MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

PARTE GENERALE

CAMPANA ENERGIE RINNOVABILI SRL

INTEGRATA CON LE LINEE GUIDA ANTITRUST E ANTICORRUZIONE

SOMMARIO

PREMESSA

La Società Campana Energie Rinnovabili S.r.l. (di seguito C.E.R.) ha adottato il Modello di Organizzazione, Gestione e Controllo previsto dal D.Lgs 8.6.2001 n. 231 (di seguito, anche il "Modello 231" o "il Modello").

In seguito, il Consiglio di Amministrazione ha più volte aggiornato il Modello 231, tenendo conto delle sopravvenute modifiche intervenute nell'organizzazione aziendale di C.E.R. S.r.l.; dell'evoluzione del quadro normativo e giurisprudenziale; delle considerazioni derivanti dall'applicazione del Modello, ivi comprese le esperienze provenienti dal contenzioso penale; degli esiti delle attività di vigilanza e delle risultanze delle attività di audit interno.

La Società ha, altresì, recentemente adottato il Codice Etico del Gruppo aggiornato e revisionato, nel quale sono stati confermati e formalizzati i principi cardine e i valori a cui tutte la Società, così come tutte quelle del Gruppo, deve fare riferimento nello svolgimento della propria attività.

Ai fini del presente aggiornamento del Modello 231 si è tenuto conto delle modifiche intervenute alla struttura organizzativa della società, dell'evoluzione del quadro normativo e giurisprudenziale in materia di responsabilità amministrativa da reato delle società e degli enti; delle valutazioni derivanti dall'applicazione dei Modelli 231 e delle esperienze provenienti dai procedimenti penali riferiti a contestate violazioni del D. Lgs. 8.6.2011 n. 231; delle *best practice* delle società italiane in ordine ai Modelli di Organizzazione, Gestione e Controllo, ivi comprese quelle delle altre società Gruppo Api.

INTRODUZIONE

1. Il Decreto Legislativo n. 231/2001 e successive modifiche e integrazioni

A seguito della firma da parte dell'Italia di alcune convenzioni internazionali (e, segnatamente, della Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali fatta a Parigi il 17.12.1997 e del II protocollo della Convenzione sulla protezione degli interessi finanziari della Comunità Europea adottato a Bruxelles il 19 giugno 1997) che richiedevano agli Stati aderenti di estendere la responsabilità anche alle persone giuridiche coinvolte nella commissione dei reati, l'Italia con Legge 29.9.2000 n. 300 aveva delegato il Governo (art. 11) ad emanare "*un decreto legislativo avente ad oggetto la disciplina della responsabilità amministrativa delle persone giuridiche e delle società, associazioni od enti privi di personalità giuridica*".

In attuazione della delega, il Legislatore, ha emanato il Decreto Legislativo 8.6.2001 n. 231 (di seguito "Decreto") entrato in vigore il 4 luglio 2001, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*", con il quale è stato introdotto un nuovo regime di responsabilità a carico degli enti e delle società, per una serie di reati commessi – nel loro interesse o a loro vantaggio – da soggetti organicamente o funzionalmente legati all'ente o alla società (come Amministratori, dirigenti e dipendenti) o che, pur in assenza di un rapporto di dipendenza, agiscano per conto o nell'interesse di questi (come agenti, e collaboratori in genere).

Superando (come si legge nella Relazione governativa che accompagna il Decreto) "*l'antica obiezione legata al presunto sbarramento dell'art. 27 Cost., e cioè all'impossibilità di adattare il principio di colpevolezza alla responsabilità degli enti*", il D.lgs. 231/2001 consente, quindi, di applicare direttamente a enti e società sanzioni di natura sia pecuniaria che interdittiva, in relazione alla commissione di una serie di reati (c.d. reati presupposto) da parte di soggetti qualificati, legati all'ente ai sensi dell'art. 5 del Decreto.

La responsabilità amministrativa degli enti ([1]) è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato: non si sostituisce, ma si aggiunge a quella della persona fisica ed è ravvisabile anche nel caso in cui quest'ultima non sia individuabile o non sia altrimenti punibile, per causa diversa dall'amnistia.

[1] Nel seguito si farà riferimento, per brevità, solo alla "responsabilità dell'ente". Resta, ovviamente, inteso che tale espressione sintetica deve, ovviamente, intendersi comprensiva anche delle società.

L'art. 8 del D. Lgs. 231/2001 prevede, infatti, che la responsabilità dell'ente sussiste anche quando l'autore del reato non è stato identificato o non è imputabile o il reato (commesso dalla persona fisica) si estingue per una causa diversa dall'amnistia (ad es., per prescrizione, per decesso dell'imputato).

Come emerge dalla Relazione governativa, tale disposizione "*chiarisce in modo inequivocabile come quello dell'ente sia un titolo autonomo di responsabilità, anche se presuppone comunque la commissione di un reato*".

Con la conseguenza che "*in tutte le ipotesi in cui… non sia possibile ascrivere la responsabilità penale in capo ad un determinato soggetto, e ciò nondimeno risulti accertata la commissione di un reato*" – ovvero questo si estingua per causa diversa dall'amnistia – *"l'ente ne dovrà rispondere sul piano amministrativo: beninteso, a condizione che sia ad esso imputabile una colpa organizzativa consistente nella mancata adozione ovvero nel carente funzionamento del modello preventivo*".

1.1 Natura e criteri di imputazione della responsabilità. Valore esimente dei Modelli di Organizzazione, Gestione e Controllo

Nel Decreto la responsabilità dell'ente è indicata come "responsabilità amministrativa" dipendente da reato: l'indicazione è formalmente corretta, anche se – sostanzialmente – la natura delle gravi sanzioni previste a carico dell'ente e le modalità di accertamento dell'illecito amministrativo dipendente da reato (che prevedono l'applicazione delle norme del codice di procedura penale, con indagini volte all'accertamento dell'illecito affidate al Pubblico Ministero, giudizio devoluto allo stesso Giudice penale competente per il reato presupposto ed estensione all'ente delle norme e garanzie processuali proprie dell'imputato) evidenziano che si tratta di una forma di responsabilità caratterizzata da una marcata impronta penalistica, in quanto strettamente dipendente dalla commissione di un reato

Secondo l'orientamento espresso dalla dottrina e dalla giurisprudenza di legittimità, la responsabilità dell'ente ai sensi del D.L.vo 231/2001 costituisce un *tertium genus* di responsabilità, che coniuga i tratti dell'ordinamento penale e di quello amministrativo e converge con la responsabilità penale della persona fisica, aggiungendosi ad essa e configurando un sistema di responsabilità colpevole basato sulla colpa d'organizzazione della persona giuridica (Cass., Sez. Un., 24.4.2014 n. 38843).

Affinché si configuri la responsabilità in capo all'ente ai sensi del D. Lgs 231/2001, peraltro, è necessaria non solo la realizzazione di uno dei reati presupposto espressamente previsti dal

Decreto, ma che la persona fisica che commette il reato sia funzionalmente legata all'ente medesimo e che la condotta illecita sia realizzata nell'interesse o a vantaggio dell'ente stesso.

Criteri di imputazione obiettivi

Sul piano obiettivo, la responsabilità dell'ente richiede che il fatto illecito sia stato commesso nell'interesse o a vantaggio dell'ente (art. 5, comma 1).

Come emerge dalla Relazione governativa che accompagna il Decreto, il richiamo all'interesse dell'ente caratterizza «*in senso marcatamente soggettivo la condotta (…) della persona fisica*» e si "accontenta" di una verifica *ex ante*. Il reato deve essere stato, cioè, commesso per favorire l'ente, senza peraltro che sia in alcun modo necessario l'effettivo conseguimento dell'obiettivo: si tratta, dunque, di un criterio che guarda alla finalità – anche non esclusiva – in vista della quale il fatto illecito è stato realizzato.

L'ente non è, tuttavia, responsabile se il fatto illecito sia stato commesso da uno dei soggetti indicati nell'art. 5 del Decreto "*nell'interesse esclusivo proprio o di terzi*" (art. 5, comma 2). Da tale disposizione si evince, peraltro, che se l'interesse perseguito è comune all'ente ed alla persona fisica (o riferibile in parte all'uno ed in parte all'altro) l'ente rimane comunque responsabile del reato commesso dalla persona fisica.

