità.
Ai fini dell'efficacia del presente Modello, è obiettivo peculiare della Società garantire una estesa e corretta divulgazione del Codice Etico, del Codice di Condotta Fornitori, della conoscenza verso tutti i dipendenti della normativa relativa al D. Lgs. 231/01 e del Modello Organizzativo e Procedure adottate nonché dei loro aggiornamenti nel tempo; a tale scopo vengono periodicamente programmati incontri formativi in conformità alla specifica procedura.
I dipendenti sono tenuti pertanto a conoscere ed osservarne il contenuto sia del Codice Etico che del Modello Organizzativo ed a contribuire per la sua concreta attuazione ed al suo effettivo funzionamento.

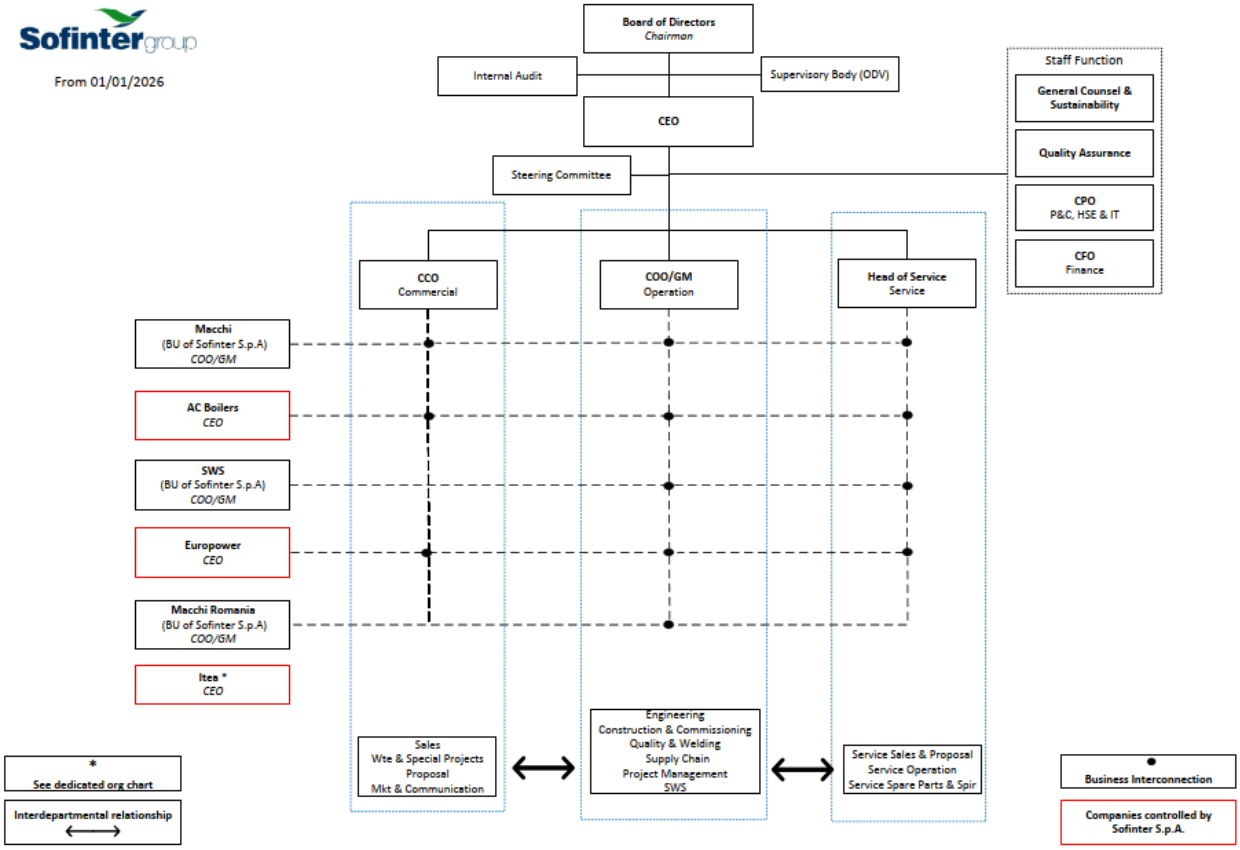
6.2 Deleghe di poteri: principi ordinatori e finalità

Il sistema dei poteri e delle deleghe tiene conto dei principi dettati dal D. Lgs. 231/01 quali:

- La separazione delle funzioni;
- La chiara individuazione delle responsabilità attribuite;
- Le linee di subordinazione gerarchica;
- Necessità di presidio territoriale;
- Il conferimento di poteri autorizzativi e di firma per valori prefissati (importi e condizioni).

I poteri e le deleghe assegnate sono limitati a responsabili gestionali, ai direttori tecnici e ai responsabili della sicurezza aziendale.

6.3 Organigramma



La struttura organizzativa della Società, e più in generale del Gruppo Sofinter, ha subito un processo di ottimizzazione con lo scopo di favorire sinergie operative e l'ottimizzazione gestionale.
In particolare:

1. A supporto delle società del Gruppo operano le seguenti funzioni di staff fornite dalla Capogruppo:

- Internal Audit;
- General Counsel & Sustainability (Corporate, Insurance and Compliance, Litigation and Contracts, Export Control e Claims & Contract Management, Sustainability);
- Quality Assurance;
- CPO (People & Culture, HSE & IT);
- CFO (Finance: Controlling Romania & minors, Consolidation, Controlling, Treasury & networking Capital).

2. Le seguenti funzioni sono state centralizzate:

- Commercial (Sales, Wte & Special Projects, Proposal, Mkt & Communication);
- Operation (Engineering, Construction & Commissioning, Quality & Welding, Supply Chain, project Management, SWS);
- Service (Service Sales & proposal, Service Operation, Service Spare Parts & Spir).

6.4 Organismo di Vigilanza (OdV)

La Società ha definito che l'OdV sia composto da un minimo di tre ad un massimo di cinque componenti che saranno nominati dal Consiglio di Amministrazione; a valle dell'accettazione formale dei soggetti nominati, viene data comunicazione per mezzo di un apposito ordine di servizio. Sarà causa di ineleggibilità a componente dell'OdV la sentenza di condanna (o di patteggiamento) anche non irrevocabile per avere commesso uno dei reati di cui al D. Lgs. 231/2001 ovvero la condanna (o patteggiamento) ad una pena che comporta l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche o delle imprese.

I componenti dell'OdV nominati dalla Società in base all'art. 6 del D. Lgs. 231/01 e alle Linee Guida – Confindustria, debbono essere individuati in base ai seguenti requisiti:

Onorabilità e moralità

I componenti dell'OdV dovranno presentare dichiarazioni di onorabilità secondo le normative vigenti.

Autonomia e Indipendenza

L'OdV dovrà essere autonomo e indipendente e non dovrà essere direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo in quanto sarebbe posto in dubbio l'obiettività di giudizio nelle verifiche di comportamento e sull'efficacia del Modello.

Professionalità

L'OdV dovrà avere competenze tecnico – professionali adeguate a poter svolgere efficacemente l'attività assegnata. Si tratta di tecniche specialistiche proprie di chi svolge questa attività, quali le capacità di analisi e valutazione dei rischi aziendali e delle misure del loro contenimento, dell'individuazione dei punti di debolezza dei processi e delle relative procedure, nonché le metodologie per l'individuazione delle frodi, ecc.

Tali tecniche devono essere applicate sia in via preventiva al fine di adottare le misure più idonee per prevenire con ragionevole certezza la commissione dei reati medesimi, sia a posteriori per accertare il compimento eventuale del reato. Nell'ambito del ruolo ricoperto dai componenti dell'OdV, la società chiede la **continuità d'azione** relativamente alla vigilanza costante sull'efficacia del Modello Organizzativo, sulla continua attuazione e aggiornamento dello stesso. L'OdV deve inoltre fornire pareri consultivi sulla costruzione del Modello Organizzativo affinché vengano evidenziati eventuali punti di debolezza; il parere consultivo non intacca l'indipendenza e l'obiettività di giudizio negli specifici eventi.

L'OdV si potrà avvalere della Funzione *Internal Audit* per effettuare le attività di verifica e controllo previste dal Modello Organizzativo, nonché delle funzioni aziendali che di volta in volta si potranno rendere utili allo svolgimento delle attività che richiedono contenuti professionali specifici. I compiti che l'OdV dovrà svolgere sono:

a) verificare l'applicazione del Modello Organizzativo relativamente alle diverse tipologie di reato;
b) valutare e monitorare l'efficacia del Modello Organizzativo relativamente alla sua capacità di prevenire la commissione dei reati;
c) proporre all'Amministratore Delegato ed al Consiglio di Amministrazione, ove necessario, l'aggiornamento e le modifiche al Modello Organizzativo stesso in relazione alla mutata normativa ed alle mutate condizioni aziendali;
d) monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello.

Sul piano operativo l'attività dell'OdV consiste nel:

- definire un piano di intervento di verifiche periodiche mirate alle attività a rischio come definite nel Modello Organizzativo;

- raccogliere e conservare le informazioni rilevanti nel rispetto del Modello Organizzativo nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse all'OdV;
- condurre le indagini interne necessarie all'accertamento di presunte violazioni portate all'attenzione dell'OdV da segnalazioni o emerse nel corso delle attività di verifica;
- verificare periodicamente la mappa delle aree a rischio di reato al fine di adeguarla ai mutamenti delle attività e dell'organizzazione dell'azienda;
- riferire periodicamente, almeno annualmente, all'Amministratore Delegato ed al Collegio Sindacale in merito all'attuazione delle politiche aziendali per l'attuazione del Modello Organizzativo.

Al fine della mappatura dei rischi (Matrice Reati 231), il *management* deve segnalare all'OdV eventuali situazioni che espongono la Società a rischio di reato. Al fine di poter svolgere i compiti sopra descritti, l'OdV:

- ha accesso ai documenti aziendali al fine di poter effettuare le verifiche necessarie, senza la preventiva autorizzazione da parte degli uffici di riferimento competenti;
- si può avvalere delle risorse professionali adeguate e disporre delle risorse finanziarie necessarie;
- si può avvalere del supporto delle varie strutture aziendali che possono essere coinvolte nella attività di controllo.

L'OdV si dota di un proprio Regolamento di funzionamento, approvandone i contenuti e presentandolo al CdA nella prima seduta utile successiva alla nomina.

6.4.1 Reporting dell'Organismo di Vigilanza

Il reporting dell'Organismo di Vigilanza viene effettuato nei confronti degli Organi Societari attraverso due linee:

- la prima, su base continuativa, direttamente con l'Amministratore Delegato;
- la seconda, su base annuale, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale. Ogni anno l'OdV trasmette al Consiglio di Amministrazione un rapporto scritto sull'attuazione del Modello Organizzativo nella Società, richiedendo l'assegnazione di un budget adeguato allo svolgimento delle attività di vigilanza, da gestire in piena autonomia.

L'OdV potrà essere convocato in qualsiasi momento dagli Organi Societari o potrà a sua volta presentare richiesta in tal senso per riferire in merito a situazioni specifiche nel funzionamento del Modello Organizzativo ogni qualvolta lo ritenga necessario od opportuno.

6.4.2 Flussi informativi verso l'Organismo di Vigilanza

Ogni funzione aziendale è tenuta ad informare l'Organismo di Vigilanza, relativamente ad ogni fatto o modifica di processo e compiti che sono interessati dal Modello Organizzativo applicato nella Società ai sensi del D. Lgs. 231/01. Al riguardo devono essere segnalati, al verificarsi dell'evento:

- comportamenti non in linea con le regole di condotta adottate dalla Società;
- la commissione di uno dei reati previsti dal D. Lgs. 231/2001 ovvero la violazione o l'elusione fraudolenta dei principi e delle prescrizioni del Modello Organizzativo;
- variazioni al sistema delle deleghe e/o variazioni delle deleghe assegnate;
- tempestivamente i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità;
- le richieste di assistenza legale inoltrata dagli enti aziendali per i reati di cui al Decreto;
- i rapporti preparati dai responsabili delle funzioni aziendali che contengono fatti, atti, eventi ed omissioni inerenti ai reati di cui al Decreto;
- l'attuazione dei provvedimenti disciplinari e delle sanzioni proposte dall'OdV.

I soggetti segnalanti, la cui identità non è divulgata, sono tutelati contro ogni forma di discriminazione, penalizzazione e ritorsione per motivi attinenti alla segnalazione. L'OdV, infatti, garantisce l'assoluta riservatezza ed anonimato delle persone segnalanti, fatti salvi gli obblighi di legge e la tutela dei diritti della Società.
Le segnalazioni pervenute all'OdV devono essere raccolte e conservate in apposito archivio al quale è consentito l'accesso solo da parte di componenti dell'OdV.
Sebbene l'OdV, in conformità al Codice Etico, ritenga preferibili le segnalazioni trasmesse non in forma anonima, sono tuttavia ammesse anche segnalazioni anonime. In tal caso, l'OdV procede preliminarmente a valutarne la fondatezza e rilevanza rispetto ai propri compiti; sono prese in considerazione le segnalazioni anonime che contengano fatti rilevanti rispetto ai compiti dell'OdV e non fatti di contenuto generico, confuso e/o palesemente diffamatorio. Le segnalazioni devono essere comunicate all'Organismo di Vigilanza o tramite comunicazione diretta o, per i dipendenti, tramite i Responsabili di Funzione, i quali devono tempestivamente trasmettere in originale quanto ricevuto all'Organismo di Vigilanza, utilizzando criteri di riservatezza a tutela dell'efficacia degli accertamenti e dell'onorabilità delle persone interessate alla segnalazione.
I componenti dell'OdV, quali soggetti Autorizzati al trattamento dei dati ai sensi della normativa sulla privacy, richiedono che i dati contenuti nelle segnalazioni inoltrate siano pertinenti rispetto alle finalità di cui al D. Lgs. 231/2001.
Nella descrizione di dettaglio del comportamento che origina la segnalazione non devono essere fornite informazioni non strettamente attinenti all'oggetto della segnalazione. In caso di segnalazioni prodotte in evidente malafede, l'OdV si riserva di archiviare le stesse cancellando i nomi e gli elementi che possano consentire l'identificazione dei soggetti segnalati.
La Società, conformemente a quanto previsto dalla L. 179/2017, recante le "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*", tutela i segnalanti da atti di ritorsione o discriminatori, diretti o indiretti, per motivi collegati, direttamente o indirettamente, alla segnalazione.
Tutte le comunicazioni da parte del soggetto segnalante nei confronti dell'Organismo di Vigilanza possono essere effettuate, alternativamente e senza preferenza, a mezzo di:

- E-mail;
- Nota/lettera.

Per il contatto con l'OdV, la Società ha istituito la seguente casella di posta elettronica riservata all'OdV stesso cui fare pervenire le segnalazioni: odv@sofinter.it; in alternativa, le segnalazioni potranno avvenire utilizzando la piattaforma aziendale, accedendo al link: sofinter.integrityline.com.
L'indirizzo di posta ordinaria è: Organismo di Vigilanza c/o General Counsel & Sustainability – Piazza Buffoni, 3 – 21013 Gallarate (VA).

6.4.3 Whistleblowing

In data 29 dicembre 2017 è entrata in vigore la Legge 30 novembre 2017, n. 179 recante le "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" che è intervenuta sull'art. 54-bis del D. Lgs. n. 165/2001 e sull'art. 6 del D. Lgs. 231/2001.
Per quanto concerne, invece, le novità introdotte dalla Legge n. 179/2017 (Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato) in tema di "Whistleblowing", il modello organizzativo dovrà ora prevedere:
1) uno o più canali che consentano a coloro che a qualsiasi titolo rappresentino o dirigano l'ente di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti e

fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte, tali canali garantiscono riservatezza dell'identità del segnalante nell'attività di gestione della segnalazione;
2) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità segnalante;
3) misure idonee a tutelare l'identità del segnalante e a mantenere la riservatezza dell'informazione in ogni contesto successivo alla segnalazione, nei limiti in cui l'anonimato e la riservatezza siano opponibili per legge.
La legge sul whistleblowing introduce nell'ordinamento giuridico italiano un apparato di norme volto a migliorare l'efficacia degli strumenti di contrasto ai fenomeni corruttivi, nonché a tutelare con maggiore intensità gli autori delle segnalazioni, incentivando il ricorso allo strumento della denuncia di condotte illecite o di violazioni dei modelli di organizzazione, gestione e controllo.
Premesso che la Società, in assenza di uno specifico dettato normativo, sino all'avvenuta introduzione della Legge sul whistleblowing, ha sempre posto particolare attenzione alla tematica delle segnalazioni, altresì disciplinando i flussi di informazione, così come previsto nel paragrafo 6.4.2.
Al fine di dare attuazione alle integrazioni apportate all'art. 6 del D. Lgs. 231/2001, si è resa necessaria l'integrazione del Modello di un sistema di gestione delle segnalazioni di illeciti che consenta di tutelare l'identità del segnalante ed il relativo diritto alla riservatezza anche attraverso l'introduzione all'interno del sistema disciplinare di specifiche sanzioni comminate in caso di eventuali atti di ritorsione ed atteggiamenti discriminatori in danno del segnalante che, in buona fede e sulla base di ragionevoli elementi di fatto, abbia denunciato comportamenti illeciti e/o in violazione del Modello e del Codice Etico.
Ciò premesso, la Società, al fine di garantire l'efficacia del sistema di whistleblowing, ha adottato la Procedura Whistleblowing che rende edotti i dipendenti circa l'esistenza di appositi canali di comunicazione che consentono di presentare le eventuali segnalazioni, fondate su elementi di fatto precisi e concordati, garantendo anche con modalità informatiche la riservatezza dell'identità del segnalante.

7. UTILIZZO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE

La Società consente l'utilizzo di sistemi di Intelligenza Artificiale esclusivamente per finalità aziendali lecite e nel rispetto della normativa vigente, del Codice Etico, delle procedure interne e delle disposizioni in materia di protezione dei dati personali, sicurezza delle informazioni e tutela della proprietà intellettuale.
È vietato utilizzare strumenti di Intelligenza Artificiale non autorizzati dalla Società o inserire nei medesimi dati riservati, informazioni confidenziali, dati personali o contenuti soggetti a vincoli di segretezza senza le necessarie autorizzazioni e garanzie.
Gli output generati mediante sistemi di Intelligenza Artificiale devono essere sottoposti a preventiva verifica e validazione da parte del personale responsabile, che mantiene la piena responsabilità delle decisioni adottate e dei documenti prodotti.
La Società adotta adeguati presidi organizzativi e di controllo al fine di prevenire rischi di commissione dei reati previsti dal D. Lgs. 231/2001 connessi all'impiego di sistemi di Intelligenza Artificiale. L'Organismo di Vigilanza riceve flussi informativi periodici in merito all'utilizzo di tali strumenti e alle eventuali anomalie o violazioni riscontrate.
Il Gruppo Sofinter ha adottato la Policy Aziendale per l'Utilizzo Responsabile dell'Intelligenza Artificiale e ha costituito e nominato il Comitato per l'Intelligenza Artificiale ("Comitato AI").
Il Comitato AI rappresenta il presidio di governance incaricato di assicurare una gestione strutturata, responsabile e conforme dei sistemi di Intelligenza Artificiale utilizzati all'interno del Gruppo, nel rispetto della normativa applicabile e delle policy aziendali.
La violazione delle disposizioni relative all'utilizzo dell'Intelligenza Artificiale costituisce inosservanza del Modello 231 ed è soggetta alle misure disciplinari previste dal sistema sanzionatorio aziendale.

8. GOVERNANCE DI SOSTENIBILITÀ E PRESIDIO DEI RISCHI ESG

La Società integra i fattori ESG nei processi decisionali, nel controllo interno e nella gestione dei rischi, in coerenza con il Codice Etico e il Codice di Condotta Fornitori. Il monitoraggio considera gli indicatori ESG rilevanti, incluse emissioni Scope 1, 2 e 3, energia, acqua, rifiuti, salute e sicurezza, persone, etica e acquisti sostenibili.

8.1 Supply chain sostenibile e CBAM

La selezione e il monitoraggio dei Fornitori includono criteri etici, sociali e ambientali, tracciabilità e affidabilità dei dati ESG, con priorità ai fornitori strategici, critici o ad alto rischio. L'accettazione del Codice di Condotta Fornitori è requisito del rapporto commerciale:

- estensione dei principi del Codice ai subfornitori rilevanti;
- sospensione o risoluzione del rapporto in caso di violazioni gravi, dati inattendibili o mancata collaborazione.

La Società assicura gli adempimenti CBAM applicabili, inclusi autorizzazione, dichiarazioni, certificati e verifica delle emissioni.
Violazioni del Codice, falsificazione o occultamento di dati e non conformità rilevanti sono segnalati all'Organismo di Vigilanza secondo i flussi definiti.

9. SISTEMA DISCIPLINARE

9.1 Principi Generali

È essenziale per l'effettività del Modello Organizzativo la costruzione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta contenute nel Codice Etico e il mancato rispetto delle misure indicate nel modello stesso. Le sanzioni previste saranno applicate ad ogni violazione delle regole di condotta aziendali e delle disposizioni contenute nel Modello, comprese la messa in atto di azioni o comportamenti non conformi a quanto previsto dalla Legge sul whistleblowing ex L. 179/2017 ed eventuali successive modificazioni ed integrazioni, a prescindere dall'eventuale esito del giudizio penale, essendo tali regole assunte dalla Società in piena autonomia e prescindono altresì dalle condotte che possono determinare illeciti.

9.2 Sanzioni verso i lavoratori subordinati

Le violazioni alle regole comportamentali contenute nel Codice Etico della Società sono considerate illeciti disciplinari. Le sanzioni erogabili nei riguardi dei lavoratori subordinati rientrano tra quelle previste dal Regolamento Aziendale, nel rispetto delle procedure previste dall'art. 7 dello Statuto dei Lavoratori (Legge n. 300 del 20 maggio 1970) ed eventuali normative sociali applicabili. Il presente Modello Organizzativo fa riferimento alle categorie di fatti sanzionabili previste nel Contratto Nazionale di Lavoro applicato in azienda; tali categorie descrivono i comportamenti sanzionati in base al rilievo che assumono le singole fattispecie considerate e le sanzioni in concreto previste per la commissione dei fatti a seconda della gravità. In particolare, con riferimento all'art. 8 titolo settimo del Contratto Nazionale di Lavoro degli addetti all'industria metalmeccanica privata e installazione impianti, l'inosservanza, da parte dei lavoratori dipendenti, delle disposizioni e procedure contenute nel presente Modello Organizzativo comporterà l'applicazione delle seguenti sanzioni in proporzione alla gravità dell'infrazione:

1. RICHIAMO VERBALE O AMMONIZIONE SCRITTA;
2. MULTA;
3. SOSPENSIONE DAL SERVIZIO E DALLA RETRIBUZIONE;
4. LICENZIAMENTO CON PREAVVISO;
5. LICENZIAMENTO SENZA PREAVVISO.

Costituisce illecito disciplinare ogni violazione delle regole previste dal Modello o da questo richiamate e, in ogni caso, la commissione (anche sotto forma di tentativo) di qualsiasi illecito penale per cui è applicabile il D. Lgs. 231/01. Costituisce, altresì, violazione del Modello il mancato rispetto degli obblighi di riservatezza sull'identità del segnalante previsti dalla Legge sul whistleblowing ex L. 179/2017 ed eventuali s.m.i. a tutela del dipendente o collaboratore che segnala illeciti, il compimento di atti di ritorsione o discriminazione nei confronti dell'autore della segnalazione, nonché il comportamento di colui che effettua con dolo o colpa grave una segnalazione che si rivela infondata. I poteri già conferiti al *management* aziendale, nei limiti della rispettiva competenza, restano invariati sia per l'accertamento delle infrazioni che per i provvedimenti disciplinari. Il sistema disciplinare è oggetto di verifiche di validità e di applicazione da parte delle funzioni preposte congiuntamente alla Direzione ed al Responsabile della gestione delle Risorse Umane.

9.3 Misure nei confronti dei Dirigenti

Nel caso di violazione da parte dei Dirigenti delle procedure interne previste dal Modello Organizzativo nell'espletamento di attività sensibili, o di comportamenti non conformi alle prescrizioni del Modello Organizzativo stesso e del Codice Etico, nonché della Legge sul whistleblowing e della procedura applicativa, la Società provvederà ad applicare, nei confronti dei

responsabili, le misure più idonee in conformità a quanto previsto dall'articolo 7 dello Statuto dei Lavoratori (Legge n. 300 del 20 maggio 1970) e dal Contratto Collettivo Nazionale di Lavoro per i Dirigenti applicato, in quanto tali violazioni saranno considerate dalla Società inadempimento alle obbligazioni derivanti dal rapporto di lavoro.

9.4 Misure nei confronti degli Amministratori e dei Sindaci

Le violazioni del Modello Organizzativo, del Codice Etico e della normativa vigente sul whistleblowing e della procedura applicativa da parte dei Consiglieri di Amministrazione e dei Sindaci vengono segnalate dall'Organismo di Vigilanza a tutti i componenti del Consiglio di Amministrazione e del Collegio Sindacale i quali provvederanno, per gli opportuni provvedimenti ed iniziative ai sensi di legge, a convocare ove necessario l'Assemblea dei Soci al fine di adottare le misure più idonee previste dalla legge.

9.5 Misure nei confronti dei Consulenti e *Partners*

La violazione da parte dei Consulenti o dei *Partners* alle regole di comportamento di cui al Modello Organizzativo ed al Codice Etico o la commissione dei reati previsti dal D. Lgs. 231/2001, viene sanzionata secondo quanto previsto nelle clausole contrattuali inserite nei relativi contratti e, nel caso di inadempimenti gravi, anche con la risoluzione del rapporto contrattuale. Resta salva l'eventuale richiesta di risarcimento nel caso in cui dal comportamento derivino danni concreti alla Società.

9.6 Misure applicabili ai destinatari delle segnalazioni ("Whistleblowing")

La Società, in caso di violazione delle disposizioni normative in materia di whistleblowing e della procedura applicativa al fine di tutelare l'identità del segnalante e lo stesso da eventuali atti di ritorsione o discriminazione, potrà applicare le seguenti sanzioni nei confronti dell'OdV. Nell'ipotesi in cui uno dei membri dell'OdV dovesse violare la riservatezza dell'identità del segnalante, gli altri componenti provvederanno a darne immediata comunicazione al Consiglio di Amministrazione cosicché lo stesso possa procedere con la revoca dell'incarico del membro inadempiente e la conseguente nomina del suo sostituto. Qualora, invece, venga accertata la violazione della riservatezza dell'identità del segnalante da parte dell'OdV nella sua totalità, il Consiglio di Amministrazione procederà alla revoca dell'incarico ed alla conseguente nomina dell'intero Organismo oltre eventuali ed ulteriori previsioni di legge.

10. MAPPATURA RISCHI POTENZIALI DEI REATI PRESUPPOSTO

Ai sensi di quanto disposto dall'art. 6 comma 2, lett. a) del Decreto, la Società, attraverso un processo di mappatura dei rischi ha identificato le Aree di attività nell'ambito delle quali possono essere potenzialmente commessi reati tra quelli previsti dal Decreto. Si precisa inoltre che alcune funzioni – aree di attività, pur non originando direttamente un rischio di reato, ne possono essere il "braccio attuativo" dell'ipotesi di reato commesso da un'altra Area. Quest'ultima, pur essendo individuata come Area a rischio potenziale, può "contaminare" e rendere "complici" altre aree senza che queste si accorgano di partecipare ad un illecito o fattispecie di reato.
Anche per queste aree d'intervento, le Procedure del Modello Organizzativo prevedono delle verifiche sulla gestione ed organizzazione del processo nella sua interezza. In particolare, si tratta delle seguenti aree:

1. modalità di gestione delle risorse finanziarie (es. sistemi gestionali delle risorse finanziarie, sia in entrata che in uscita, che possono comportare flussi finanziari atipici);
2. gestione delle ispezioni (es. D. Lgs. 81/2008, verifiche tributarie, Inps, ecc. ed eventuali contestazioni che ne derivino);
3. gestione degli adempimenti ordinari (es. pratiche amministrative, gestione del possibile contenzioso giudiziale e stragiudiziale con la P.A.);
4. gestione del processo di emissione degli ordini d'acquisto (processo di approvvigionamento di beni e servizi con riferimento agli acquisti gestiti dalle unità competenti della Società e/o gestiti mediante contratto di servizi, alle fasi del processo relative alla richiesta di approvvigionamento, alla selezione del fornitore e alla stipula del contratto, all'utilizzo e gestione dei contratti, alla revisione dei contratti stipulati);
5. processo di gestione delle utilità con particolare riferimento alla gestione degli omaggi, delle sponsorizzazioni, delle liberalità e delle spese di rappresentanza;
6. processo di approvvigionamento, acquisto e vendita di materie prime e prodotti sul mercato con particolare riferimento alle fasi di selezione della controparte, negoziazione e stipula del contratto;
7. processo di selezione e assunzione delle risorse umane;
8. gestione del processo di approvazione delle fatture per il pagamento;
9. società o enti appartenenti allo stesso gruppo ma aventi sede in Stati diversi per le seguenti transazioni: (i) Contratti infragruppo di acquisto e/o di vendita; (ii) Gestione dei flussi finanziari; (iii) Investimenti infragruppo.

Il risultato dell'analisi dei processi e funzioni, effettuato dalla Società, è la Matrice Reati 231, che evidenzia le attività sensibili di illecito e le responsabilità delle funzioni coinvolte. La Società ha adottato specifici Protocolli di Controllo e procedure finalizzate ad evitare il compimento dei reati previsti dal D. Lgs. 231/2001, ritenuti potenziali in base all'analisi effettuate dei processi sensibili. La Matrice Reati è parte integrante del Modello Organizzativo e rappresenta lo strumento che individua le aree e l'intensità del rischio di commissione dei reati previsti dalla norma. Essa rappresenta inoltre lo strumento principale per la realizzazione, la verifica e il miglioramento continuo del Modello Organizzativo coerente con il D. Lgs. e costituisce per l'OdV utile base informativa da cui avviare l'osservazione e l'indagine diretta al miglioramento continuo.
La documentazione relativa alla matrice Reati-Attività sensibili e al modello di misurazione dei rischi e controlli è archiviata presso il Dipartimento Legal and Corporate Compliance della Società.