Inversamente, il "vantaggio" guarda al risultato che l'ente ha obiettivamente tratto dalla commissione dell'illecito e – come emerge sempre dalla Relazione governativa al Decreto – richiede sempre una verifica *ex post* e può sussistere a prescindere dall'intenzione di chi lo ha commesso, anche quando l'autore del fatto non abbia agito nell'interesse dell'ente.

L'imputazione all'ente di un reato presupposto richiede, inoltre, che il fatto illecito sia stato commesso da uno dei soggetti indicati nell'art. 5, comma 1, D.lgs. 231/2001 e cioè:

a) da persone che rivestano funzioni di rappresentanza, amministrazione, direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitino, anche in via di fatto, la gestione o il controllo dell'ente stesso (art. 5, comma 1 lett. a);

b) da persone sottoposte alla direzione o vigilanza dei soggetti sopra indicati (art, 5, comma 1 lett. b).

Criteri di imputazione soggettivi e valore esimente deli Modelli di organizzazione, gestione e controllo.

Come si legge nella Relazione governativa, nel declinare la responsabilità dell'ente il legislatore si è preoccupato – in armonia con i principi enunciati dalla CEDU – di estendere "*le imprescindibili garanzie del diritto penale anche ad altre forme di diritto sanzionatorio a contenuto punitivo, a prescindere dalle astratte etichette giuridiche*" impresse sul piano legislativo e, conseguentemente, di "*creare un sistema che, per la sua evidente affinità con il diritto penale, di cui condivide la stessa caratterizzazione afflittiva*" si dimostrasse rispettoso dei fondamentali principi a fondamento di quest'ultimo, *"primo tra tutti… la colpevolezza*".

Ai fini della responsabilità dell'ente, pertanto, non è sufficiente che il reato sia ad esso imputabile sul piano oggettivo (i.e. sia stato commesso nel suo interesse/a suo vantaggio da uno dei soggetti di cui all'art. 5), ma è necessario che – come si legge nella Relazione governativa – gli sia rimproverabile: il reato "*dovrà costituire anche espressione della politica aziendale o quanto meno derivare da una colpa di organizzazione*".

La "colpevolezza" dell'ente presuppone e richiede, quindi, che si accerti (nei modi di cui si dirà appresso) che la realizzazione del fatto illecito sia stata determinata da una politica di impresa non corretta o da deficit strutturali nell'organizzazione aziendale, che non ne abbiano prevenuto la commissione.

La responsabilità dell'ente potrà, invece, essere esclusa (alle condizioni di seguito indicate) qualora quest'ultimo – prima della commissione del reato – abbia adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. n. 231/2001, idoneo a prevenire la commissione di reati della specie di quello che è stato realizzato.

Come si evince dal dettato normativo degli artt. 6 e 7 del D. Lgs. 231/2001, peraltro, la responsabilità dell'ente (e l'efficacia esimente dei Modelli di organizzazione, gestione e controllo) assume connotati differenziati, sempre ché il reato presupposto sia stato commesso da un soggetto in posizione apicale (i.e. da uno dei soggetti indicati nell'art. 5, comma 1 lett. *a)* del D. Lgs. 231/2001) oppure da un soggetto sottoposto alla direzione o vigilanza di un soggetto apicale (art. 5, comma 1, lett. *b)* del D. Lgs 231/2001).

Nell'ipotesi in cui il reato sia stato commesso da **soggetti in posizione apicale** (art. 6 D. Lgs 231/2001), come evidenziato nella Relazione governativa, è prevista una inversione dell'ordinario onere probatorio e "*si parte dalla presunzione*" che "*il requisito «soggettivo» di responsabilità dell'ente sia soddisfatto, dal momento che il vertice esprime e rappresenta la politica dell'ente*", con la conseguenza che – in questo caso – spetterà all'ente dimostrare, per essere esentato dalla responsabilità, che:

a. l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b. il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (Organismo di vigilanza);

c. i soggetti in posizione apicale hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d. non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza di cui alla lettera b).

Qualora, invece, il reato sia stato commesso da **soggetti sottoposti alla direzione o vigilanza di un apicale** (art. 7 D. Lgs 231/2001) l'ente viene chiamato a rispondere della commissione del reato presupposto solo qualora si provi – secondo i principi ordinari (e, quindi, con onere probatorio a carico dell'accusa) – che la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.

L'inosservanza degli obblighi di direzione o vigilanza è – in ogni caso – esclusa se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi (art. 7, comma 2 D.lgs. 231/2001).

1.2 Requisiti di idoneità dei Modelli di organizzazione, gestione e controllo

All'affermazione generale dell'efficacia esimente dei Modelli di organizzazione, il legislatore ha fatto poi seguire norme interpretative, volte a precisare a quali condizioni opera tale esenzione dalla responsabilità.

Il contenuto (e i requisiti di idoneità) dei Modelli di organizzazione sono delineati nell'art. 6, commi 2 e 2-bis del D. Lgs. 231/2001, che enuclea le condizioni minime che il Modello deve soddisfare, affinché possa ritenersi idoneo a prevenire la commissione dei reati presupposto.

In particolare, ai sensi dell'art. 6, comma 2 del Decreto, il modello organizzativo deve:

a) individuare le attività nel cui ambito possono essere commessi i reati presupposto;

b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;

d) prevedere obblighi di informazione nei confronti dell'organismo, deputato a vigilare sul funzionamento e l'osservanza dei modelli (Organismo di Vigilanza);

e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Inoltre, ai sensi dell'art. 6 comma 2-bis del D. Lgs 231/2001, il Modello – ai sensi del D. Lgs. 10.3.2023 n. 24 attuativo della c.d. Direttiva Whistleblowing ([2]) – deve prevedere specifici canali di segnalazione interna per le segnalazioni *whistleblowing*, che garantiscano la riservatezza dell'identità della persona segnalante (nonché della persona coinvolta e della persona comunque menzionata nella segnalazione e del contenuto della segnalazione), il divieto di ritorsione e un sistema disciplinare, conforme a quanto previsto dal D.lgs. 24/2023 (sul punto, cfr. *infra* par. 4.7).

Ulteriori requisiti sono delineati dall'art. 7, commi 3 e 4 D. Lgs. 231/2001, che – sebbene riferito alla responsabilità dell'ente per il caso di reati commessi dai c.d. sottoposti – introduce due principi rilevanti ai fini dell'esonero della responsabilità dell'ente di carattere ed applicazione generale.

L'art. 7, comma 3 D. Lgs. 231/2001 stabilisce che il Modello di organizzazione deve prevedere, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge ed a scoprire ed eliminare tempestivamente situazioni di rischio.

A sua volta, l'art 7, comma 4 del D. Lgs. 231/2001 definisce i requisiti per l'efficace attuazione del Modello di organizzazione (e l'esenzione dalla responsabilità dell'ente), richiedendo che:

- vi sia una verifica periodica e l'eventuale modifica del Modello qualora siano scoperte rilevanti violazioni delle prescrizioni, ovvero qualora intervengano mutamenti nell'organizzazione o nell'attività;

[2] Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione europea e di disposizioni normative nazionali.

– sia previsto un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello (condizione già prevista dalla lettera *e) sub* art. 6 comma 2).

Questi principi forniscono una fondamentale chiave interpretativa, evidenziando che il Modello non deve intendersi quale strumento statico, ma deve rappresentare un apparato dinamico ed in costante evoluzione ed aggiornamento, che consenta all'ente di eliminare – attraverso una corretta e mirata implementazione del Modello nel corso del tempo – eventuali carenze che, al momento della sua adozione, non era possibile individuare e di far fronte alle modifiche intervenute nell'assetto organizzativo o nell'attività dell'ente o all'evoluzione della legislazione (e, in particolare, ad eventuali novità normative inerenti ai reati presupposto e/o all'introduzione di nuovi reati presupposto) .

Con riferimento ai reati di omicidio e lesioni colpose commessi con violazione delle norme per la tutela della salute e della sicurezza nei luoghi di lavoro, inoltre, il D. Lgs. 9.4.2008 n. 81 ha previsto (art. 30) che – per quanto attiene alla prevenzione di tali reati – il Modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa, adottato ed efficacemente attuato, deve assicurare un sistema aziendale per l'adempimento di tutti gli obblighi relativi:

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

b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;

c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

d) alle attività di sorveglianza sanitaria;

e) alle attività di informazione e formazione dei lavoratori;

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

g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Tale Modello organizzativo e gestionale deve, altresì, prevedere (art. 30, commi 2, 3 e 4 D. Lgs. 81/2008)

– idonei sistemi di registrazione dell'avvenuta effettuazione delle sopra menzionate attività;

- per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- un idoneo sistema di controllo sull'attuazione del medesimo Modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del Modello organizzativo dovranno essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

L'art. 30, comma 5 del D. Lgs. 81/2008 prevede, infine, che – in sede di prima applicazione – i Modelli si presumono conformi ai requisiti sopra indicati, qualora siano definiti conformemente alle Linee Guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007.

Si segnala che da marzo 2021, la norma British Standard OHSAS 18001 è stata sostituita dalla UNI ISO 45001:2018 "*Sistemi di gestione per la salute e sicurezza sul lavoro – Requisiti e guida per l'uso*", che definisce internazionalmente gli standard di un sistema di gestione della sicurezza e salute. La norma è stata recepita a livello nazionale dall'Ente Italiano di Normazione (UNI) ed è coerente con le normative richiamate nell'articolo 30 del D. Lgs. 81/2008 (di cui costituisce un'evoluzione).

Il Modello di Sòlergys S.p.A., per tutto quanto rappresentato in premessa ed esposto di seguito nonché nella Parte Speciale, rispetta caratteristiche e requisiti descritti in premessa.

1.3 I reati presupposto

In ragione dell'estensione del principio di legalità anche agli illeciti amministrativi dipendenti da reato (art. 2 D. Lgs. 231/2001), gli enti possono essere chiamati a rispondere solo della commissione dei reati che siano espressamente previsti nel Decreto (c.d. reati presupposto) e per i quali il Decreto preveda – al momento della loro commissione – la responsabilità dell'ente.

Il catalogo dei reati presupposto – originariamente limitato ad una serie di reati contro la Pubblica Amministrazione ([3]) – è stato in seguito notevolmente ampliato, per effetto di un'ininterrotta serie di interventi legislativi.

In particolare, già negli anni immediatamente successivi all'entrata in vigore del Decreto la responsabilità degli enti è stata estesa ad una serie di reati in materia di falsità in monete, in carte di pubblico credito e valori di bollo, ai reati societari, ai reati con finalità di terrorismo o di eversione dell'ordine democratico ([4]).

---

[3] Inizialmente, il Decreto prevedeva la responsabilità amministrativa di enti e società solo in riferimento ad alcuni reati contro la Pubblica Amministrazione e precisamente:

– indebita percezione di erogazioni pubbliche (art. 316 ter c.p.);

– truffa in danno dello Stato o di altro ente pubblico (art. 640, co 2° n. 1, c.p.);

– truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.);

– frode informatica in danno dello Stato o di altro ente pubblico (art. 640 ter c.p.);

– corruzione per un atto d'ufficio (art. 318 c.p., 321 c.p.);

– corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p., 321 c.p.);

– corruzione in atti giudiziari (art. 319 ter c.p.);

– corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.);

– istigazione alla corruzione (art. 322 c.p.);

– concussione (art. 317 c.p.);

– malversazione di erogazioni pubbliche (art. 316 bis c.p.);

– indebita percezione di contributi, finanziamenti, mutui agevolati o altre erogazioni concessi o erogati dallo Stato, da altri enti pubblici o dalla Comunità Europea (art. 316 ter c.p.).

[4] In particolare, l'art. 6 del D.L. 25.9.2011 n. 350 (convertito in Legge 23.11.2001 n. 409) ha inserito nell'ambito del D. Lgs. 231/2001 l'art. 25-bis, con il quale la responsabilità degli enti ad una serie di ipotesi criminose in materia di "falsità in monete, in carte di pubblico credito e in valori di bollo" e segnatamente ai seguenti reati:

– 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 dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);

– Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);

– Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);

– Uso di valori di bollo contraffatti o alterati (art. 464 c.p.).

In seguito, l'art. 3 del D. Lgs. 11.4.2002 n. 61, nell'ambito della riforma del diritto societario, ha introdotto nel Decreto l'art. 25-ter, estendendo il regime di responsabilità amministrativa di enti e società ai reati societari (false comunicazioni sociali - art. 2621 c.c., false comunicazioni sociali in danno dei soci o dei creditori - art. 2622 c.c., falso in prospetto - art. 2623 c.c., falsità nelle relazioni o nelle comunicazioni della società di revisione - art. 2624 c.c., impedito controllo - art. 2625 c.c., indebita restituzione dei conferimenti - art. 2626 c.c., illegale ripartizione

Successivamente, il catalogo dei reati presupposto ai quali consegue la responsabilità degli enti è stato ulteriormente allargato ai reati in materia di pornografia minorile e contro la personalità individuale ai reati di *market abuse* ed ai c.d. "reati transnazionali" ([5]).

---

degli utili e delle riserve - art. 2628 c.c., illecite operazioni sulle azioni o quote sociali o della società controllante - art. 2628 c.c., operazioni in pregiudizio dei creditori - art. 2629 c.c., formazione fittizia del capitale - art. 2632 c.c., indebita ripartizione dei beni sociali da parte dei liquidatori - art. 2633 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.).

Successivamente con la Legge 14.1.2003 n. 7, la responsabilità amministrativa da reato degli enti e delle società è stata estesa alla commissione dei delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali (art. 25-quater D. Lgs. 231/01).

[5] A seguire, con la Legge 11.08.2003 n. 228 è stato introdotto l'art. 25-quinquies d.lgs. 231/01, con il quale la responsabilità degli Enti è stata estesa alla commissione di delitti contro la personalità individuale previsti dalla sezione I del capo XII del libro II del codice penale (riduzione in schiavitù - art. 600 c.p.; prostituzione minorile - art. 600 bis c.p.; pornografia minorile - art. 600 ter c.p.; detenzione di materiale pornografico - art. 600 quater c.p.; iniziative turistiche volte allo sfruttamento della prostituzione - art. 600 quinquies c.p.; tratta e commercio di schiavi - art. 601 c.p.; alienazione e acquisto di schiavi - art. 602 c.p.).

Nel corso del 2005, con la Legge 18.04.2005 n. 62 (c.d. Legge Comunitaria 2004) e la Legge 28.12.2005 n. 262 sono stati introdotti l'art. 25-sexies ed è stato integrato e modificato l'art. 25-ter.

In particolare, la Legge 62/2005 ha introdotto nel Decreto l'art. 25-sexies, che ha esteso la responsabilità amministrativa di enti e società anche alle ipotesi di "market abuse" e segnatamente alla commissione dei reati di abuso di informazioni privilegiate (art. 184 T.U. della Finanza - D. Lgs. 24.2.1998 n. 58) e manipolazione del mercato (art. 185 T.U. della Finanza).

La Legge 62/2005 ha introdotto nel T.U. della Finanza l'art. 187-quinquies, con il quale è stata prevista una nuova forma di responsabilità dell'Ente conseguente alla commissione (nel suo interesse o vantaggio) degli illeciti amministrativi di abuso di informazioni privilegiate (art. 187-bis T.U. della Finanza) e di manipolazione del mercato (art. 187-ter T.U. della Finanza).

A sua volta, la Legge 262/2005, oltre a raddoppiare le sanzioni pecuniarie contemplate dall'art. 25 ter d.lgs. 231/2001 in materia di reati societari, ha esteso previsto la responsabilità amministrativa degli enti e delle società alla commissione del reato di omessa comunicazione del conflitto di interessi (art. 2629-bis c.c.).

In seguito, con la legge 9.1.2006 n. 7 ha introdotto l'art. 25-quater, con il quale la responsabilità amministrativa degli enti e delle società è stata estesa al delitto di cui all'art. 583-bis c.p. (pratiche di mutilazione degli organi genitali femminili).

Successivamente, con la Legge 6.2.2006 n. 38 è stato integrato l'art. 25-quinquies del Decreto, estendendo la responsabilità amministrativa per i reati di cui all'art. 600-ter c.p. e 600-quater c.p. anche alle ipotesi di cui all'art. 600-quater1 c.p. (i.e., alle ipotesi in cui il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni 18 o parti di esse).