11. AGGIORNAMENTO DEL MODELLO ORGANIZZATIVO

Essendo il presente Modello Organizzativo un "atto di emanazione dell'organo Dirigente" (in conformità alla prescrizione dell'art. 6, comma 1, lettera a del Decreto), la sua adozione, così come le successive modifiche e integrazioni, anche su proposta dell'Organismo di Vigilanza, sono rimesse alla competenza del Consiglio di Amministrazione della Società.
È peraltro riconosciuta all'Amministratore dotato di idonei poteri la facoltà di apportare al testo eventuali modifiche o integrazioni di carattere formale e non sostanziale, riferendo periodicamente al Consiglio di Amministrazione della Società in merito alle suddette modifiche apportate.
Nel contesto di detti poteri, l'Amministratore potrà inoltre adottare o modificare le procedure aziendali e i protocolli di controllo inerenti alle aree aziendali sensibili indicate nel presente Modello e nella Matrice Reati 231.
In ogni caso, il Modello Organizzativo, le procedure e i protocolli di controllo inerenti ai processi sensibili ivi indicati dovranno essere tempestivamente modificati:

- qualora intervengano mutamenti rilevanti nel sistema normativo;
- qualora intervengano mutamenti rilevanti nell'assetto societario e/o organizzativo aziendale;
- quando siano individuate violazioni o elusioni delle prescrizioni, allo scopo di mantenere l'efficienza del Modello Organizzativo.

L'Organismo di Vigilanza ha il compito di monitorare lo stato di avanzamento e i risultati dell'aggiornamento del Modello Organizzativo e delle eventuali modifiche delle procedure e dei protocolli di controllo, fornendone adeguata informativa alla Società.

12. DOCUMENTI DI RIFERIMENTO PER LA PREDISPOSIZIONE DEL MODELLO ORGANIZZATIVO

A. Codice Etico di Gruppo
B. Codice di Condotta Fornitori
C. Sistema Qualità: manuale della qualità e procedure
D. Sistema Gestione Sicurezza sul Lavoro
E. D. Lgs. 231/01
F. Linee Guida Confindustria

13. ALLEGATI AL MODELLO ORGANIZZATIVO

Modello Organizzativo – Parte Speciale
Matrice Reati 231 – Attività aziendali sensibili
Protocolli di Controllo
Manuale Anti-Corruzione

Appendice: Evoluzione del Modello Organizzativo

DATA	*DESCRIZIONE*
28 ottobre 2004	**Modello Organizzativo / EDIZIONE 1**
28 ottobre 2004	**Codice Etico / EDIZIONE 1**
24 marzo 2006	**Modello Organizzativo / EDIZIONE 2** Approvazione del Modello Organizzativo – Ed. 2, che ha recepito: - le nuove normative in materia di D. Lgs. 231/01; - le evoluzioni organizzative avvenute dal 28 ottobre 2004.
29 marzo 2007	**Modello Organizzativo / EDIZIONE 3** Approvazione del Modello Organizzativo – Ed. 3, che ha: - diminuito il numero minimo dei componenti dell'OdV, da tre a due; - aggiornato le partecipazioni della Società e conseguentemente l'Allegato 1.
30 ottobre 2008	**Modello Organizzativo / EDIZIONE 4** Approvazione del Modello Organizzativo – Ed. 4, che ha: - aggiornato le partecipazioni della Società e conseguentemente l'Allegato 1; - recepito le normative relative a: (i) delitti informatici e trattamento illecito di dati introdotto dalla L.18 marzo 2008 n. 48, art. 7; (ii) omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (ex art. 25-septies del D. Lgs. 231/01) introdotto dalla L. 3 agosto 2007 n. 123, art. 9; (iii) reati di ricettazione, riciclaggio e impiego di utilità illecite (ex art. 25-octies del D. Lgs. 231/01 introdotto dal D. Lgs. 21 novembre 2007 n. 231, art 63); - recepito le variazioni dell'organizzazione aziendale.
8 luglio 2011	**Modello Organizzativo / EDIZIONE 5** Recepisce le normative relative a: • Delitti in materia di violazione dei diritti d'autore e induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (ex art. 25-novies e art. 25-decies del D. Lgs. 231/01), • art. 10 ex Legge 16 marzo 2006, n. 146 – "Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001" pubblicata nella Gazzetta Ufficiale n. 85 dell'11 aprile 2006 – Supplemento ordinario n. 91.
27 marzo 2013	**Codice Etico / EDIZIONE 2**
28 marzo 2014	**Modello Organizzativo / EDIZIONE 6** Recepisce le normative relative a: ***Art. 25-undecies***: *"Reati Ambientali"* ***Art. 25-duodecies***: *"Impiego dei lavoratori privi di permesso di soggiorno"*
1° dicembre 2017	**Codice Etico / EDIZIONE 3**
26 gennaio 2018	**Modello Organizzativo / EDIZIONE 7** Approvazione del Modello Organizzativo – Ed. 7, che ha recepito: • la nozione di pubblico ufficiale; • le nuove normative in materia di D. Lgs. 231/01 (Autoriciclaggio e L. n. 9 del 2013); • l'inserimento del nuovo paragrafo 9. Aggiornamento del Modello Organizzativo; • l'introduzione dei nuovi allegati – Matrice Reati e Manuale Anti Corruzione; • le variazioni dell'organizzazione aziendale; • l'adozione e l'approvazione del Regolamento di funzionamento da parte dell'Organismo di Vigilanza; • tra i compiti dell'OdV, la possibilità di accedere ai documenti aziendali al fine di poter effettuare le verifiche necessarie, senza la preventiva autorizzazione da parte degli uffici di riferimento competenti; • la richiesta annuale dell'OdV al CdA dell'assegnazione di un budget adeguato per lo svolgimento delle attività di vigilanza, da gestire in piena autonomia.

25 maggio 2018	**Modello Organizzativo / EDIZIONE 8** Approvazione del Modello Organizzativo – Ed. 8, che ha recepito: - le variazioni dell'organizzazione aziendale; - le nuove normative in materia di D. Lgs. 231/01 (Art. 25-terdecies Razzismo e xenofobia); - il reporting OdV su base semestrale nei confronti del CdA e del Collegio Sindacale; - le variazioni dei flussi informativi verso l'OdV e delle segnalazioni all'OdV
21 febbraio 2019	**Codice Etico / EDIZIONE 4**

22 ottobre 2021	**Modello Organizzativo / EDIZIONE 9**
	Recepisce:
	- le nuove normative in materia di D. Lgs. 231/01:
	  - Art. 25-ter lettera s-bis: "Corruzione tra privati" (art. 2635 c.c.) e "Istigazione alla corruzione tra privati "(art. 2635 bis c.c.);
	  - Art. 25-quaterdecies: "Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati" [articolo aggiunto dalla L. n. 39/2019];
	  - Art. 25-quinquiesdecies: "Reati tributari" [articolo aggiunto dalla L. n. 157/2019 e dal D. Lgs. n. 75/2020];
	  - Art. 25- sexiesdecies: "Contrabbando" [articolo aggiunto dal D. Lgs. n. 75/2020];
	  - Nuove fattispecie di reati fiscali, tra le quali i delitti di: dichiarazione infedele, omessa dichiarazione, indebita compensazione, dichiarazione fraudolenta mediante l'uso di fatture false e contrabbando, e dall'attuazione della c.d. Direttiva PIF n. 1371/2017 del Parlamento Europeo e del Consiglio Europeo del 5 luglio 2017, recante norme per la "*lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale";*
	- le variazioni dell'organizzazione aziendale;
	- il par. 6.4.3 Whistleblowing: la tutela da parte della Società, conformemente a quanto previsto dalla L. 179/2017, degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato;
	- il par. 7.6 Misure applicabili ai destinatari delle segnalazioni ("Whistleblowing").

aprile 2022	**Modello Organizzativo / EDIZIONE 9** Recepisce le nuove normative in materia di D. Lgs. 231/01: - Art. 25 octies 1 "Illeciti in materia di mezzi di pagamento diversi dai contanti"; - Art. 25-septiesdecies: "Delitti contro il patrimonio culturale" [Legge 9 marzo 2022 n. 22]; - Art. 25-duodevicies: "Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici".
17 dicembre 2024	**Modello Organizzativo / EDIZIONE 10** Recepisce: - le nuove normative in materia di D. Lgs. 231/01; - le variazioni dell'organizzazione aziendale e della struttura societaria; - il riferimento alla Procedura Whistleblowing e al nuovo canale di segnalazione; - il riferimento al Nuovo Codice di Condotta Fornitori.
26 febbraio 2026	**Modello Organizzativo / EDIZIONE 11** Recepisce: - le nuove normative in materia di D. Lgs. 231/01; - le variazioni dell'organizzazione aziendale e della struttura societaria.
26 maggio 2026	**Modello Organizzativo / EDIZIONE 12** Recepisce: - la riforma dei reati ambientali – D. Lgs. 21 aprile 2026 – Parte Speciale.
23 ottobre 2026	**Modello Organizzativo / EDIZIONE 13** Recepisce: - la nuova normativa in materia di D. Lgs. 231/01 (Art. 25-vicies: "Reati commessi con l'uso di intelligenza artificiale"); - il riferimento all'utilizzo dei sistemi di Intelligenza Artificiale;

	- il riferimento alla Governance di sostenibilità e presidio dei rischi ESG; Supply chain sostenibile e CBAM.

Il presente **Modello Organizzativo – Edizione 13** è stato approvato dall'Amministratore Delegato della Società, in virtù di delega allo stesso conferita dal Consiglio di Amministrazione, in data 23 ottobre 2026 e sostituisce le precedenti edizioni.

MODELLO ORGANIZZATIVO – PARTE SPECIALE

La Parte Speciale ha la finalità di definire linee, regole e principi di comportamento che tutti i destinatari del Modello 231 dovranno seguire al fine di prevenire, nell'ambito delle specifiche attività sensibili svolte nella società, la commissione di reati previsti dal Decreto e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.
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
- Ordini di servizio
- Comunicazioni organizzative
- Sistemi di gestione delle problematiche di sicurezza e ambientali
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto

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

I CONTROLLI DELL'ODV

Fermo restando quanto previsto nella Parte Generale relativamente ai suoi poteri e doveri, ivi compreso quello, discrezionale, di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio, 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 esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni.
A tal fine, all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante.

ELENCO FATTISPECIE DI REATO PREVISTE DAL DECRETO LEGISLATIVO 231/01

Elenco fattispecie di reato previste dal Decreto Legislativo 231/01:
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 [Articolo modificato dalla L. 161/2017 e dal D.Lgs.n.75 del 14 luglio 2020]
Delitti informatici e trattamento illecito di dati - Art. 24 bis [Articolo aggiunto dalla L. 48/2008, modificato dai D.Lgs. n.7 e n.8/2016, dal D.L. n. 105/2019 e dalla L. n. 90 del 28 giugno 2024]
Delitti di criminalità organizzata - Art. 24 ter [Articolo aggiunto dalla L. n. 94/2009, modificato dalla L. 69/2015]
Peculato, concussione, induzione indebita a dare o promettere utilità', corruzione, indebita destinazione di denaro o cose mobili - Art. 25 [Articolo modificato dalla L. n. 190/2012 e dalla Legge n. 3 del 9 gennaio 2019 e dal D. Lgs. n. 75 del 14 luglio 2020. Rubrica modificata, unitamente al testo , da legge di conversione n. 112 dell'8 agosto 2024]
Falsità in monete, in carte di pubblico credito, in valori in bollo e in strumenti o segni di riconoscimento - Art. 25 bis [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. n. 125/2016]
Delitti contro l'industria e il commercio - Art. 25 bis 1 [Articolo aggiunto dalla L. n. 99/2009]
Reati Societari - Art. 25 ter [Articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla l. 69/2015 e successivamente dal D.Lgs. n. 38/2017 e da D. lgs. n. 19 del 2 marzo 2023]
Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal Codice penale e dalle leggi speciali - Art. 25 quater [Articolo aggiunto dalla L. n. 7/2003]
Pratiche di mutilazione degli organi genitali femminili - Art. 25 quater 1 [Articolo aggiunto dalla L. n. 7/2006]
Delitti contro la personalità individuale - Art. 25 quinquies [Articolo aggiunto dalla L. n. 228/2003 e modificato dalla L. n. 199/2016]
Reati di abuso di mercato - Art- 25 sexies [Articolo aggiunto dalla L. n. 62/2005] e altre fattispecie in materia di abusi di mercato [Articolo modificato dal D. Lgs. n. 107/2018 e dalla Legge n. 238 del 23 dicembre 2021]
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro Art. 25 septies [Articolo aggiunto dalla L. n. 123/2007]
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio – Art. 25-octies [Articolo aggiunto dal D. Lgs. 231/2007; modificato dalla L. n. 186/2014 e da D. lgs. n. 195 del 18 novembre 2021]
Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori – Art. 25 octies-1 [Articolo aggiunto dal D. Lgs. n. 184 del 18 novembre 2021 e modificato dal D.L 10 agosto 2023 n. 105 coordinato con la Legge di conversione n. 137 del 9 ottobre 2023]
Reati in misura di violazione di misure restrittive dell'Unione Europea - Art. 25 octies-2 [Articolo aggiunto da D.Lgs. n. 211 del 30 dicembre 2025]
Delitti in materia di violazione del diritto d'autore – Art. 25 novies [Articolo aggiunto dalla L. n. 99/2009]
Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria – Art. 25 decies [Articolo aggiunto dalla L. n. 116/2009]
Reati ambientali – Art. 25 undecies [Articolo aggiunto dal D. Lgs. 121/2011, modificato dalla L. n. 68/2015, da D. Lgs. n. 21/2018, da D. Lgs. n. 116 dell'8 agosto 2025, da Legge n. 147 del 3 ottobre 2025 e dal D. Lgs. n. 81 del 21 aprile 2026]
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare – Art. 25 duodecies [Articolo aggiunto dal D. Lgs. n. 109/2012 e modificato dalla Legge n. 161/2017]
Razzismo e xenofobia – Art. 25 terdecies [Articolo aggiunto dalla L. n. 167/2017 e modificato dal D. lgs. n. 21/2018]
Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati – Art. 25-quaterdecies [Articolo aggiunto dall'art. 5 della L. n. 39/2019]
Reati tributari – Art. 25 quinquiesdecies [Articolo aggiunto dal D.L. n. 124/2019 coordinato con Legge di conversione n. 157/2019 e modificato dal D.Lgs. n. 75/2020 e dal D. Lgs. n. 156/2022]
Contrabbando – Art. 25 sexiesdecies [Articolo aggiunto dal D.Lgs. n. 75/2020 e modificato nel testo dal D. lgs. n. 141 del 26 settembre 2024]
Disposizioni in materia di reati contro il patrimonio culturale – Art. 25 septiesdecies [Articolo aggiunto da L.n. 22 del 09 marzo 2022]
Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici – Art. 25 duodevicies [Articolo aggiunto da L.n. 22 del 09 marzo 2022]
Disposizioni in materia di Delitti contro gli animali – Art. 25 undevicies [Articolo aggiunto da L. n. 82 del 06 giugno 2025]
Reati commessi mediante Sistemi di Intelligenza Artificiale - [Art. 25-vicies aggiunto dal Decreto Legislativo No. 160 del 2026]
Delitti tentati – Art. 26
Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato [Costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva] - Art.12 L. 9/2013
Reati transnazionali [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale] - L. 146/2006.

Le fattispecie di reato ex art. 24-*bis* del D. Lgs. 231/2001
Delitti informatici e trattamento illecito dei dati

Riferimenti normativi:
- Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter*, c.p.);
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-*quater*, c.p.);
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615- *quinquies*, c.p.) – ABROGATO DALLA LEGGE N. 90 DEL 28 GIUGNO 2024;
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-*bis* c.p.);
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater*, c.p.);
- 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.);
- Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617-*sexies* c.p.);
- Circostanze attenuanti (art. 623-*quater* c.p.);
- Estorsione (art. 629 c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis*, c.p.);
- Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-*ter*, c.p.);
- Danneggiamento di sistemi informatici e telematici (art. 635-*quater*, c.p.);
- 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.);
- Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635- *quinquies*, c.p.);
- Circostanze attenuanti (art. 639-*ter* c.p.);
- Documenti informatici (art. 491-*bis*, c.p.);
- Frode informatica (Art. 640-*ter*);
- Frode informatica del soggetto che presta servizi di certificazione 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. n. 105 del 21 ottobre 2019).

Attività sensibili
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 della società 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. n. 231/2001:
- ✓ accesso abusivo a sistemi e/o divulgazione, intercettazione o sottrazione delle informazioni di natura info-telematica (comprensiva di credenziali di accesso) e/o utilizzo di programmi informatici al fine di acquisire o diffondere illecitamente informazioni di natura riservata, ovvero distruggere, danneggiare o rendere inservibili sistemi informatici di terze parti. Il profilo di rischio può realizzarsi anche attraverso attività svolta da soggetti terzi;
- ✓ alterazione o falsificazione di atti, documenti e scritture predisposte e inviate in forma telematica.

I potenziali reati associabili sono:
- ✓ accesso abusivo a un sistema informatico o telematico;
- ✓ detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- ✓ diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- ✓ intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- ✓ installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- ✓ danneggiamento di informazioni, dati e programmi informativi utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
- ✓ falsità relativamente a documenti informatici.

Strumenti di controllo del sistema organizzativo
La presente Parte Speciale prevede l'espresso obbligo, a carico degli esponenti aziendali in via diretta e, tramite apposite clausole contrattuali, a carico dei collaboratori esterni e partner, di evitare tutti i comportamenti che integrino i reati sopra descritti. Il sistema per la prevenzione dei reati perfezionato dalla società è stato realizzato applicando alle attività sensibili i seguenti standard di controllo:
- l'esistenza di una politica in materia di sicurezza del sistema informativo;
- l'adozione e l'attuazione di uno strumento normativo che definisce i ruoli e le responsabilità nella gestione delle modalità di accesso di utenti interni alla società e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici;
- l'adozione e l'attuazione di uno strumento normativo che dispone controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature;

- l’adozione e l’attuazione di uno strumento normativo che assicura la correttezza e la sicurezza dell’operatività dei sistemi informativi tramite policy, procedure e protocolli di controllo;
- l’adozione e l’attuazione di uno strumento che disciplina gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi e alle applicazioni;
- l’adozione e l’attuazione di uno strumento che definisce adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica;
- l’adozione e l’attuazione di uno strumento normativo che disciplina i ruoli, le responsabilità e le modalità operative delle attività di verifica periodica dell’efficienza ed efficacia del sistema di gestione della sicurezza informatica;
- l’adozione e l’attuazione di uno strumento normativo che definisca i ruoli e le responsabilità nella gestione degli acquisti di software e materiale IT.

Le fattispecie di reato ex art. 24-*ter* del D. Lgs. 231/2001
Delitti di criminalità organizzata

Riferimenti normativi:
- Art. 416 c.p. (Associazione per delinquere);
- Art. 416-*bis* c.p. (Associazione di tipo mafioso anche straniere);
- Art. 416-bis.1 c.p. (Circostanze aggravanti e attenuanti per reati connessi ad attività mafiose);
- Art. 416-ter c.p. (Scambio elettorale politico-mafioso);
- Art. 630 c.p. (Sequestro di persona a scopo di estorsione);
- Art. 74 DPR 309/1990 (Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope).

Le Aree sensibili
Alla luce dei risultati del *risk assessment* eseguito dalla società, le seguenti aree di attività aziendale sono risultate rilevanti in relazione al rischio di commissione di reati di criminalità organizzata:
- ✓ Finance, Treasury & Networking Capital and Controlling
- ✓ Sales/Proposal
- ✓ Integrated Supply Chain
- ✓ Client & Field Service

Di seguito a titolo esemplificativo, e non esaustivo, sono considerate attività a rischio:
- ✓ nell'ambito delle operazioni di natura straordinaria, attraverso la gestione impropria del ruolo ricoperto dalla società al fine di promuovere, finanziare, costituire, organizzare ovvero partecipare ad associazioni, sia di carattere nazionale che transnazionale, anche finalizzate ad attività terroristiche o di eversione dell'ordine democratico e anche in caso di cooperazione di esponenti della società con due o più soggetti per il perseguimento di qualsiasi delitto non colposo;
- ✓ gestione impropria del ruolo ricoperto all'interno della società al fine di promuovere, costituire, organizzare ovvero partecipare ad associazioni realizzate mediante cooperazione con due o più soggetti per il perseguimento di finalità illecite;
- ✓ il reato potrebbe dirsi integrato qualora più soggetti riferibili alla società o insieme anche a soggetti esterni (fornitori, clienti, rappresentanti della P.A., consulenti, ecc.), si associno allo scopo di commettere più delitti (ad esempio contro la P.A. o contro la proprietà industriale ecc.) anche mediante: a) il finanziamento dell'associazione criminale tramite l'erogazione di denaro; b) l'assunzione di personale o la nomina di consulenti o l'assegnazione di lavori a fornitori legati da vincoli di parentela e/o di affinità con esponenti di note organizzazioni criminali.

Al di fuori delle ipotesi di partecipazione all'associazione, il dipendente della società potrebbe concorrere nel reato, nella forma del concorso esterno, nel caso in cui, pur non essendo integrato nella struttura organizzativa del sodalizio criminoso, apporti un contributo al conseguimento degli scopi dell'associazione, ad esempio agevolando con qualsiasi mezzo la commissione dei delitti scopo dell'associazione.

Strumenti di controllo del sistema organizzativo
La presente Parte Speciale, oltre agli specifici principi di comportamento relativi alle aree di rischio sopra indicate, richiama i principi generali di comportamento previsti dal presente Modello adottato dalla società, alla cui osservanza tutti gli amministratori e dipendenti/collaboratori della società sono tenuti.
Si è ritenuto che, per la prevenzione di detti reati, possano svolgere un'adeguata funzione preventiva:
- i presidi di corporate governance implementati dalla società;
- i presidi di controllo previsti dai protocolli che costituiscono parte integrante del Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/01 adottato dalla società;
- i principi presenti nel Codice Etico della società;
- procedure aziendali che costituiscono parte integrante del Corporate Compliance Program del Gruppo Sofinter.

Reati commessi nei rapporti con la Pubblica Amministrazione, Corruzione e Concussione (artt. 24 e 25 e 25-*ter*, limitatamente al reato di corruzione tra privati del Decreto)

Riferimenti normativi:

- Divieto temporanei di trattare con la Pubblica Amministrazione (Art. *289 bis* c.p.p.)
- Peculato (Art. 314 c.p.);
- Indebita destinazione di denaro o cose mobili (Art. 314-*bis* c.p.);
- Peculato mediante profitto dell'errore altrui (Art. 316 c.p.);
- Indebita percezione di erogazioni pubbliche (Art. 316-*ter* c.p.);
- Malversazione di erogazioni pubbliche (Art. 316-*bis* c.p.);
- Concussione (Art. 317 c.p.);
- Corruzione per l'esercizio della funzione (Art. 318 c.p.);
- Corruzione per un atto contrario ai doveri d'ufficio (Art. 319 c.p.);
- Circostanze aggravanti (Art. 319-*bis* c.p.);
- Corruzione in atti giudiziari (Art. 319-*ter* c.p.);
- Induzione indebita a dare o promettere utilità (Art. 319-*quater*);
- 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, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (Art. 322-*bis* c.p.);
- Riparazione pecuniaria (Art. 322-*quater* c.p.);
- Abuso d'ufficio (Art. 323 c.p.); Abrogato dalla L. n. 114 del 09/08/2024;
- Circostanze attenuanti (Art. 323-*bis* c.p.);
- Causa di non punibilità (Art. 323-ter c.p.);
- Traffico di influenze illecite (Art. 346-*bis* c.p.);
- Turbata libertà degli incanti (Art. 353 c.p.);
- Turbata libertà del procedimento di scelta del contraente (Art. 353-*bis* c.p.);
- Frode nelle pubbliche forniture (Art. 356 c.p.);
- Truffa (Art. 640 c.p.);
- Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640-*bis* c.p.);
- Frode informatica (Art. 640-*ter* c.p.);
- Applicabilità dell'art. 322-*ter* c.p. (Art. 640-*quater* c.p.);
- Frode in agricoltura (Art. 2 L. 898 23 dicembre 1986 – Modificato dal D. Lgs. 184 dell'08/11/21 e dal D. Lgs. 156 del 04/10/22);
- Corruzione tra privati (Art. 2635 c.c.);
- Istigazione alla corruzione tra privati (Art. 2635-*bis* c.c.);
- Pene accessorie (Art. 2635-*ter* c.c.).

Definizione Enti della Pubblica Amministrazione: viene comunemente considerato "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 o di atti autoritativi. Non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti sono soggette nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose previste dal Decreto. Le figure che assumono rilevanza a tal fine sono soltanto quelle dei "**Pubblici Ufficiali**" e degli "**Incaricati di Pubblico Servizio**".

Le Aree sensibili

Ai fini del Modello, sono da considerarsi potenzialmente a rischio tutte quelle aree aziendali che, per lo svolgimento delle proprie attività tipiche, intrattengono rapporti con la P.A. (c.d. **rischio diretto**).

Allo stesso modo, sono da considerarsi a rischio le aree aziendali che, pur non implicando direttamente l'instaurazione di rapporti con la P.A., gestiscono strumenti di tipo finanziario o utilità di altro genere che potrebbero essere impiegati per attribuire vantaggi e utilità a pubblici ufficiali (c.d. **rischio indiretto**).

A titolo esemplificativo, e non esaustivo, sono ad esempio attività a rischio diretto:

- ✓ partecipazione a tutte le procedure che coinvolgano rapporti con la P.A.;
- ✓ richiesta, percezione, utilizzo e rendicontazione di finanziamenti, sovvenzioni e contributi pubblici;
- ✓ rapporti con Pubblici Ufficiali in occasione di verifiche e ispezioni (Guardia di finanza, Agenzia delle Entrate, Vigili del Fuoco, Ispettori dell'ASL, dell'INPS, dell'INAIL, Polizia Provinciale, ecc.);
- ✓ stipula di contratti, convenzioni e atti in genere con la Pubblica Amministrazione;
- ✓ rapporti con soggetti pubblici per l'ottenimento, il mantenimento e il rinnovo di autorizzazioni, concessioni, licenze, servitù, necessarie o utili per l'esercizio delle attività aziendali;
- ✓ contrattazioni, negoziazioni, trattative private con Enti pubblici svolte con la Pubblica Amministrazione per l'ottenimento di commesse, appalti, forniture, servizi, concessioni, partnership, asset, o altre operazioni similari, caratterizzate comunque dal fatto di essere svolte in un contesto competitivo, ovvero per il recupero di crediti nei confronti della PA.

A titolo esemplificativo, e non esaustivo, sono considerate attività a rischio indiretto:

- ✓ amministrazione, finanza e contabilità, in cui il rischio principale riguarda l'ipotesi di accantonamento di somme di denaro ("fondi occulti") a scopi corruttivi;
- ✓ consulenze, su cui grava il rischio che gli incarichi dissimulino illecite attribuzioni di utilità a soggetti legati direttamente o indirettamente a pubblici ufficiali che hanno rapporti diretti con la società al fine di ottenere un ingiusto vantaggio a danno della P.A.;
- ✓ gestione degli approvvigionamenti di beni e servizi, su cui grava il rischio che gli incarichi dissimulino illecite attribuzioni di utilità a soggetti legati direttamente o indirettamente a pubblici ufficiali che hanno rapporti diretti con la società, allo scopo esclusivo di alterarne l'indipendenza di giudizio e di procurare alla società un vantaggio ingiusto;
- ✓ contenziosi giudiziali e stragiudiziali e procedimenti arbitrali, in cui il rischio concerne sia le ipotesi di reato di corruzione in atti giudiziari, sia la simulazione di transazioni per determinare distrazione di liquidità dalla contabilità ufficiale volte ad alimentare i fondi occulti;
- ✓ omaggi, spese di rappresentanza e sponsorizzazioni, su cui grava il rischio che le elargizioni siano direttamente o indirettamente rivolte a pubblici ufficiali o incaricati di pubblico servizio che hanno rapporti diretti con la società, allo scopo esclusivo di alterarne significativamente l'indipendenza di giudizio e di procurare alla società un vantaggio ingiusto.

Per un dettaglio delle attività sensibili, dei reati ipotizzabili, dei presidi esistenti e della valutazione del rischio si rimanda alla Matrice Reati 231 – Attività sensibili aziendali – Rischi, allegata al Modello Organizzativo.

Strumenti di controllo del sistema organizzativo

L'Ente è dotato di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati ai principi generali di:

- chiara descrizione delle linee di riporto;
- conoscibilità, trasparenza e pubblicità dei poteri attribuiti (all'interno dell'ente e nei confronti dei terzi interessati);
- chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione, dei relativi poteri e responsabilità.

Le procedure interne sono caratterizzate dai seguenti elementi:

- distinzione, all'interno di ciascun processo, tra il soggetto che assume la decisione (impulso decisionale), il soggetto che esegue tale decisione e il soggetto cui è affidato il controllo del processo;
- traccia scritta di ciascun passaggio rilevante del processo;
- adeguato livello di formalizzazione.

Ai fini dell'attuazione delle regole comportamentali in conformità a quanto previsto dal D. Lgs. 231, i Destinatari della presente Parte Speciale del Modello, oltre a rispettare le previsioni di legge esistenti in materia, le norme nel Codice Etico e i principi indicati nella Parte Generale del presente Modello, devono rispettare i protocolli comportamentali, posti a presidio dei rischi-reato sopra identificati e riferibili alle attività a rischio. Il sistema di deleghe e procure concorre, insieme agli altri strumenti del presente Modello, alla prevenzione dei rischi-reato nell'ambito delle attività a rischio identificate.

La società, mediante organigrammi o comunicazioni organizzative adeguatamente divulgati al suo interno, definisce:

- la delimitazione dei ruoli, la descrizione dei compiti di ciascuna funzione e dei relativi attribuzioni e poteri;
- la descrizione delle linee di riporto.