Segnatamente, con la Legge 16.3.2006 n. 146 il legislatore – nel ratificare la Convenzione ed i Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale adottati dall'Assemblea Generale il 15.11.2000 ed il 31.5.2001 – ha previsto la responsabilità degli enti e delle società per i seguenti reati transnazionali:

– associazione a delinquere (art. 416 c.p.);

– associazione a delinquere di stampo mafioso (art. 416-bis c.p.);

– associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del D.P.R. 43/1973);

– associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 T.U. del D.P.R. 9.10.1990 n. 309);

– riciclaggio e impiego di denaro, beni e altre utilità di provenienza illecita (art. 648-bis e 648-ter c.p.);

– immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5 del T.U. di cui al d.lgs. 25.7.98 n. 286);

– intralcio alla giustizia, nella forma dell'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'A.G. e del favoreggiamento personale (artt. 377-bis c.p. e 378 c.p.).

Negli anni fra il 2007 ed il 2009, la responsabilità di enti e società è stata, altresì, estesa ai reati di omicidio e lesioni (colpose) commessi con violazione della normativa poste a tutela della salute e della sicurezza nei luoghi di lavoro, ai delitti di ricettazione, riciclaggio e reimpiego di denaro, beni od utilità di provenienza illecita, ai reati informatici, nonché ai reati di criminalità organizzata, ad alcuni delitti contro l'amministrazione della giustizia, nonché ai reati attinenti la tutela del diritto d'autore e ad una serie di reati contro l'industria e il commercio ([6]).

Si definisce "reato transnazionale" il reato punito il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato e:

a) sia commesso in più di uno Stato;

b) ovvero, sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;

c) ovvero, sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;

d) ovvero, sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

[6] In particolare, la Legge 3.8.2007 n. 123 del 2007 ha introdotto nel Decreto l'art. 25-septies, con il quale la responsabilità di enti e società è stata estesa ai reati di lesioni colpose gravi e gravissime (art. 590 c.p.) ed al reato di omicidio colposo (art. 589 c.p.) commessi in violazione delle norme per la tutela della salute e della sicurezza del lavoro.

In seguito, il D. Lgs. 21.11.2007 n. 231 ha inserito nel Decreto l'art. 25-octies, con il quale la responsabilità amministrativa di enti e società è stata estesa ai reati di ricettazione, riciclaggio ed impiego di denaro, beni o altra utilità di provenienza illecita (art. 648 c.p., 648-bis c.p. e 648-ter c.p.).

Nel corso del 2008, con la Legge 18.03.2008 n. 48 è stato poi introdotto nel Decreto l'art. 24-bis, che ha inserito nel catalogo dei reati presupposto i delitti informatici e segnatamente i reati di:

– falsità in un documento informatico pubblico o privato avente efficacia probatoria (art. 491-bis c.p.);

– accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);

– detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.);

– diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);

– intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);

– installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);

– danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);

– danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque – di pubblica utilità (art. 635-ter c.p.);

– danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);

– danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);

– frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.).

In seguito, con la Legge 15.7.2009 n. 94 ha introdotto l'art. 24 ter e con esso i delitti di criminalità organizzata:

– associazione per delinquere (art. 416 c.p.);

– associazione di tipo mafioso (art. 416-bis c.p.);

– scambio elettorale politico-mafioso (art. 416-ter c.p.);

– associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del D.P.R. 309/1990);

Negli anni successivi, fra il 2011 e il 2017, la responsabilità amministrativa da reato di enti e società è stata ancora allargata ad una serie di reati contro l'ambiente previsti dal D. Lgs. 152/2006 e, in seguito, ai nuovi delitti contro l'ambiente previsti dal codice penale (art. 452-bis e ss. c.p.) ([7]),

---

– sequestro di persona a scopo di estorsione (art. 630 c.p.);

– illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, comma 2, lettera a) numero 5) c.p.p.).

– delitti commessi avvalendosi delle condizioni previste dall'art. 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo.

Sempre nel corso del 2009, con la Legge 23.7.2009 n. 99 ha disposto l'introduzione degli artt. 25-bis.1 e 25-novies. Segnatamente, l'art. 25-novies ha introdotto i seguenti reati:

– utilizzo dei programmi di file sharing per uso personale (art. 171 lett. a bis l. 22.4.1941 n. 633);

– reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore e la reputazione (art. 171 co 3 l. 633/941);

– tutela penale del software e delle banche dati (art. 171 bis l. 633/1941);

– tutela penale delle opere audiovisive o letterarie (art. 171 ter l.633/1941);

– responsabilità relative ai supporti (art. 171 septies l. 633/1941);

– trasmissioni audiovisive ad accesso condizionato (art. 171 octies l. 633/1941).

L'art. 25 bis1 ha introdotto invece i seguenti reati:

– 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.).

La Legge 3.8.2009 n. 116 ha introdotto l'art. 25-novies (poi art. 25-decies) che ha esteso la punibilità degli enti anche in caso di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.).

La Legge n. 90/2024 ha apportato modifiche significative al Codice Penale riguardo ai reati informatici. Gli aggiornamenti includono:

– un aumento delle sanzioni pecuniarie per i reati informatici previsti dall'art. 24-bis del D.Lgs. 231/2001, con pene che ora variano da un minimo di 200 a un massimo di 700 quote.

– la sostituzione dell'art. 615-quinquies con l'art. 635-quater 1, riguardante la detenzione e diffusione abusiva di dispositivi informatici.

– l'introduzione del nuovo reato di estorsione mediante reati informatici, punito con una sanzione pecuniaria da 300 a 800 quote e sanzioni interdittive non inferiori ai due anni.

[7] Con il D. Lgs. 7.7.2011 n. 121, il legislatore ha inserito l'art. 25-undecies d.lgs. 231/2001 con il quale sono stati introdotti nel Decreto i reati in materia ambientale, e segnatamente:

– il reato previsto dall'art. 727-bis c.p., introdotto nel codice dall'art. 1 d.lgs. 121/2011 (uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette);

– il reato previsto dall'art. 733-bis c.p., introdotto nel codice dall'art. 1 d.lgs. 121/2011 (distruzione o deterioramento di habitat all'interno di un sito protetto);

nonché ai reati di immigrazione clandestina e impiego di manodopera extracomunitaria irregolare ([8]), ai reati di induzione indebita a dare o promettere utilità, di corruzione tra privati, adescamento di minorenni, istigazione alla corruzione tra privati, autoriciclaggio e caporalato ([9]).

– i reati previsti dall'art. 137 D Lgs. 152/2006 commi 2 e 3 (scarico non autorizzato di acque reflue industriali contenenti sostanze pericolose e scarico delle medesime sostanze in violazione delle prescrizioni imposte con l'autorizzazione), 5, periodo primo e secondo (scarico di acque reflue industriali in violazione dei limiti tabellari), 11 (violazione dei divieti di scarico al suolo, nelle acque sotterranee e nel sottosuolo) e 13 (scarico in mare da parte di navi e aeromobili di sostanze di cui è vietato lo sversamento);

– i reati previsti dall'art. 256 T.U.A. commi 1 lett. a e b (attività di gestione di rifiuti non autorizzata), 3, primo e secondo periodo (realizzazione o gestione di una discarica non autorizzata), 4 (inosservanza delle prescrizioni contenute nell'autorizzazione), 5 (miscelazione non consentita di rifiuti) e 6 (deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi);

– i reati previsti dall'art. 257 T.U.A. commi 1 e 2 (omessa bonifica e omissione della comunicazione agli enti competenti di un evento in grado di determinare la contaminazione del suolo, sottosuolo o acque sotterranee);

– i reati previsti dal comma 4, secondo periodo, dell'art. 258 e dai commi 6 e 7 dell'art. 260-bis d.lgs. 152/2006 (predisposizione o uso di un falso certificato di analisi dei rifiuti);

– il reato previsto dall'art. 259 T.U.A. (traffico illecito di rifiuti);

– il reato previsto dall'art. 260 T.U.A. (attività organizzata per il traffico illecito di rifiuti);

– il reato previsto dall'art. 279 comma 5 T.U.A. (inquinamento atmosferico);

– i reati previsti dall'art. 1, comma 1 e 2, e dall'art. 2, commi 1 e 2, della l. 7.2.1992 n. 150 (importazione, esportazione, trasporto e uso illecito di specie animali e commercio di piante riprodotte artificialmente);

– il reato previsto dall'art. 6, comma 4, Legge 150/1992 (illecita detenzione di esemplari vivi di mammiferi e rettili di specie selvatica o provenienti da riproduzioni in cattività che costituiscano pericolo per la salute o l'incolumità pubblica);

– il reato previsto dall'art. 3-bis Legge 150/1992 (falsificazione o alterazione di certificazioni e licenze e uso di certificazioni e licenze falsi o alterati per l'importazione di animali);

– il reato previsto dall'art. 3, comma 6 Legge 28.12.1993 n. 549 (violazione delle disposizioni sull'impiego delle sostanze lesive dell'ozono);

– i reati previsti dagli artt. 8 (inquinamento doloso) e 9 (inquinamento colposo) del d.lgs. 29.12.2007 n. 202 relativo all'inquinamento provocato dalle navi.