Le fattispecie di reato ex art. 25-*bis* del D. Lgs. 231/2001
Falsità in monete, in carte di pubblico credito, in valori in bollo e in strumenti o segni di riconoscimento

Riferimenti normativi:
- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (Art. 453 c.p.);
- Alterazione di monete (Art. 454 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 e messa in circolazione di valori 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.);
- Indebito utilizzo e falsificazione di carte di credito e di pagamento (Art. 493-ter c.p.);
- Trasferimento fraudolento di valori (Art. 512-*bis* c.p.).

Le Aree sensibili

Sono state individuate, nell'ambito della struttura organizzativa e aziendale, delle aree sensibili, ovvero quelle aree e settori aziendali rispetto ai quali è stato ritenuto astrattamente sussistente il rischio di commissione dei reati in tema di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento. Con riferimento agli illeciti sopra elencati, le "aree sensibili" ritenute più specificamente a rischio di reato risultano essere le seguenti:
- ✓ Gestione delle transazioni finanziarie (incassi e pagamenti);
- ✓ Emissione, contabilizzazione e archiviazione delle fatture attive e delle note di credito;
- ✓ Controlli sulla regolarità delle fatture attive;
- ✓ Liquidazione delle prestazioni e incassi;
- ✓ Verifica e controllo dell'inserimento della clausola relativa all'obbligo di tracciabilità dei flussi finanziari nelle commesse pubbliche;
- ✓ Apertura/chiusura di conti correnti; riconciliazione degli estratti conto bancari e delle operazioni di cassa; registrazione degli incassi e dei pagamenti in contabilità generale;
- ✓ Gestione della cassa;
- ✓ Gestione delle donazioni, elargizioni, offerte ed altre iniziative liberali;
- ✓ Gestione delle missioni/trasferte; gestione, controllo e autorizzazione delle note spese; gestione e controllo dei benefit e dei mezzi in dotazione; gestione delle spese di rappresentanza e dei beni in rappresentanza.

Strumenti di controllo organizzativi

Tutti i soggetti Destinatari coinvolti nelle aree sensibili e nelle attività strumentali sono tenuti, nell'ambito della propria attività, al rispetto delle norme di comportamento, conformi ai principi dettati dal Modello e, in particolare, dal Codice Etico, dai protocolli di controllo specifici e dalle procedure aziendali. In generale è fatto divieto di:
a) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate;
b) richiedere, sollecitare, suggerire a dipendenti e/o collaboratori comportamenti vietati dal Modello;
c) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
d) porre in essere qualsiasi situazione di conflitto di interessi nei confronti della Pubblica Amministrazione in relazione a quanto previsto dalle suddette ipotesi di reato;
e) porre in essere i comportamenti indicati ai precedenti punti sia direttamente, sia per interposta persona.

Le fattispecie di reato ex art. 25-*bis*.1 del D. Lgs. 231/2001
Delitti contro l'industria e il commercio

Riferimenti normativi:
- Turbata libertà dell'industria o del commercio (Art. 513 c.p.);
- Illecita concorrenza con minaccia o violenza (Art. 513-*bis* 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.).

Le Aree sensibili
Di seguito sono elencate le cosiddette Aree sensibili o a rischio identificate con riferimento ai reati contro l'industria e il commercio:
- ✓ Sales/Proposal
- ✓ Integrated Supply Chain
- ✓ Quality & Welding

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale i seguenti reati:
- ✓ accesso alle informazioni e/o segreti industriali dei competitor, anche attraverso il riconoscimento o la promessa di denaro o altra utilità a soggetti terzi, per l'ideazione, progettazione e realizzazione di nuovi prodotti ai fini registrativi;
- ✓ ideazione, progettazione e realizzazione di nuovi prodotti ai fini registrativi, usurpando titoli di proprietà industriali altrui;
- ✓ mancata formulazione di rilievi in caso di non conformità e/o controlli sui processi di produzione, importazione e commercializzazione di componenti allo scopo di rivenderlo al cliente, violando dolosamente invenzioni tutelate da brevetto;
- ✓ produzione e commercializzazione indebita di prodotti in violazione degli accordi di licenza usurpando titoli di proprietà industriali altrui.

Strumenti di controllo del sistema organizzativo
Al fine di prevenire i reati sopra enunciati, tutti i destinatari devono rispettare, oltre i principi di comportamento già previsti ed espressi nel Codice Etico, anche quelli riportati nei documenti organizzativi adottati dalla società, nonché tenere comportamenti conformi a quanto previsto dalle vigenti norme di legge.
Di seguito, i presidi di controllo generali:
- Codice Etico;
- formazione in ordine al Modello e alle tematiche di cui al D. Lgs. n. 231/2001, rivolta alle risorse operanti nell'ambito delle aree a rischio;
- diffusione del Modello tra le risorse della società, mediante pubblicazione del Modello e dei protocolli maggiormente significativi (ad es., Codice Etico, Sistema Disciplinare, Procedure rilevanti, ecc.) sulla intranet aziendale;
- diffusione del Modello tra i Terzi Destinatari tenuti al rispetto delle relative previsioni (ad es. fornitori, appaltatori, consulenti) mediante pubblicazione dello stesso sul sito della società;
- dichiarazione con cui i Destinatari del Modello, inclusi i Terzi Destinatari (ad es. fornitori, consulenti, appaltatori), si impegnano a rispettare le previsioni del Decreto;
- Sistema Disciplinare volto a sanzionare la violazione del Modello e dei Protocolli a esso connessi;
- acquisizione di una dichiarazione, sottoscritta da ciascun destinatario del Modello della società, di impegno al rispetto dello stesso, incluso il Codice Etico;
- creazione di una "Sezione 231" all'interno della intranet, presso cui pubblicare tutti i documenti rilevanti nell'ambito del Modello dell'Associazione (ad es. Modello, Codice Etico, Protocolli in esso richiamati).

Le fattispecie di reato ex art. 25-*ter* del D. Lgs. 231/2001
Reati societari

Riferimenti normativi:
- False comunicazioni sociali (Art. 2621 c.c.);
- False comunicazioni sociali delle società quotate (Art. 2622 c.c.);
- Impedito controllo (Art. 2625 c.c.);
- Indebita restituzione dei conferimenti (Art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (Art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote societarie o della società controllante (Art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (Art. 2629 c.c.);
- Omessa comunicazione del conflitto di interessi (Art. 2629-bis c.c.);
- 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.);
- Istigazione alla corruzione tra privati (Art. 2635-bis c.c.);
- Pene accessorie (Art. 2635-ter c.c.);
- 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 c.c.);
- False o omesse dichiarazioni per il rilascio del certificato preliminare (Art. 54 D. Lgs. n. 19 del 2 marzo 2023).

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

Le Aree sensibili
Le Funzioni principalmente sensibili alla realizzazione della fattispecie di reato ex art. 25 *ter* del D. Lgs. 231/2001 sono Finance, Treasury & Networking Capital and Controlling e Legal and Corporate Governance.
La normativa vieta di porre in essere, *inter alia*, i seguenti comportamenti:
- ✓ occultamento di documenti o altri artifici al fine di impedire e ostacolare sindaci, soci, revisori o membri di organi di controllo nello svolgimento dell'attività di controllo;
- ✓ esposizione di fatti materiali non rispondenti al vero o omissione di informazioni, la cui comunicazione è imposta dalla legge, sulla situazione economica, patrimoniale e finanziaria della società o del gruppo al quale essa appartiene, inducendo in errore i destinatari. Soggetti attivi di tali reati possono essere amministratori, CFO, preposti alla redazione dei documenti contabili societari, sindaci e liquidatori. Relativamente all'attività in esame, i reati in oggetto possono essere commessi durante l'iter e le attività propedeutiche all'approvazione del progetto di bilancio e/o nella redazione di qualsivoglia comunicazione sociale, ad esempio omettendo informazioni, ovvero riportando dati falsi o alterati nella documentazione relativa alla contabilità generale;
- ✓ determinazione di poste valutative di bilancio non conformi alla reale situazione patrimoniale, economica e finanziaria della società, in collaborazione con gli amministratori; esposizione in bilancio di altre poste inesistenti o di valore difforme da quello reale, ovvero occultamento di fatti rilevanti tali da mutare la rappresentazione delle effettive condizioni economiche della società;
- ✓ simulazione o fraudolenta disposizione di progetti, prospetti e documentazione da sottoporre all'approvazione dell'assemblea dei soci, anche in concorso con altri;
- ✓ ripartizione dei beni della società tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, cagionando loro un danno;
- ✓ riconoscimento o promessa di denaro o altra utilità a soggetti intermediari quale prezzo della propria mediazione illecita verso un pubblico ufficiale, incaricato di pubblico servizio o uno degli altri soggetti di cui all'art. 322-bis del c.p. per ottenere favori nell'ambito di procedimenti tributari, giudiziari o stragiudiziali;
- ✓ occultamento di documenti o altri artefici al fine di impedire e ostacolare eventuali verifiche e controlli.

Strumenti di controllo del sistema organizzativo
La presente Parte Speciale, oltre agli specifici principi di comportamento relativi alle aree di rischio sopra indicate, richiama i principi generali di comportamento previsti dal presente Modello, alla cui osservanza tutti gli amministratori e dipendenti/collaboratori della società sono tenuti.
Nell'espletamento delle operazioni attinenti alla gestione sociale devono essere adottati e rispettati:
- i protocolli di controllo e le procedure aziendali, la documentazione, le disposizioni inerenti la struttura organizzativa gerarchico-funzionale e la normativa vigente;
- le norme inerenti il sistema amministrativo, contabile, finanziario e di controllo di gestione della società;
- il Modello Organizzativo.

Il Modello prevede l'espresso divieto di:
- porre in essere, collaborare o dare causa all'adozione di comportamenti che – considerati individualmente o collettivamente – integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 ter del Decreto);

- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo, in quanto idonei e diretti in modo univoco alla loro commissione;
- violare i principi e le procedure aziendali parti integranti del Modello stesso.

Le fattispecie di reato ex art. 25-*quater d*el D. Lgs. 231/2001
Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali

Riferimenti normativi:
- Associazioni sovversive (Art. 270 c.p.);
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordinamento democratico (Art. 270-*bis* c.p.);
- Circostanze aggravanti e attenuanti (Art. 270-*bis*.1 c.p.);
- Assistenza agli associati (Art. 270-*ter* c.p.);
- Arruolamento con finalità di terrorismo anche internazionale (Art. 270-*quater* c.p.);
- Organizzazione di trasferimenti per finalità di terrorismo (Art. 270-*quater.1* c.p.);
- Addestramento ad attività con finalità di terrorismo anche internazionale (Art. 270-*quinquies* c.p.);
- Finanziamento di condotte con finalità di terrorismo (Art. 270-*quinquies*.1 c.p.);
- Sottrazione di beni o denaro sottoposti a sequestro (Art. 270-*quinquies*.2 c.p.);
- Detenzione di materiale con finalità di terrorismo (art. 270-*quinquies*.3 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.);
- Atto di terrorismo nucleare (Art. 280-ter c.p.);
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.);
- Sequestro di persona a scopo di coazione (Art. 289-ter c.p.);
- Istigazione a commettere alcuno dei delitti preveduti dai capi primo e secondo (art. 302 c.p.);
- Cospirazione politica mediante accordi (Art. 304 c.p.);
- Cospirazione politica mediante associazione (Art. 305 c.p.);
- Banda armata: formazione e partecipazione (Art. 306 c.p.);
- Associazione ai partecipi di cospirazione o di banda armata (Art. 307 c.p.);
- Fabbricazione o detenzione di materie esplodenti (art. 435 c.p.);
- Impossessamento, dirottamento e distruzione di un aereo o danneggiamento installazioni a terra (Artt. 1 e 2 L. 342/1976).

Attenzione meritano, inoltre, le fattispecie di cui agli artt. 272 c.p. (propaganda ed apologia sovversiva o antinazionale), 280 c.p. (attentato per finalità terroristiche o di eversione), 284 c.p. (insurrezione armata contro i poteri dello Stato), 289-*bis* c.p. (sequestro di persona a scopo di terrorismo o di eversione).
L'analisi dei processi aziendali ha consentito di individuare le attività nel cui ambito potrebbero astrattamente essere realizzate le fattispecie di reato richiamate dall'art. 25 *quater* del D. Lgs. 231/2001 (Reati Finanziamento al terrorismo).

Le Aree Sensibili
Di seguito sono elencate le cosiddette Aree sensibili o a rischio identificate con riferimento ai reati di finanziamento al terrorismo:
- ✓ Finance, Treasury & Networking Capital and Controlling
- ✓ Sales/Proposal
- ✓ Integrated Supply Chain
- ✓ Client & Field Service

Di seguito a titolo esemplificativo, e non esaustivo, sono state individuate attività a rischio:
- ✓ operazioni di natura straordinaria, attraverso la gestione impropria del ruolo ricoperto dalla società, al fine di promuovere, finanziare, costituire, organizzare, ovvero partecipare ad associazioni, sia di carattere nazionale che transnazionale, anche finalizzate ad attività terroristiche o di eversione dell'ordine democratico e anche in caso di cooperazione di esponenti della società con due o più soggetti per il perseguimento di qualsiasi delitto non colposo;
- ✓ la conclusione di contratti per eseguire opere per clienti collegati ad associazioni con finalità terroristiche agevolandone le attività;
- ✓ la conclusione di contratti per la fornitura di beni o manodopera con fornitori collegati ad associazioni con finalità terroristiche (ad es. attraverso fatture false o gonfiate la società potrebbe trasferire risorse finanziarie per finanziare attività terroristiche).

Strumenti di controllo del sistema organizzativo
Per ognuna delle attività sensibili identificate sono stati individuati i sistemi dei controlli e i presidi in essere a mitigazione dei rischi in riferimento ai reati con finalità di terrorismo o di eversione dell'ordine democratico:
- la società garantisce la conformità dell'operatività alle disposizioni vigenti in materia di antiterrorismo/antiriciclaggio, avvalendosi di specifici applicativi in grado di consultare i dati dei nominativi sospetti di finanziamento al terrorismo;
- gli uffici preposti, in conformità alle vigenti prescrizioni di legge e al ruolo rivestito nei rapporti con i fornitori e/o clienti, approntano e consultano le liste antiterrorismo predisposte dagli organismi ufficiali;
- controlli automatici sui nominativi sospetti di terrorismo e Paesi con cui è vietato dalla normativa operare (Black List);
- la società vieta di concludere contratti ovvero aprire nuovi rapporti a favore di soggetti – persone fisiche o persone giuridiche – i cui nominativi siano contenuti nelle Liste antiterrorismo;
- tracciabilità delle attività sia a livello di sistema informatico sia in termini documentali;

- prevedere l'assegnazione di responsabilità per quanto attiene alla gestione delle operazioni potenzialmente sospette di finanziamento al terrorismo;
- protocolli di prevenzione, procedure e Codice Etico.

Le fattispecie di reato ex art. 25-*quinquies* del D. Lgs. 231/2001
Delitti contro la personalità individuale

Riferimenti normativi:
- 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* c.p.)
- Pornografia virtuale (Art. 600-*quater1* c.p.)
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (Art. 600-*quinquies* c.p.)
- Tratta di persone (Art. 601 c.p.)
- Traffico di organi prelevati da persona vivente (art. 601-*bis* c.p.);
- 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.);
- Tortura (Art. 613-*bis* c.p.);
- Istigazione del pubblico ufficiale a commettere tortura (Art. 613-*ter* c.p.);

Le Aree sensibili
Attività sensibili individuate:
1) selezione dei fornitori;
2) rapporti con appaltatori;
3) selezione di partner;
4) rapporti con soggetti terzi che implicano l'utilizzo da parte dell'Ente di manodopera facente capo ai medesimi soggetti terzi.

Reati ipotizzabili:
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
- Riduzione o mantenimento in schiavitù o in servitù;
- Intermediazione illecita e sfruttamento del lavoro.

Strumenti di controllo del sistema organizzativo
Nelle aree "a rischio reato" considerate sono presenti i seguenti Presidi di Controllo Generali (a cui si aggiungono Presidi di Controllo Specifici in relazione a singole attività sensibili o categorie di attività sensibili):
1) Codice Etico;
2) formazione in ordine al Modello e alle tematiche di cui al D. Lgs. n. 231/2001, rivolta alle risorse operanti nell'ambito delle aree a rischio, con modalità di formazione appositamente pianificate in considerazione del ruolo svolto;
3) diffusione del Modello tra le risorse interne, mediante consegna di copia su supporto documentale o telematico e pubblicazione del Modello e dei protocolli maggiormente significativi (ad es., Codice Etico, Sistema Disciplinare, Procedure rilevanti, ecc.) sulla intranet aziendale;
4) diffusione del Modello tra i Terzi Destinatari tenuti al rispetto delle relative previsioni (ad es., fornitori, appaltatori, consulenti) mediante pubblicazione dello stesso sul sito della società o messa a disposizione in formato cartaceo o telematico;
5) dichiarazione con cui i Destinatari del Modello, inclusi i Terzi Destinatari (ad es., fornitori, consulenti, appaltatori), si impegnano a rispettare le previsioni del Decreto;
6) Sistema Disciplinare volto a sanzionare la violazione del Modello e dei Protocolli ad esso connessi, ivi compreso quello previsto dal CCNL applicabile;
7) acquisizione di una dichiarazione, sottoscritta da ciascun destinatario del Modello di impegno al rispetto dello stesso, incluso il Codice Etico;
8) creazione di una "Sezione 231" all'interno della intranet, presso cui pubblicare tutti i documenti rilevanti nell'ambito del Modello (ad es. Modello, Codice Etico, Protocolli interni ove richiamati).

Le fattispecie di reato ex art. 25-*septies* del D. Lgs. 231/2001
Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Riferimenti normativi:
- Omicidio colposo (Art. 589 c.p.);
- Lesioni personali colpose (Art. 590 c.p.);
- Sanzioni per il datore di lavoro ed il dirigente (Art. 55 D. Lgs. n. 81 del 9 aprile 2008).

Le attività sensibili individuate, in riferimento al reato di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro richiamati dall'art. 25 *septies* del D. Lgs. 231/2001, sono tutte le aree e i processi aziendali con presenza di fattori di rischio, come individuati nel Documento di Valutazione dei Rischi ai sensi del D. Lgs. 81/2008 e s.m.i.

Le Aree Sensibili
Di seguito sono elencate le cosiddette Aree sensibili o a rischio identificate con riferimento ai reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro:
- ✓ HSE Department (Health, Safety, Environment) – RSPP – Datore di Lavoro – D.D.L. e Dirigenti Preposti.

Di seguito a titolo esemplificativo, e non esaustivo, sono ad esempio attività a rischio:
- ✓ violazione o omissioni, scarsa diligenza, imprudenza o imperizia, da parte della società, nell'adempimento degli obblighi derivanti dalle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (es. omessa attività di valutazione dei rischi, di controllo, prevenzione, formazione, protezione, predisposizione di flussi documentali previsti ex lege, etc.) che possano implicare le fattispecie di reato di omicidio colposo o lesioni colpose in caso di infortunio grave o gravissimo di dipendenti o collaboratori;
- ✓ mancata/non corretta definizione del sistema di procure/deleghe/nomine in materia di salute e sicurezza sui luoghi di lavoro: RSPP – ASPP – RLS – Addetti alla gestione delle emergenze (emergenze, incendio, primo soccorso) – Medico;
- ✓ competente – Delegato del datore di lavoro – Sostituto delegato del datore di lavoro;
- ✓ mancata/non completa adozione della documentazione in materia di sicurezza e salute sul luogo di lavoro prevista dalla normativa e nel SSL; es: documento di valutazione dei rischi (DVR), istruzioni gestione delle emergenze, istruzioni primo soccorso, istruzioni evacuazione, istruzioni sorveglianza sanitaria, segnaletica di sicurezza;
- ✓ mancata/non completa verifica periodica sul rispetto delle prescrizioni in materia di sicurezza e salute sul luogo di lavoro previste dalla normativa e nel SSL, ivi incluse le visite periodiche in materia sanitaria.

Strumenti di controllo del sistema organizzativo
La società si è dotata di un Sistema di Sicurezza sul Lavoro (SSL), che disciplina obblighi e modalità in materia di salute e sicurezza sul lavoro, individuando ruoli e responsabilità, nello specifico:
- Modello organizzativo per l'applicazione del D. Lgs. 81/08 in tema di salute e sicurezza sul luogo di lavoro;
- linee guida aziendali per la gestione delle emergenze e della segnaletica di sicurezza;
- linee guida aziendali per la gestione della informazione, formazione e comunicazione in tema di salute e sicurezza sui luoghi di lavoro, tale da garantire a tutti i livelli aziendali conoscenze utili all'identificazione, riduzione e gestione dei rischi in ambiente di lavoro;
- linee guida aziendali per la gestione di impianti, macchine, attrezzature, sostanze e dispositivi di protezione individuale;
- linee guida aziendali per la gestione della sorveglianza sanitaria;
- linee guida aziendali per la gestione dei presidi di sicurezza negli appalti di lavori, servizi e forniture, ivi inclusi gli aspetti riguardanti i costi della sicurezza nei contratti;
- procedura per il monitoraggio e aggiornamento del Sistema di Sicurezza sul Lavoro (SSL);
- linee guida per la valutazione dei rischi, che descrive la metodologia per una corretta esecuzione e gestione della valutazione dei rischi, oltre che per l'esecuzione e l'aggiornamento/verifica della valutazione del rischio e la redazione dei relativi documenti di valutazione dei rischi (DVR);
- procedure interne, protocolli 231 e Codice Etico.

Le fattispecie di reato ex art. 25-*octies* del D. Lgs. 231/2001
Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

Riferimenti normativi:
- Ricettazione (Art. 648 c.p.);
- Riciclaggio (Art. 648-*bis* c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (Art. 648-*ter* c.p.);
- Autoriciclaggio (Art. 648-*ter* 1 c.p.).

La normativa italiana in tema di prevenzione dei Reati di Riciclaggio prevede norme tese a ostacolare le pratiche di riciclaggio, vietando tra l'altro l'effettuazione di operazioni di trasferimento di importi rilevanti con strumenti anonimi e assicurando la ricostruzione delle operazioni attraverso l'identificazione e l'adeguata verifica della clientela e la registrazione dei dati in appositi archivi.
Nello specifico, il corpo normativo in materia di riciclaggio è costituito anzitutto dal Decreto Antiriciclaggio, che in parte ha abrogato e sostituito la L. 197/1991.

Le Aree Sensibili
Nell'ambito del *Risk Assessment*, svolto dalle strutture interne competenti e aggiornato annualmente, anche attraverso interviste alle risorse delle Divisioni/Aree interessate a conoscenza dello specifico ambito analizzato, sono individuate tutte le attività a rischio reato inerenti la presente parte speciale e riferite ai macro-processi ed ai processi aziendali. A seguito di una approfondita analisi della sua realtà aziendale, le principali Attività Sensibili che la società ha individuato al proprio interno sono le seguenti:
- ✓ Finance, Treasury & Networking Capital and Controlling
- ✓ Sales/Proposal
- ✓ People & Culture / HR Administration
- ✓ Legal and Corporate Governance
- ✓ Integrated Supply Chain
- ✓ Quality & Welding
- ✓ Client & Field Service

In relazione alle descritte Attività Sensibili – tutte astrattamente ipotizzabili – si ritengono particolarmente coinvolti alcuni organi e funzioni aziendali.
Di seguito a titolo esemplificativo, e non esaustivo, sono ad esempio attività a rischio:
- ✓ operazioni straordinarie e di Merger & Acquisition effettuate attraverso proventi derivanti dalla commissione o dalla partecipazione in concorso a delitti non colposi, con condotte finalizzate a ostacolare concretamente l'identificazione della provenienza delittuosa delle risorse impiegate;
- ✓ relativamente a tale tipo d'attività, i reati di riciclaggio o impiego di denaro o altre utilità potrebbero verificarsi nell'interesse e/o a vantaggio della società mediante vendite a clienti nuovi di cui è difficoltoso l'accertamento dell'oggetto sociale, la conoscenza del profilo economico e la verifica nel tempo della titolarità del rapporto commerciale (per esempio nel caso di continui mutamenti della compagine sociale);
- ✓ violazione della vigente normativa in materia di antiriciclaggio realizzata attraverso una gestione impropria del ruolo ricoperto in azienda al fine di instaurare/mediare rapporti negoziali finalizzati a sostituire, trasferire denaro, beni, altra utilità di origine illecita, ovvero a porre in essere una serie di azioni mirate a rendere complesso identificarne la provenienza, con particolare ma non esclusivo riferimento a transazioni con paesi c.d. "blacklist";
- ✓ utilizzo di denaro proveniente da attività illecite (ad es. reati commessi nell'ambito delle dichiarazioni dei redditi della società stessa) per il pagamento delle note spese;
- ✓ evasione delle imposte sui redditi o sul valore aggiunto mediante l'utilizzo di fatture per operazioni (anche in parte) inesistenti e impiego delle risorse così ottenute per effettuare una donazione;
- ✓ processo di selezione del fornitore/appaltatore al fine di generare un beneficio economico per la società (es. prezzo d'acquisto maggiormente competitivo), mediante l'importazione di beni/prodotti contraffatti e/o alterati.

Strumenti di controllo del sistema organizzativo
La presente Parte Speciale si riferisce a comportamenti posti in essere da amministratori, dirigenti, dipendenti nonché collaboratori esterni e partner della società, compresi gli eventuali soggetti appartenenti ad altre società coinvolti nella gestione delle aree di attività a rischio, e comunque di chi, anche solo di fatto, rientri nelle categorie di apicali o subordinati della società.
Si è ritenuto che, per la prevenzione di detti reati, possano svolgere un'adeguata funzione preventiva:
- protocolli specifici di prevenzione che costituiscono parte integrante del Modello di Organizzazione, Gestione e Controllo *ex* D. Lgs. 231/01 adottato dalla società;
- i principi presenti nel Codice Etico;
- procedure aziendali che costituiscono parte integrante del Corporate Compliance Program del Gruppo Sofinter;
- tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici;
- segregazione dei compiti (applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla);
- esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate (devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni).

Le fattispecie di reato ex art. 25-*octies*.1 del D. Lgs. 231/2001
Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori

Riferimenti normativi:
- 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.);
- Trasferimento fraudolento di valori (Art. 512-bis c.p.);
- Frode informatica (Art. 640-*ter* c.p.).

Le Aree Sensibili
Le fattispecie di cui all'art. 25 *octies*-1 potrebbero assumere rilevanza in riferimento alle attività di riscossione delle vendite che richiedono l'impiego di strumenti di pagamento diversi dal contante, quali vendite online, pagamenti con l'impiego di dispositivi che consentono l'utilizzo di moneta elettronica, carte prepagate, di debito o di credito.
Inoltre, il campo di applicazione della Direttiva è relativo non solo ai mezzi di pagamento diversi dal contante c.d. "tradizionali", ma anche al denaro virtuale e ai relativi pagamenti che impiegano il denaro elettronico, valuta virtuale e pagamenti tramite telefoni cellulari.
Le Funzioni principalmente sensibili alla realizzazione della fattispecie di reato *ex* art. 25 *octies*-1 sono le seguenti:
- Finance, Treasury & Networking Capital and Controlling.

Le attività sensibili individuate sono le seguenti:
- ✓ Personale della società, avendo ricevuto carte di credito o di pagamento contraffatte o clonate, le utilizza effettuando transazioni relative a spese di trasferta;
- ✓ Attività strumentale alla realizzazione dei reati di corruzione/induzione indebita a dare o promettere utilità/traffico di influenze illecite. I flussi monetari e finanziari in uscita aventi l'obiettivo di assolvere le obbligazioni di varia natura contratte dalla società potrebbero costituire supporto alla costituzione di disponibilità finanziarie – sia in Italia che all'estero – destinabili al Pubblico Ufficiale, Incaricato di Pubblico Servizio o Soggetto Privato.

Strumenti di controllo del sistema organizzativo
Con riferimento ai delitti in materia di strumenti di pagamento diversi dai contanti, si rimanda ai principi di controllo riportati nei Reati informatici e nei Reati contro la Pubblica Amministrazione.
Ad integrazione delle regole comportamentali di carattere generale, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei delitti in materia di strumenti di pagamento diversi dai contanti, con particolare riferimento ai processi strumentali alla commissione dei reati quali la gestione dei flussi monetari e finanziari:
- ogni movimentazione di cassa deve essere autorizzata dai soggetti dotati di idonei poteri e supportata da opportuna documentazione;
- le carte di credito attingono al conto corrente della società e possono essere esclusivamente utilizzate per le cd. "spese di cantiere". La società non ammette l'uso promiscuo delle carte di credito, le quali sono provviste del nominativo del dipendente al quale esse sono assegnate;
- i pagamenti sono effettuati tramite strumenti che ne assicurano la tracciabilità (e.g. bonifici bancari, etc.) e, solo in via residuale e previa autorizzazione, tramite l'utilizzo di contanti nel rispetto dei limiti previsti dalle leggi vigenti;
- i pagamenti devono sempre essere effettuati in favore del soggetto che ha erogato il bene e/o il servizio, con obbligo di effettuare controlli specifici sull'identità di interposte persone;
- le operazioni che comportano l'utilizzo o impiego di risorse economiche o finanziarie devono sempre avere una causale espressa e devono essere documentate e registrate in conformità ai principi di correttezza e trasparenza contabile;
- gli incassi e i pagamenti della società, nonché i flussi di denaro devono sempre essere tracciabili e provabili documentalmente;
- sono previsti la verifica della regolarità dei pagamenti anche con riferimento alla coincidenza tra destinatario/ordinante e controparte effettivamente coinvolta nella transazione e il controllo della correttezza dei flussi finanziari aziendali con riferimento ai pagamenti verso terzi;
- per la gestione dei flussi in entrata e in uscita, sono utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione Europea o enti creditizi/finanziari situati in uno Stato extracomunitario che imponga obblighi equivalenti a quelli previsti dalle leggi sul riciclaggio e preveda il controllo del rispetto di tali obblighi;
- sono effettuati controlli formali e sostanziali e un costante monitoraggio dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi, tenendo conto della sede legale della società controparte, degli istituti di credito utilizzati, di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- la società assicura il tracciamento del numero delle carte di credito assegnate ai dipendenti risalendo dal conto corrente ad essa intestata;
- è vietato utilizzare conti correnti in forma anonima o con intestazione fittizia, né in Italia né presso altri Stati esteri;
- i titolari delle firme elettroniche e/o digitali sono individuati in base ai regolamenti contrattuali con le Autorità di Certificazione emittenti delle firme; la custodia e l'utilizzo dei dispositivi di firma elettronica e/o digitale sono rimessi ai titolari degli stessi e devono conformarsi ai regolamenti contrattuali con le Autorità di Certificazione emittenti delle firme.