In seguito, la Legge 68/2015 ha modificato l'art. 25-undecies, estendendo il catalogo dei reati presupposto della responsabilità amministrativa degli enti con riferimento ai reati di: inquinamento ambientale (art. 452 bis c.p.); disastro ambientale (art. 452 quater c.p.); inquinamento ambientale e disastro ambientale colposi (art. 452 quinquies c.p.); associazione a delinquere (comune e mafiosa) con l'aggravante ambientale (art. 452 octies c.p.); traffico e abbandono di materiale ad alta radioattività (art. 452 sexies c.p.).

[8] L'art. 2 del D. Lgs. 16.07.2012 n. 109 ha introdotto l'art. 25-duodecies che prevede tra i reati presupposto l'impiego di cittadini di paesi terzi il cui soggiorno è irregolare.

In seguito, la Legge 161/2017 ha modificato l'art. 25-duodecies, estendendo la responsabilità dell'ente alle ipotesi contemplate dall'art. 12, commi 3, 3-bis, 3-ter (promozione, direzione, organizzazione, finanziamento o trasporto di stranieri nel territorio dello Stato ovvero compimento di altri atti diretti a procurarne illegalmente l'ingresso nel territorio dello Stato, ovvero di altro Stato del quale la persona non è cittadina o non ha titolo di residenza permanente, è punito con la reclusione) e comma 5 (favoreggiamento della permanenza nel territorio dello Stato dello straniero in condizione di illegalità) del D. Lgs. 286/1998.

La Legge 205/2017 ha successivamente esteso la responsabilità degli enti alla commissione dei delitti di procurato ingresso illecito e favoreggiamento dell'immigrazione clandestina di cui all'art. 12 del D.lgs. 286/1998.

Infine il D.L. n.145 dell'11.10.2024 modifica l'art. 22 D.Lgs n. 286/1998 (Lavoro subordinato a tempo determinato e indeterminato) ed introduzione dell'Art.18-ter D.Lgs n.286/1998 (Permesso di soggiorno per gli stranieri vittime di intermediazione illecita e sfruttamento del lavoro) facenti parte dell'Art. 25-duodecies del D.Lgs 231/01 (Impiego di cittadini di paesi terzi il cui soggiorno è irregolare).

Negli anni più recenti, il catalogo dei reati presupposto è stato ulteriormente esteso al delitto di traffico di influenze illecite (art. 346-bis c.p.), ai reati di frode in competizioni sportive e di esercizio abusivo di gioco e scommessa, ai reati fiscali e di contrabbando, ai reati di frode nelle pubbliche forniture, al delitto di peculato e peculato mediante profitto dell'errore altrui (art. 314 e 316 c.p.), di abuso di ufficio (art. 323 c.p.), ai delitti in materia di pagamento con metodi diversi dal contante ([10]).

---

[9] La Legge 6.11.2012 n. 190, ha esteso la responsabilità da reato degli Enti ai reati di induzione indebita a dare o promettere utilità e di corruzione tra privati.

Il D. Lgs. 4.3.2014 n. 39 ha inserito tra i reati presupposto quello di adescamento di minorenni.

Con la Legge 186/2014 è stato modificato l'art. 25-octies estendendo la responsabilità degli enti alla nuova fattispecie di autoriciclaggio di cui all'art. 648 ter.1 c.p.

L'art. 12 della Legge 69/2015 ha modificato l'art. 25-ter, inasprendo le sanzioni per i reati presupposto di false comunicazioni sociali (art. 2621 e 2621 bis c.c.) e false comunicazioni sociali delle società quotate (art. 2622 c.c.).

La Legge 199/2016 ha inserito tra i reati presupposto quello di intermediazione illecita e sfruttamento del lavoro, di cui all'art. 603 bis c.p., inserito nell'art. 25-quinques.

Il D. Lgs. n. 38/2017 ha inserito nell'art. 25-ter il delitto di istigazione alla corruzione tra privati (art. 2635 bis c.c.) ed aumentato la sanzione pecuniaria per il reato di corruzione tra privati (art. 2635 c.c.).

[10] In particolare, con la Legge 9.1.2019 n. 3 il catalogo dei reati presupposto è stato esteso alla fattispecie di cui all'art. 346 bis c.p., traffico di influenze illecite (inserito nell'art. 25 del d.lgs. 231/2001), mentre la Legge 39/2019 ha introdotto l'art. 25-quaterdecies, riferito ai reati di frode in competizioni sportive e di esercizio abusivo di gioco o di scommessa e giochi d'azzardo a mezzo di apparecchi vietati (artt. 1 e 4 della l. 401/1989).

La Legge 18.11.2019, n. 133 (Conversione in legge del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica) ha inserito i reati previsti dall'art. 1, comma 11, del Decreto legge nell'art. 24-bis del D. Lgs. 8 giugno 2001, n. 231.

La Legge 19.12.2019, n. 157 (Conversione in legge del decreto-legge 26 ottobre 2019, n. 124) ha modificato l'art. 25-quinquiesdecies, ricomprendendovi le fattispecie di cui agli artt. 2, 3, 8, 10 e 11 del D. Lgs. 74/2000. Con l'art. 5 del D. Lgs. 75/2020 – poi modificato dal D. Lgs. 156/2022 – il legislatore ha, in seguito, esteso (art. 25-quinquiesdecies, comma 1-bis) la responsabilità dell'ente anche ai delitti di cui agli artt. 4, 5 e 10-quater D.lgs. 74/2000, quando siano commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, da cui consegua o possa conseguire un danno complessivo pari o superiore a 10.000.000 di euro

Sempre con il D. Lgs. 14 luglio 2020, n. 75 il catalogo dei reati presupposto è stato, inoltre, ampliato introducendo all'art. 24, il delitto di frode nelle pubbliche forniture (art. 356 c.p.) e il delitto di cui all'articolo 2 della legge 23.12.1986, n. 898; all'art. 25, i reati di peculato (art. 314, primo comma c.p.) e peculato mediante profitto dell'errore altrui (art. 316 c.p.) e di abuso d'ufficio (art. 323 c.p.) ed all'art. 25-sexiesdecies i delitti di contrabbando.

Il D. Lgs. 8.11.2021 n. 184 ha inserito l'art. 25-octies1 relativo ai delitti in materia di pagamento con metodi diversi dal contante, prevedendo la responsabilità dell'ente in relazione ai reati di cui agli artt. 493-ter (Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti) e 493-quater (Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti) c.p. e una sanzione pecuniaria sino a 500 quote per il delitto di cui all'articolo 640-ter, nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale. È stata prevista, inoltre, la responsabilità dell'ente in relazione ad ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando abbia ad oggetto strumenti di pagamento diversi dai contanti.

Con il D. Lgs. 8.11.2021 n. 195 sono state introdotte modifiche alle fattispecie di cui all'art. 25-octies D. Lgs. 231/2001. In particolare, per i reati di ricettazione (art. 648 c.p.), di riciclaggio (art. 648 bis c.p.), di impiego di

Fra il 2022 ed il 2024, il catalogo dei reati presupposto è stato ulteriormente esteso ai reati contro il patrimonio culturale ([11]) al delitto di false o omesse dichiarazioni per il rilascio del certificato preliminare, nonché ai delitti di turbata libertà degli incanti (art. 353 c.p.) e di turbata libertà del procedimento di scelta dei contraenti (art. 353-bis c.p.) ed al reato di trasferimento fraudolento di valori (art. 512-bis c.p.) ([12]).

Nella seconda metà del 2024 sono, infine, intervenuti alcuni importanti interventi normativi in materia di reati contro la Pubblica Amministrazione, di contrabbando, nonché in materia di tutela del diritto d'autore e di delitti informatici.