Le fattispecie di reato ex art. 25-*octies.2* del D. Lgs. 231/2001
Delitti in materia di violazione di misure restrittive dell'Unione Europea [Articolo aggiunto dal D. Lgs. n. 211 del 30/12/2025]

Riferimenti normativi:
- Violazione delle misure restrittive dell'Unione Europea (Art. 275-*bis* c.p.);
- Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione Europea (Art. 275-*ter* c.p.);
- Violazione delle condizioni dell'autorizzazione allo svolgimento di attività (Art. 275-*quater* c.p.);
- Violazione colposa di misure restrittive dell'Unione Europea (Art. 275-*quinquies* c.p.)

Le Aree Sensibili
Le aree a rischio riguardano i processi con impatto su export, import, transazioni internazionali, obblighi informativi e rapporti con soggetti sanzionati.
- **Area Export / Commercio Internazionale**

Rischi:
- ✓ esportazione o riesportazione di beni verso Paesi o soggetti sanzionati (Russia, Bielorussia, Iran, Siria, ecc.);
- ✓ vendita di beni *dual use* senza autorizzazioni;
- ✓ contratti con entità ufficialmente non sanzionate ma controllate da soggetti designati (reato di elusione).

- **Area Acquisti e Supply Chain**

Spesso gli impianti includono parti prodotte o integrate tramite:
- ✓ fornitori esteri,
- ✓ subappaltatori,
- ✓ distributori.

La catena può nascondere soggetti sanzionati o destinazioni finali vietate, anche tramite triangolazioni. Rischio: elusione indiretta delle sanzioni UE tramite Paesi non soggetti a restrizioni ma utilizzati come "scudo".
- **Progettazione e assistenza tecnica su impianti in Paesi soggetti a sanzioni**

Le misure restrittive UE non colpiscono solo beni materiali, ma anche:
- ✓ servizi di ingegneria,
- ✓ assistenza tecnica,
- ✓ consulenze per progettazione, installazione, manutenzione.

Prestare assistenza tecnica a entità sanzionate è vietato. Rischio: configurazione di "prestazione di servizi vietati", anche senza trasferimento di beni.
- **Pagamenti internazionali e finanziamenti di progetto**

Le società di impiantistica operano spesso tramite:
- ✓ anticipi,
- ✓ lettere di credito,
- ✓ escrow account,
- ✓ finanziamenti strutturati.

Le misure restrittive possono vietare operazioni finanziarie con determinati soggetti. Rischio: movimentazione di fondi per conto o a favore di soggetti sanzionati (reclusione + multa).
- **Ignoranza o omissione degli obblighi informativi**

Nel settore impiantistico è tipico gestire:
- ✓ beni in transito,
- ✓ depositi temporanei,
- ✓ magazzini doganali,
- ✓ fondi per appalti esteri.

Rischio: responsabilità per mancata comunicazione anche involontaria.
- **Gestione di documentazione tecnica e commerciale**

Nel settore impiantistico la documentazione coinvolge:
- ✓ schede tecniche,
- ✓ manuali,
- ✓ certificazioni di conformità,
- ✓ dichiarazioni di uso finale.

Rischio: una documentazione imprecisa può configurare condotta elusiva.

Strumenti di controllo del sistema organizzativo
1) Screening e verifica delle controparti
Lo screening è considerato uno dei meccanismi più importanti per evitare:
- rapporti con soggetti designati,
- operazioni vietate,
- elusioni tramite società schermo o Paesi terzi.

Strumenti operativi:
- verifica automatizzata su liste UE (consolidated list), ONU, OFAC, UK HMT;
- controllo del titolare effettivo (beneficial owner) per evitare interposizioni;
- monitoraggio continuo (non solo al momento della stipula).

2) Controlli su beni, tecnologie e servizi

Il decreto evidenzia la necessità di controllare beni e servizi con rischio di rilevanza strategica, in particolare:

- *dual use*,
- prodotti militari,
- componenti tecnologiche soggette a restrizioni,
- servizi di assistenza tecnica.

Strumenti:

- classificazione dei beni (codici doganali, ECCN, dual use);
- verifica delle autorizzazioni UE e nazionali;
- embargo check per Paesi soggetti a misure restrittive;
- blocco automatico dell'export in assenza di clearance.

3) Controllo delle operazioni finanziarie

Strumenti:

- filtri su pagamenti internazionali verso banche/istituzioni colpite da restrizioni;
- verifiche su lettere di credito, escrow accounts, project financing;
- blocco automatico dei pagamenti sospetti;
- revisione del flusso di approvazione delle transazioni.

4) Controllo dei flussi documentali

Strumenti:

- gestione digitale e tracciabile di tutta la documentazione di export e contrattuale;
- verifica dell'uso finale (EUC – End Use Certificate);
- controlli formali e sostanziali su: fatture, polizze di carico, contratti, schede tecniche.

5) Monitoraggio della supply chain e dei Paesi terzi

Strumenti:

- verifica dei subfornitori e subappaltatori;
- controllo del Paese di origine/destinazione effettiva delle merci;
- audit periodici su fornitori a rischio;
- inserimento di clausole contrattuali sanctions-compliant.

6) Obblighi informativi e procedure interne di segnalazione

Strumenti:

- procedure interne di reporting verso autorità (MEF, Banca d'Italia, ADM);
- flussi informativi chiari tra funzioni aziendali;
- canali di whistleblowing specifici per sanzioni UE.

Le fattispecie di reato ex art. 25-*novies* del D. Lgs. 231/2001
Delitti in materia di violazione del diritto d'autore

Riferimenti normativi:

- Messa a disposizione del pubblico di un'opera dell'ingegno protetta o parte di essa - Reati commessi su opera altrui non destinata alla pubblicazione qualora ne risulti offeso l'onore/reputazione (Art. 171 Legge 22 aprile 1941, n. 633);
- Abusiva pubblicazione contenuta in supporti non contrassegnati ai sensi della legge 166/2024 - Riproduzione trasferimento su altro supporto del contenuto della banca dati (Art. 171-b*is* Legge 22 aprile 1941, n. 633);
- Abusiva duplicazione di opere dell'ingegno destinate al circuito televisivo, cinematografico, etc. (Art. 171-*ter* Legge 22 aprile 1941, n. 633);
- Mancata comunicazione dei dati di identificazione dei supporti ai sensi della Legge n. 166/2024 (Art. 171-*septies* Legge 22 aprile 1941, n. 633);
- Fraudolenta produzione, vendita o importazione di apparati di decodifica (Art. 171-*octies* Legge 22 aprile 1941, n. 633);
- Utilizzare, duplicare, riprodurre in modo abusivo opere o materiali protetti (Art. 174-*te*r Legge 22 aprile 1941, n. 633);
- Obblighi di segnalazioni e notifiche (Art. 174-*sexies* Legge 22 aprile 1941, n. 633);
- Accordi tra SIAE, altri organismi di gestione collettiva ed entità di gestione indipendenti (Art. 181-*bis* – Legge 22 aprile 1941, n. 633).

Le Aree sensibili

Le attività sensibili individuate, in riferimento ai Delitti in materia di violazione del diritto d'autore richiamati dall'art. 25 *novies* del D. Lgs. 231/2001, sono le seguenti:

- ✓ Utilizzo di risorse e informazioni di natura informatica o telematica, ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore (con particolare riferimento alle occasioni di reato "Gestione delle attività connesse all'acquisto e all'utilizzo di software, banche dati o di qualsiasi altra opera dell'ingegno tutelata dal diritto d'autore" e "Gestione delle attività connesse all'implementazione e/o aggiornamento del sito internet e, più in generale, utilizzo della rete telematica aziendale");
- ✓ Gestione delle attività di presentazione della società al pubblico;
- ✓ Utilizzo improprio di opere o di parte di opere (es. grafiche, letterarie, ecc.) protette dal diritto d'autore;
- ✓ Utilizzo improprio, ad esempio nel corso di un convegno o di altra presentazione in pubblico, di opere o di parte di opere protette dal diritto d'autore;
- ✓ Utilizzo di software, banche dati o altra opera dell'ingegno in assenza di idonea o valida licenza/autorizzazione da parte del titolare dei relativi diritti;
- ✓ Gestione abusiva, fraudolenta o comunque impropria di opere altrui o di parti di esse, attraverso la loro pubblicazione sul sito internet o comunque la loro diffusione attraverso la rete telematica aziendale.

Strumenti di controllo del sistema organizzativo

Per le operazioni riguardanti la gestione di server, siti internet, social network e diffusione di notizie verso l'interno/esterno, la gestione delle informazioni coperte da diritto d'autore/proprietà intellettuale, la gestione delle attività di acquisizione e sviluppo di apparecchiature, dispositivi (anche di rilevazione) o programmi informatici e di servizi di installazione, manutenzione, connessione o di altra natura relativi a hardware, software e reti relative, componenti tecniche connesse con il sistema, i protocolli/procedure prevedono che:

- le opere/informazioni protette da diritto d'autore/proprietà intellettuale acquistate dalla società ai fini dell'attività aziendale siano catalogate in un apposito database;
- per le opere/informazioni delle quali siano state acquisite le licenze d'uso, il database comprenda anche i seguenti dati: (i) data di acquisto della licenza; (ii) data di scadenza della licenza; (iii) tipo di utilizzo autorizzato dal contratto di licenza (es. upload su sito internet, diffusione in pubblico, utilizzo per brochure e relativo numero di copie massime utilizzabili, ecc.);
- siano definiti e attivati criteri e modalità per controllare l'accesso da parte degli utenti a siti di download di contenuti;
- siano previsti controlli da parte del Dipartimento/Ufficio competente sulle attività che comportano l'utilizzo di opere/informazioni tutelate dal diritto d'autore/proprietà intellettuale;
- siano definiti i criteri e le modalità per la gestione dei sistemi software, che devono prevedere la compilazione e manutenzione di un inventario aggiornato dei software in uso presso la società;
- siano definiti e attivati criteri e modalità per controllare che l'acquisto e l'uso di software e di altre opere/informazioni tutelate dal diritto di autore/proprietà intellettuale siano formalmente autorizzati e certificati;
- sia prevista l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o non licenziati e/o potenzialmente nocivi;
- le applicazioni tengano traccia delle modifiche ai dati e ai sistemi compiute dagli utenti (qualora la gestione della presente attività sia affidata in outsourcing, i contratti che regolano i rapporti con i fornitori del servizio prevedano apposite clausole che impongano, per i fornitori di software, la conformità dei software forniti a leggi e normative vigenti e la manleva per la società in caso di violazioni commesse dai fornitori del servizio stessi).

Le fattispecie di reato ex art. 25-*decies* del D. Lgs. 231/2001
Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria

Riferimenti normativi:
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 377-*bis* c.p.).

L'analisi dei processi della società ha consentito di individuare le seguenti attività "sensibili", nel cui ambito potrebbe astrattamente realizzarsi la fattispecie di reato in oggetto:
- ✓ Gestione dei rapporti con l'Autorità Giudiziaria;
- ✓ Gestione consulenze e prestazioni professionali;
- ✓ Gestione di eventuali contenziosi giudiziali e stragiudiziali.

Le Aree sensibili
Le Funzioni principalmente sensibili alla realizzazione della fattispecie di reato ex art. 25-*decies* del D. Lgs. 231/2001 sono People & Culture/HR Administration e Legal and Corporate Governance.
La normativa vieta di porre in essere i seguenti comportamenti:
- ✓ usare violenza o minaccia, compiere atti intimidatori ovvero offrire o promettere denaro o altra utilità al fine di indurre un soggetto chiamato a rendere dichiarazioni avanti l'autorità giudiziaria, a non rendere tali dichiarazioni o a rendere dichiarazioni mendaci.

Strumenti di controllo del sistema organizzativo
Ai fini dell'attuazione delle regole comportamentali in conformità a quanto previsto dal D. Lgs. 231, i Destinatari della presente Parte Speciale del Modello, oltre a rispettare le previsioni di legge esistenti in materia, le norme nel Codice Etico e i principi indicati nella Parte Generale del presente Modello, devono rispettare i protocolli comportamentali, posti a presidio dei rischi-reato sopra identificati e riferibili alle attività a rischio.
Si rinvia anche a quanto indicato nel Codice Etico e nelle procedure e protocolli per quanto attiene i principi specifici di comportamento e gli standard di controllo esistenti in merito a:
- gestione di consulenze e prestazioni professionali
- gestione di eventuali contenziosi giudiziali e stragiudiziali.

Le fattispecie di reato ex art. 25-*undecies* del D. Lgs. 231/2001
Reati ambientali

Riferimenti normativi:
- Inquinamento ambientale (Art. 452-*bis* c.p.);
- Commercio di prodotti inquinanti (Art. 452-*bis*.1 c.p.)
- Morte o lesioni come conseguenza del delitto di inquinamento ambientale e di commercio di prodotti inquinanti (Art. 452-*ter* c.p.);
- Disastro ambientale (Art. 452-*quater* c.p.);
- Delitti colposi contro l'ambiente (Art. 452-*quinquies* c.p.);
- Traffico e abbandono di materiale ad alta radioattività (Art. 452-*sexies* c.p.);
- Impedimento del controllo (Art. 452-*septies* c.p.);
- Circostanze aggravanti (Art. 452-*octies* c.p.);
- Omessa bonifica (Art. 452-*terdecies* c.p.);
- Attività organizzate per il traffico illecito di rifiuti (Art. 452-*quaterdecies* c.p.);
- Nozione di abusività (Art. 452-*quinquiesdecies*);
- Circostanze aggravanti (Art. 452-sexiesdecies);
- Uccisione, distruzione, cattura, prelievo, detenzione e commercio 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.) – ABROGATO dal D. lgs. n. 81 del 21 aprile 2026;
- Codice dell'Ambiente – D. Lgs 152/06;
- Legge 7 febbraio 1992, n. 150;
- Legge 28 dicembre 1993, n. 549 – Misure a tutela dell'ozono stratosferico e dell'ambiente;
- D. Lgs 6 novembre 2007 n. 202 – Attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni.

Le Aree sensibili

La presente Parte Speciale si riferisce ai reati ambientali richiamati dall'art. 25 *undecies* del D. Lgs. 231/2001 e in particolare individua le cosiddette attività "sensibili" (quelle dove è teoricamente possibile la commissione del reato e che sono state individuate nell'ambito dell'attività di *risk assessment*), specificando i principi comportamentali e i presidi di controllo operativi per l'organizzazione, lo svolgimento e la gestione delle operazioni svolte nell'ambito delle sopracitate attività "sensibili".