Con il D.L. 4.7.2024, n. 92 (convertito, con modificazione, in Legge 8.8.2024 n. 112), con cui è stato introdotto nell'ordinamento l'art. 314-bis, che prevede il reato di "Indebita destinazione di denaro o cose mobili", aggiunto al catalogo dei reati presupposto (mediante inserimento nell'art. 25 del Decreto).

In seguito, con la Legge 114/2024 è stato abrogato il delitto di abuso d'ufficio (art. 323 c.p.) e riformulato il reato di traffico di influenze illecite (art. 346 bis).

Inoltre con il D.L. 9.8.2024 n. 113 (convertito in Legge 143/2024) il legislatore ha introdotto nella Legge 633/1941 (Protezione del diritto d'autore e di altri diritti connessi) l'art.174-sexies, che impone specifici obblighi di segnalazione, allorché si venga a conoscenza di condotte penalmente rilevanti ai sensi della legge sulla tutela del diritto d'autore o ai sensi degli artt. 615-ter c.p. o 640-

---

denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.) e autoriciclaggio (art. art. 648 ter 1 c.p.), è stato ampliato il novero dei reati presupposto alle contravvenzioni punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi e (per i soli reati di riciclaggio e autoriciclaggio) è stata estesa la punibilità ai beni provenienti da qualsiasi delitto, anche colposo.

[11] La legge 9.3.2022, n. 22 ha introdotto gli artt. 25-septiesdecies – in relazione ai delitti contro il patrimonio culturale di cui agli artt. 518-bis, 518-ter, 518-quater, 518-octies, 518-novies, 518-decies, 518-undecies, 518-duodecies, 518-quaterdecies c.p. – e 25-octiesdecies – in relazione alle fattispecie di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici di cui agli artt. 518-sexies e 518-terdecies c.p.

[12] In particolare, il D. Lgs 2.3.2023 n. 19 ha apportato modifiche all'art. 25-ter D.Lgs 231/2001 sui reati societari aggiungendo quale nuova fattispecie penale il delitto di false o omesse dichiarazioni per il rilascio del certificato preliminare previsto dalla normativa attuativa della direttiva (UE) 2019/2121, del Parlamento europeo e del Consiglio (si tratta del certificato preliminare rilasciato dal notaio per attestare il regolare adempimento degli atti e delle formalità preliminari alla realizzazione di una fusione transfrontaliera).

il D.L. 10.8.2023 n. 105 (convertito in Legge 9.10.2023 n. 137) ha modificato l'art. 24 del Decreto, inserendo fra i reati presupposto i delitti dei delitti di turbata libertà degli incanti e di turbata libertà del procedimento di scelta del contraente (art. 353 e 353-bis c.p.), nonché l'art. 25-octies1, inserendo fra i reati presupposto il delitto di trasferimento fraudolento di valori (art. 512-bis c.p.).

Con il D.L. n. 19/2024 entrato in vigore il 2.3.2024 la fattispecie di cui all'art. 512 bis, recentemente inserita tra i reati presupposto, è stata modificata con l'aggiunta di una nuova condotta: "*La stessa pena di cui al primo comma si applica a chi, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni*".

ter c.p., la cui violazione è fonte di responsabilità per l'ente ai sensi dell'art. 24-bis del Decreto ([13]).

Con il D.lgs. 26.9.2024 n. 141 il legislatore ha modificato il testo dell'art. 25-sexdecies, inserendo fra i reati presupposto – oltre ai reati di contrabbando – i delitti previsti dal D. Lgs. 504/1995 (Testo Unico in materia di accise) ([14]).

Ed ancora, con il D.L. 11.10.2024 n.145 (convertito, con modificazioni, in Legge 9.12.2024 n. 187) con il quale sono state introdotte alcune modifiche alla disciplina dettata dal D. Lgs. 286/1998, richiamato dall'art. 25-duodecies del Decreto.

---

[13] In particolare, il D.L.113/2024 impone ai prestatori di servizi di accesso alla rete, ai soggetti gestori di motori di ricerca ed ai fornitori di servizi della società dell'informazione (ivi inclusi i fornitori e gli intermediari di Virtual Private Network o comunque di soluzioni tecniche che ostacolano l'identificazione dell'indirizzo IP di origine), agli operatori di content delivery network ed ai fornitori di servizi di sicurezza internet e di DNS distribuiti, di segnalare all'Autorità giudiziaria o alla polizia giudiziaria eventuali condotte, consumate o tentate, penalmente rilevanti ai sensi della Legge 633/1941 o dei delitti di "Accesso abusivo a un sistema informatico o telematico" (615-ter c.p.) e di "Frode informatica" (art. 640-ter c.p.).

Inoltre, con la Legge 28.6.2024 n. 90 è stato introdotto nell'art. 24-bis del Decreto l'art. 635-quater1 c.p., con contestuale eliminazione dei riferimenti all'art. 615-quinquies (abrogato) e sono state incrementate le sanzioni pecuniarie e la durata delle sanzioni interdittive previste.

[14] In particolare, con il D. Lgs. 141/2024, il legislatore ha riconfermato l'inserimento nel novero dei reati presupposto previsti dall'art. 25-sexies dei reati in materia di contrabbando già previsti dal D.P.R. 23 gennaio 1973 n. 43 (e ora inseriti nell'Allegato al D. Lgs. 141/2024 recante le Disposizioni nazionali complementari al codice doganale dell'Unione):

Art. 78 (Contrabbando per omessa dichiarazione)

Art. 79 (Contrabbando per dichiarazione infedele)

Art. 80 (Contrabbando nel movimento delle merci marittimo, aereo e nei laghi di confine)

Art. 81 (Contrabbando per indebito uso di merci importate con riduzione totale o parziale dei diritti)

Art. 82 (Contrabbando nell'esportazione di merci ammesse a restituzione di diritti)

Art. 83 (Contrabbando nell'esportazione temporanea e nei regimi di uso particolare e di perfezionamento)

Art. 84 (Contrabbando di tabacchi lavorati)

e ha contestualmente esteso la responsabilità dell'ente ai reati in materia di accise previsti dal D. Lgs. 504/1995:

Art. 40 (Sottrazione all'accertamento o al pagamento dell'accisa sui prodotti energetici)

Art. 40-bis (Sottrazione all'accertamento o al pagamento dell'accisa sui tabacchi lavorati)

Art. 40-quinques, comma 3 (Vendita di tabacchi lavorati senza autorizzazione o acquisto da persone non autorizzate alla vendita)

Art. 41 (Fabbricazione clandestina di alcole e di bevande alcoliche)

Art. 42 (Associazione a scopo di fabbricazione clandestina di alcole e di bevande alcoliche)

Art. 43 (Sottrazione all'accertamento ed al pagamento dell'accisa sull'alcole e delle bevande alcoliche)

Art. 46 (Alterazione di congegni, impronte e contrassegni)

Art. 47 (Deficienze ed eccedenze nel deposito e nella circolazione dei prodotti soggetti ad accisa)

Art. 49 (Irregolarità nella circolazione)

In seguito, con il D. lgs. 12.6.2025 n. 81 il legislatore ha modificato l'art. 88 del D.lgs. n. 141/2024, riferito alle circostanze aggravanti del contrabbando.

Ulteriori modifiche sono state introdotte con il D. L. 11.4.2025 n. 48, con il quale il legislatore ha allargato il catalogo dei reati presupposto previsti dall'art. 25-*quater* D. Lgs. 231/2001, ricomprendendovi le nuove fattispecie di cui all'art. 270-*quinquies*3 c.p. (detenzione di materiale con finalità di terrorismo) e di cui all'art. 435, secondo comma c.p. (divulgazione, diffusione o pubblicizzazione di materiale contenente istruzioni sulla preparazione o sull'uso di materie o sostanze esplodenti o di tecniche o metodi finalizzati alla commissione di delitti contro la pubblica incolumità) ([15]).

Infine, con la Legge 6.6.2025 n. 82 il legislatore ha esteso il catalogo dei reati presupposto anche alle fattispecie penali contro gli animali, con introduzione nel Decreto dell'articolo 25-undevicies, che inserisce tra i reati presupposto i delitti di uccisione di animali (articolo 544-bis c.p.), maltrattamento di animali (art. 544-ter c.p.), spettacoli o manifestazioni vietati perché comportanti sevizie o strazio per gli animali (art. 544-quater c.p.), divieto di combattimento tra animali (art. 544-quinquies c.p.) e uccisione o danneggiamento di animali altrui (art. 638 c.p.).

L'elenco dettagliato dei reati attualmente previsti dal D. Lgs. 8.6.2001 n. 231 è allegato al presente Modello (Allegato n. 1).

Si riportano di seguito le "famiglie di reato" attualmente contemplate dal Decreto, rinviando all'Allegato 1 per il dettaglio delle singole fattispecie penali ivi ricomprese:

1. Indebita percezione di erogazioni, truffa in danno dello Stato o 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);
2. Delitti informatici e trattamento illecito di dati (Art. 24-bis);
3. Delitti di criminalità organizzata (Art. 24-ter);
4. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione (Art. 25);
5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis);
6. Delitti contro l'industria e il commercio (Art. 25-bis.1);

[15] In particolare, la fattispecie di cui all'art. 270-quinquies3 punisce chiunque si procura o detiene materiale contenente istruzioni sulla preparazione o sull'uso di congegni bellici micidiali; mentre il secondo comma dell'art. 435 c.p. punisce chiunque, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza materiale contenente istruzioni sulla preparazione o sull'uso delle materie o sostanze sopra indicate, o su qualunque altra tecnica o metodo per il compimento di taluno dei delitti non colposi contro l'incolumità.

7. Reati societari (Art. 25-ter);
8. Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (Art. 25-quater);
9. Pratiche di mutilazione degli organi genitali femminili (Art. 25-quater.1);
10. Delitti contro la personalità individuale (Art. 25-quinquies);
11. Reati di abuso di mercato (Art. 25-sexies);
12. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e dalla salute sul lavoro (Art. 25-septies);
13. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-octies);
14. Delitti in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies1)
15. Delitti in materia di violazione del diritto d'autore (Art. 25-novies);
16. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria (Art. 25-decies);
17. Reati ambientali (Art. 25-undecies);
18. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies);
19. Reati di razzismo e xenofobia (Art. 25-terdecies);
20. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 24-quaterdecies);
21. Reati tributari (Art. 25-quinquiesdecies);
22. Contrabbando (art. 25-sexiesdecies);
23. Delitti contro il patrimonio culturale (Art. 25-septiesdecies)
24. Riciclaggio di beni culturali e devastazione o saccheggio di beni culturali e paesaggistici (Art. 25-duodevicies)
25. Reati contro gli animali (Art. 25-undevicies)
26. Reati transnazionali (L. 146/2006).

1.4 Le sanzioni previste dal D.lgs. 231/2001

L'articolo 9, comma 1, del Decreto individua le sanzioni che possono essere comminate all'ente per gli illeciti amministrativi dipendenti da reato, ovvero:

1) la sanzione pecuniaria;

2) le sanzioni interdittive;

3) la confisca;

4) la pubblicazione della sentenza.

La determinazione della sanzione è attribuita alla discrezionalità del Giudice penale competente per il procedimento relativo ai reati dai quali dipende la responsabilità amministrativa (art. 36 D. Lgs. 231/2001).

Ove venga accertata la responsabilità dell'ente in relazione ad uno dei reati presupposto previsti dagli artt. 24 e ss. del Decreto, tuttavia, **si applica sempre la sanzione pecuniaria** (art. 10, comma 1 D. Lgs. 231/2001) e deve farsi sempre luogo – con la sentenza di condanna o di applicazione della pena – alla **confisca del prezzo o del profitto del reato** (anche per equivalente), salvo che per la parte che può essere restituita al danneggiato e salvi i diritti dei terzi di buona fede (art. 19, commi 1 e 2 D. Lgs. 231/2001).

L'ente è responsabile della commissione dei delitti richiamati negli artt. 24 ss. del Decreto, anche se realizzati nelle forme del tentativo: in tal caso, però, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà (art. 26, comma 1 D. Lgs. 231/2001). Inoltre, lo stesso, non risponde quando volontariamente impedisca il compimento dell'azione o la realizzazione dell'evento (art. 26, comma 2 D. Lgs. 231/2001).

La **"sanzione pecuniaria"** consiste nel pagamento da parte dell'ente di una somma di danaro da 10.329 Euro (art. 12, comma 4 D. Lgs. 231/2001) a 1.549.000 Euro (art. 10, commi 2 e 3 D. Lgs. 231/2001. Le sanzioni pecuniarie vengono applicate secondo un sistema "per quote" in numero non inferiore a 100 e non superiore a 1.000 (art. 10, comma 2 D. Lgs. 231/2001) e l'importo di una quota va da un minimo di 258 € a un massimo di 1.549 € (art. 10, comma 3).

Il Decreto non consente il pagamento in misura ridotta (art. 10, comma 4), così escludendo sia il ricorso all'oblazione, che l'applicazione delle disposizioni di cui all'art. 16 della Legge 689/1981.

Nella commisurazione della sanzione il Giudice determina il numero delle quote sulla base di una serie di indici individuati dall'art. 11, comma 1 del Decreto, analoghi a quelli previsti dall'art.

133 c.p. per la commisurazione della pena (gravità del fatto, grado di responsabilità dell'ente, attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti), mentre l'importo delle quote è fissato sulla base delle condizioni economiche e patrimoniali dell'ente, allo scopo di assicurare l'efficacia della sanzione (art. 11, comma 2 D. Lgs. 231/2001).

L'art. 12 elenca una serie di circostanze "attenuanti" cui consegue la riduzione della sanzione pecuniaria. In particolare, la sanzione pecuniaria è ridotta della metà e non può essere comunque superiore a 103.291 Euro qualora: *a)* l'autore del reato abbia commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne abbia ricavato un vantaggio (o ne abbia ricavato un vantaggio minimo) e *b)* il danno patrimoniale cagionato sia di particolare tenuità (art. 12, comma 1 D. Lgs. 231/2001).

La sanzione è, invece, ridotta da un terzo alla metà se l'ente, prima dell'apertura del dibattimento di primo grado, abbia: *a)* risarcito integralmente il danno ed eliminato le conseguenze dannose o pericolose del reato o, comunque, si sia efficacemente adoperato in tal senso; ovvero *b)* abbia adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quelli verificatosi (art. 12, comma 2 D. Lgs. 231/2001). Se concorrono entrambe le circostanze appena indicate, la sanzione pecuniaria è ridotta dalla metà a due terzi (art. 12, comma 3 D. Lgs. 231/2001).

L'ente risponde del pagamento delle sanzioni pecuniarie con il proprio patrimonio o il fondo comune (art. 27, comma 1 D. Lgs. 231/2001).

Le **"sanzioni interdittive"** sono individuate dall'art. 9, comma 2 del Decreto e possono essere irrogate solo in riferimento ai reati presupposto per i quali siano state espressamente previste dal Decreto ([16]) e solo qualora ricorra almeno una delle seguenti condizioni:

[16] Le sanzioni interdittive sono previste, in particolare, in caso di accertata responsabilità dell'ente in relazione alla commissione di reati contro la pubblica amministrazione, di alcuni reati contro la fede pubblica, dei delitti in materia di terrorismo e di eversione dell'ordine democratico, dei delitti contro la personalità individuale e delle pratiche di mutilazione degli organi genitali femminili, dei reati transnazionali, dei reati di omicidio e lesioni colpose commessi con violazione delle norme in materia di tutela della salute e della sicurezza nei luoghi di lavoro, dei delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, dei delitti informatici e trattamento illecito di dati, per i delitti in materia di pagamento di strumenti di pagamento diversi dai contanti, per i reati in materia di violazione del diritto d'autore, per i delitti di inquinamento e disastro ambientale (452-bis e 452-quater c.p.), per alcuni dei reati previsti dal T.U. Ambiente e dal D. Lgs. 207/2002 (inquinamento provocato dalle navi), per i reati di immigrazione clandestina e impiego di cittadini di paesi terzi il cui soggiorno è irregolare; per i delitti di razzismo e xenofobia previsti dalla Legge 654/1075, per i delitti di frode in competizione sportiva ed esercizio abusivo di gioco o scommessa, per i reati tributari, per i reati di contrabbando e in materia di accise, per i delitti contro il patrimonio culturale.

- l'ente abbia tratto dal reato un profitto di rilevante entità e il reato sia stato commesso da soggetti in posizione apicale, ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato sia stata determinata o agevolata da gravi carenze organizzative (art. 13, comma 1 lett. *a)* D. Lgs. 231/2001);
- in caso di reiterazione degli illeciti (art. 13, comma 1 lett. *b)* D. Lgs. 231/2001).