Di seguito sono elencate le Aree sensibili o a rischio identificate con riferimento ai reati ambientali:
- ✓ HSE Department (Health, Safety, Environment) – Servizi Generali – Manutentori

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale i seguenti reati:
- ✓ assenza o scarsa manutenzione del depuratore che comporti scarichi oltre i limiti;
- ✓ gestione non corretta delle attività operative (es. dosaggio di sostanze chimiche in produzione) che genera un superamento dei limiti nelle acque di scarico;
- ✓ sversamento di sostanze chimiche pericolose nella rete idrica che comporti il superamento dei limiti autorizzati;
- ✓ violazione e/o mancati controlli di quanto previsto dall'autorizzazione;
- ✓ realizzazione e conduzione di scarichi non autorizzate/sospese/revocate (scarichi di acque reflue industriali art. 137 comma 2, 3, 5, 11 e 13 D. Lgs. 152/06; scarichi di sostanze pericolose art. 108 D. Lgs. 152/06);
- ✓ falsa indicazione sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione del certificato di analisi dei rifiuti, ovvero utilizzo di un certificato di analisi falso durante il trasporto di rifiuti propri non pericolosi (traffico illecito di rifiuti art. 259 D. Lgs.152/2006; violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari D. Lgs. 152/06, art. 258, comma 4);
- ✓ aree di deposito non adeguatamente pavimentate/impermeabilizzate (inquinamento ambientale art. 452-bis c.p.);
- ✓ gestione/manutenzione non corretta degli impianti produttivi, conduzione delle attività in difformità alle prescrizioni autorizzative/mancati controlli (prevenzione e limitazione delle emissioni in atmosfera D. Lgs. n. 152/06, art. 279, comma 5; inquinamento ambientale art. 452 bis c.p.);
- ✓ violazione del divieto di utilizzo di sostanze lesive per l'ozono stratosferico (cessazione e riduzione dell'impiego di sostanze lesive art. 3 comma 6 legge 549/93; inquinamento ambientale art. 452 *bis* c.p.).

Strumenti di controllo del sistema organizzativo

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo *ex* D. Lgs.231/2001, del Codice Etico, nello svolgimento delle attività sensibili sopra citate, tutti i Destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento e controllo: adottare comportamenti prudenti, corretti, trasparenti e collaborativi per la salvaguardia dell'ambiente, conformemente alla propria formazione ed esperienza, nonché alle istruzioni ed ai mezzi forniti o predisposti dalla società.

In linea generale, è richiesto di:
- rispettare la normativa al fine della protezione dell'ambiente, esercitando in particolare ogni opportuno controllo e attività idonee a salvaguardare l'ambiente stesso;
- utilizzare correttamente le apparecchiature e le altre attrezzature di lavoro al fine di evitare problematiche in materia ambientale;
- adoperarsi direttamente, a fronte di un pericolo rilevato e nei soli casi di urgenza, compatibilmente con le proprie competenze e possibilità;

- svolgere l'attività di gestione e smaltimento dei rifiuti con il minor impatto ambientale possibile;
- adempimenti in materia di salute e sicurezza dei lavoratori (*ex* D. Lgs. 81/2008) e normativa ambientale;
- procedure e Codice Etico.

Le fattispecie di reato ex art. 25-*duodecies* del D. Lgs. 231/2001
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Riferimenti normativi:
- Decreto Legislativo 25 luglio 1998, n. 286 – "Testo Unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero".

Tale reato è costituito dalla condotta di chi, in qualità di datore di lavoro, occupa alle proprie dipendenze lavoratori stranieri privi del permesso di soggiorno, ovvero il cui permesso sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, ovvero sia revocato o annullato se i lavoratori occupati sono (alternativamente):
- in numero superiore a tre;
- minori in età non lavorativa;
- sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'art. 603-*bis* c.p., cioè esposti a situazioni di grave pericolo, con riferimento alle prestazioni da svolgere e alle condizioni di lavoro.

Le Aree sensibili
- People & Culture/HR Administration
- Integrated Supply Chain

Le attività sensibili individuate, in riferimento ai delitti richiamati dall'art. 25 *duodecies* del D. Lgs. 231/2001, sono le seguenti:
- ✓ Selezione e assunzione del personale: impiego di lavoratori stranieri privi del permesso di soggiorno o con permesso scaduto del quale non sia stato chiesto, nei termini di legge, il rinnovo o con permesso revocato o annullato;
- ✓ Scelta del fornitore/appaltatore: scelta di fornitori che non assicurano adeguate tutele nei confronti dei propri dipendenti o che impiegano lavoratori stranieri privi del permesso di soggiorno o con permesso scaduto del quale non sia stato chiesto, nei termini di legge, il rinnovo, o con permesso revocato o annullato;
- ✓ Scelta del fornitore/appaltatore: scelta di fornitori che sottopongono i lavoratori a condizioni di particolare sfruttamento o mantengono gli stessi in stato di soggezione continuativa.

Strumenti di controllo del sistema organizzativo
La presente Parte Speciale prevede l'espresso divieto a carico della società (e dei Destinatari, Dipendenti, e Consulenti/Partner nella misura necessaria alle funzioni dagli stessi svolte) di:
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- violare i principi e le procedure esistenti in azienda e/o previste nella presente Parte Speciale.

Nello specifico è fatto assoluto divieto di:
1. Assumere o comunque impiegare lavoratori stranieri privi di regolare permesso di soggiorno;
2. Assumere o comunque impiegare lavoratori stranieri il cui permesso di soggiorno sia scaduto e del quale non sia stato chiesto il rinnovo nei termini di legge;
3. Assumere o comunque impiegare lavoratori stranieri il cui permesso di soggiorno sia stato revocato o annullato.

Ai fini dell'attuazione delle regole elencate, devono rispettarsi, oltre ai principi generali contenuti nella Parte generale del Modello e nel Codice Etico, anche i protocolli di controllo e le procedure aziendali specifiche.

Le fattispecie di reato ex art. 25-*quinquiesdecies* del D. Lgs. 231/2001
Reati tributari

Riferimenti normativi:
- 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. 74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, commi 1 e 2-*bis*, D. Lgs. 74/2000);
- Occultamento o distruzione di documenti contabili (art. 10, D. Lgs. 74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art. 11, D. Lgs. 74/2000);
- Dichiarazione infedele (art. 4, D. Lgs. 74/2000);
- Omessa dichiarazione (art. 5, D. Lgs. 74/2000);
- Indebita compensazione (art. 10-*quater*, D. Lgs. n. 74/2000).

Le Aree sensibili

Le attività di *risk assessment* svolte hanno individuato per i reati sopra indicati le seguenti attività "sensibili", ovvero quei processi aziendali per i quali si è ritenuto astrattamente sussistente il rischio di commissione dei reati in esame:
- Finance, Treasury & Networking Capital and Controlling.

Destinatari della presente Parte Speciale sono gli amministratori, il responsabile della funzione preposta alla redazione dei documenti contabili societari e della relativa documentazione fiscale, i sindaci, i revisori contabili, nonché i dipendenti soggetti a vigilanza e controllo da parte dei soggetti apicali nelle aree di attività a rischio. Le attività sensibili individuate, in riferimento ai Reati tributari richiamati dall'art. 25 *quinquiesdecies* del D. Lgs. 231/2001, sono le seguenti:

✓ Gestione fiscalità:
  - dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, ad esempio allo scopo di ottenere risparmi di imposta;
  - dichiarazione fraudolenta mediante altri artifici, quali ad esempio documenti falsi finalizzati all'evasione fiscale;
  - emissione di fatture o altri documenti per operazioni inesistenti, così da permettere ad altre società di evadere le imposte;
  - occultamento o distruzione di documenti contabili, in modo tale da rendere impossibile la ricostruzione effettiva del volume di affari della società;
  - sottrazione fraudolenta al pagamento delle imposte, esemplificata dalla dispersione di beni societari atta a generare un risparmio fraudolento per la società.

✓ Finance:
  - la società registra nella contabilità fatture per operazioni (anche in parte) inesistenti, da utilizzare al fine di evadere le imposte sui redditi o sul valore aggiunto;
  - la società indica in bilancio poste simulate supportate da documenti falsi, al fine di potere indicare in dichiarazione elementi passivi fittizi o elementi attivi inferiori a quelli reali;
  - la società occulta documenti contabili ostacolando così la ricostruzione del reddito da parte degli organi dell'Amministrazione Finanziaria.

✓ Finance:
  - dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsti dall'art. 2 D.L. 10/03/2000 n. 74.

Strumenti di controllo del sistema organizzativo

La presente parte speciale prevede l'espresso obbligo di:
- tenere comportamenti in linea con i principi espressi nel Codice Etico e nel presente Modello Organizzativo;
- rispettare le procedure adottate con particolare riferimento a quelle relative alla gestione delle attività sensibili sopra indicate;
- assicurare il regolare funzionamento dei flussi finanziari e della contabilità;
- garantire la trasparenza e la correttezza dei documenti contabili e dei relativi flussi finanziari;
- garantire un corretto e trasparente processo di gestione delle operazioni straordinarie, compresa la vendita di eventuali asset aziendali;
- assicurare la veridicità dei dati predisposti e garantire una corretta e precisa tenuta e custodia delle scritture contabili e fiscali;
- assicurare la trasparente gestione delle forniture di beni e servizi;
- rispettare la normativa fiscale-tributaria.

Gli standard di controllo di carattere generale da considerare e applicare con riferimento alle Attività Sensibili individuate sono i seguenti:
- Esistenza di Procedure / Linee Guida Formalizzate: disposizioni idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività sensibile;
- Tracciabilità: tracciabilità e verificabilità ex post delle operazioni tramite adeguati supporti documentali/informatici;
- Segregazione dei compiti: applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- Esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate: devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni.

Le fattispecie di reato ex art. 25-vicies del D. Lgs. 231/2001
Reati commessi mediante sistemi di Intelligenza Artificiale

Riferimenti normativi:
- Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi (Art. 437-bis c.p. – introdotto dal D. Lgs. n. 160 del 9 settembre 2026);
- Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale (Art. 612-quater c.p. – introdotto dalla L. n. 132/2025).

A seguito dell'introduzione del nuovo art. 25-vicies del D. Lgs. 231/2001, relativo ai reati commessi con l'utilizzo di sistemi di intelligenza artificiale, la Società individua le seguenti attività sensibili nelle quali l'impiego di sistemi AI potrebbe determinare un rischio di commissione dei reati presupposto.

Le Aree Sensibili

1. Progettazione e Ingegneria

Attività relative a:
- utilizzo di sistemi AI per progettazione di impianti, caldaie, HRSG e componenti critici;
- simulazioni di processo;
- generazione automatica di documentazione tecnica;
- elaborazione di analisi di rischio.

Rischi 231:
- alterazione o manomissione dei sistemi AI;
- utilizzo di dati tecnici non validati;
- assenza di supervisione umana su elaborazioni decisive per la sicurezza.

2. Sicurezza Industriale e Process Safety

Attività relative a:
- sistemi predittivi per manutenzione;
- monitoraggio impianti e apparecchiature;
- sistemi automatici di controllo e allarme;
- valutazioni HSE supportate da AI.

Rischi 231:
- omessa adozione di misure di sicurezza sui sistemi AI ad alto rischio;
- affidamento esclusivo alle decisioni dell'algoritmo senza verifica umana.

3. Information Technology e Cybersecurity

Attività relative a:
- sviluppo, configurazione e gestione di strumenti AI;
- utilizzo di AI generativa;
- gestione infrastrutture cloud;
- amministrazione di modelli e dataset.

Rischi 231:
- alterazione illecita dei sistemi;
- accessi non autorizzati;
- mancata tracciabilità delle attività;
- utilizzo di sistemi AI non autorizzati (shadow AI).

4. Procurement e Gestione Fornitori

Attività relative a:
- acquisto di software AI;
- selezione di fornitori tecnologici;
- utilizzo di piattaforme AI esterne.

Rischi 231:
- acquisizione di sistemi non conformi;
- mancata verifica dei requisiti di sicurezza, affidabilità e conformità normativa.

5. Risorse Umane

Attività relative a:
- screening CV;
- valutazione candidati;
- sistemi AI per performance management;
- formazione assistita da AI.

Rischi 231:
- utilizzo improprio di dati personali;
- processi decisionali automatizzati non controllati.

6. Marketing, Comunicazione e Relazioni Esterne
Attività relative a:
- generazione automatica di contenuti;
- utilizzo di immagini, audio e video generati artificialmente;
- pubblicazioni web e social media.

Rischi 231:
- diffusione di contenuti falsificati (deepfake);
- comunicazioni ingannevoli o lesive di diritti di terzi.

Principi Generali di Controllo del sistema organizzativo
Il Gruppo Sofinter ha adottato la Policy Aziendale per l'Utilizzo Responsabile dell'Intelligenza Artificiale.
ll Gruppo Sofinter riconosce il ruolo strategico dell'Intelligenza Artificiale (AI) quale leva abilitante per l'innovazione dei processi industriali, l'efficientamento operativo e il rafforzamento della competitività del Gruppo, in particolare nei contesti di progettazione, gestione degli impianti e supporto alle decisioni.
L'adozione di soluzioni di AI è guidata da un duplice principio: da un lato, valorizzare le opportunità offerte dalle tecnologie avanzate per migliorare qualità, sicurezza ed efficienza dei servizi erogati; dall'altro, garantire che il loro utilizzo avvenga nel rispetto di un approccio human-centric, affidabile e controllato, assicurando elevati standard di sicurezza, nonché dei diritti fondamentali delle persone coinvolte.
La Policy Aziendale per l'Utilizzo Responsabile dell'Intelligenza Artificiale si configura come elemento integrante del sistema di governance aziendale e si coordina con i principali framework normativi e di controllo già adottati, tra cui:
- il Modello di Organizzazione, Gestione e Controllo ex D. Lgs. 231/2001,
- il Codice Etico di Gruppo,
- il sistema di gestione della protezione dei dati personali conforme al Regolamento (UE) 2016/679 (GDPR),
- le misure di sicurezza e resilienza adottate in ambito cybersecurity in conformità alla Direttiva (UE) 2022/2555 (NIS2).

In tale contesto, il regolamento definisce un quadro organico, vincolante e in continuo aggiornamento per la gestione dell'intero ciclo di vita dei sistemi di Intelligenza Artificiale, dalla fase di valutazione e acquisizione fino all'esercizio e monitoraggio.
Il framework adottato si basa sui principi e requisiti previsti dal Regolamento (UE) 2024/1689 (AI Act), quale riferimento normativo primario per garantire lo sviluppo, l'implementazione e l'utilizzo di sistemi di AI sicuri, trasparenti e affidabili all'interno dell'Unione Europea.
L'adozione di sistemi di Intelligenza Artificiale da parte del Gruppo Sofinter non è finalizzata a ridurre o limitare le tutele previste dalla normativa lavoristica, dal contratto collettivo applicato o dagli accordi collettivi vigenti.
L'utilizzo dell'AI deve avvenire nel rispetto dei principi di dignità della persona, non discriminazione, correttezza, trasparenza e tutela dei diritti dei lavoratori.