Le sanzioni interdittive previste dal Decreto sono le seguenti:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio;
- il divieto di pubblicizzare beni o servizi.

Il divieto di contrattare con la pubblica amministrazione può anche essere limitato a determinati tipi di contratto o a determinate amministrazioni, mentre l'interdizione dall'esercizio dell'attività comporta la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali allo svolgimento dell'attività stessa (art. 14, comma 2 D. Lgs. 231/2001).

Il tipo e la durata delle sanzioni interdittive sono determinate discrezionalmente dal Giudice penale, entro i limiti edittali previsti dal Decreto e con l'osservanza dei criteri indicati dall'art. 14 del Decreto.

Quanto alla **durata**, le sanzioni interdittive – salvo quanto previsto dall'art. 25, comma 5 del Decreto – hanno una durata non inferiore a 3 mesi e non superiore a 2 anni (art. 13, comma 3 D. Lgs. 231/2001).

Ordinariamente, la durata delle sanzioni interdittive è determinata dalle singole norme del Decreto che le prevedono, in riferimento ai diversi reati presupposto.

Con la Legge 9.1.2019 n. 3 la durata delle sanzioni interdittive è, peraltro, stata aumentata in riferimento alla commissione di una serie di delitti contro la pubblica amministrazione (previsti come reati presupposto dall'art. 25 del Decreto).

In particolare, l'art. 25 comma 5 del Decreto prevede che per i reati di concussione (art. 317 c.p.) corruzione per atto contrario ai doveri d'ufficio (art. 319 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), induzione indebita a dare o promettere utilità (art. 319-quater c.p.) e istigazione alla

corruzione (art. 322, secondo e quarto comma c.p.) le sanzioni interdittive abbiano una durata da 4 a 7 anni se il reato è stato commesso da uno dei soggetti di cui all'art. 5 comma 1 lett. a) (i.e. da un soggetto apicale) e da 2 a 4 anni se il reato è stato commesso da uno dei soggetti di cui all'art. 5 comma 1 lett. b) (i.e. da un sottoposto).

Queste disposizioni, tuttavia, non si applicano – e la durata delle sanzioni interdittive resta quella di cui all'art. 13, comma 2 del Decreto (da 3 mesi a 2 anni) – allorché l'ente, prima della sentenza di primo grado, si sia efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e l'individuazione del responsabile, ovvero per il sequestro delle somme (o delle altre utilità) trasferite ed abbia eliminato le carenze organizzative che hanno determinato il reato, mediante l'adozione di un Modello organizzativo idoneo a prevenire reati della stessa specie di quello verificatosi (art. 25, comma 5-bis D. Lgs. 231/2001).

Con riferimento, invece, ai **criteri di scelta** delle sanzioni interdittive, l'art. 14 del Decreto prevede che queste debbano avere ad oggetto la specifica attività alla quale si riferisce l'illecito ascritto all'ente e che il Giudice penale ne determini la tipologia e la durata avuto riguardo ai criteri di cui all'art. 11 (gravità del fatto, grado di responsabilità dell'ente, attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti) e tenendo conto della loro idoneità a prevenire illeciti del tipo di quello commesso (art. 14, comma 1 D. Lgs. 231/2001).

Il Giudice – se lo ritiene necessario – può applicare congiuntamente più sanzioni interdittive (art. 14, comma 3, D. Lgs. 231/2001).

Le sanzioni dell'interdizione dall'esercizio dell'attività, del divieto di contrattare con la pubblica amministrazione e del divieto di pubblicizzare beni o servizi possono essere applicate – nei casi più gravi e quando l'ente sia già stato condannato più volte – anche in via definitiva (art. 16, commi 1 e 2 D. Lgs. 231/2001) ([17]).

---

[17] L'art. 16, comma 1 del Decreto prevede che il Giudice possa disporre l'interdizione definitiva dall'esercizio dell'attività quando l'ente abbia tratto un profitto di rilevante entità dalla commissione dell'illecito e sia già stato condannato almeno 3 volte negli ultimi 7 anni all'interdizione temporanea dall'esercizio dell'attività.

Analogamente, l'art. 16, comma 2 del Decreto prevede che il Giudice possa applicare all'ente in via definitiva la sanzione del divieto di contrattare con la pubblica amministrazione ovvero di pubblicizzare beni o servizi, allorché quest'ultimo sia già stato condannato alla stessa sanzione 3 volte negli ultimi 7 anni.

Come si legge nella Relazione governativa, in questi casi "*la definitività della sanzione*" si giustifica in ragione del fatto che "*l'ente è rimasto sostanzialmente insensibile all'irrogazione di precedenti, identiche sanzioni interdittive, lasciando così trasparire l'impossibilità di rimanere sul mercato nel rispetto delle leggi. Pur non essendo intrinsecamente illecito, è*

Nei casi in cui – accertata la responsabilità dell'ente – si dovrebbe fare luogo all'applicazione di una sanzione interdittiva temporanea, che potrebbe determinare l'interruzione dell'attività dell'ente, il Giudice penale può – concorrendo le condizioni di cui all'art. 15 del Decreto ([18]) – consentire la prosecuzione dell'attività, nominando un Commissario giudiziale, per un periodo pari alla durata della sanzione interdittiva che dovrebbe essere inflitta (art. 15, comma 1 D. Lgs. 231/2001).

Nel caso in cui, invece, l'ente o una sua unità organizzativa venga stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di uno o più reati presupposto, il Giudice dispone l'interdizione definitiva dall'esercizio dell'attività (art. 16, comma 3 D. Lgs. 231/2001).

Ai sensi dell'art. 45 d.lgs. 231/2001, le sanzioni interdittive possono essere applicate anche in via cautelare, qualora sussistano gravi indizi per ritenere la sussistenza della responsabilità dell'ente per un illecito amministrativo dipendente da reato e vi siano fondati e specifici elementi che facciano ritenere concreto il pericolo di commissione di reati della stessa indole di quello per cui si procede.

Data la rilevante afflittività delle sanzioni interdittive, il Decreto ha peraltro previsto un meccanismo, che consente all'ente di escluderne l'applicazione, a fronte di condotte "riparatorie" successive alla commissione dell'illecito.

In particolare, ai sensi dell'art. 17 – ferma in ogni caso l'applicazione delle sanzioni pecuniarie – le sanzioni interdittive non si applicano all'ente che, prima dell'apertura del dibattimento abbia:

a) risarcito integralmente il danno ed eliminato le conseguenze dannose o pericolose del reato ovvero si sia comunque efficacemente adoperato in tal senso;

b) eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di Modelli organizzativi idonei a prevenire reati della specie di quello verificatosi;

c) messo a disposizione il profitto conseguito ai fini della confisca.

---

tuttavia un ente strutturalmente incapace di rispettare le norme e di prevenire o di contenere in maniera apprezzabile il rischio-reato".

[18] In particolare, l'art. 15 del Decreto prevede che il Giudice possa disporre la prosecuzione dell'attività – nominando un Commissario giudiziale – allorché *a)* l'ente svolga un pubblico servizio o un servizio di pubblica necessità, la cui interruzione potrebbe provocare pregiudizio alla collettività; *b)* l'interruzione dell'attività potrebbe determinare rilevanti ripercussioni sull'occupazioni e *b-bis*) l'attività dell'ente è svolta in stabilimenti (o parti di essi) dichiarati di interesse strategico nazionale.

Ai fini dell'esclusione dell'applicazione delle sanzioni interdittive, le tre condizioni di cui sopra devono sussistere tutte congiuntamente, prima che – nel giudizio per l'accertamento della responsabilità dell'ente – venga dichiarato aperto il dibattimento.

A tal fine, il Giudice penale può – su istanza dell'ente – disporre la sospensione del processo prima dell'apertura del dibattimento, affinché l'ente possa provvedere agli adempimenti richiesti dall'art. 17, qualora dimostri di essere stato nell'impossibilità di effettuarle prima (art. 65 D. Lgs. 231/2001).

Analogamente, nel corso delle indagini, il Giudice per le indagini preliminari può disporre la sospensione delle misure cautelari eventualmente applicate all'ente, se questo richiede di poter realizzare gli adempimenti di cui all'art. 17, indicando un termine per la realizzazione di tali condotte riparatorie (art. 49, comma 1).

La rilevanza di queste condotte "riparatorie" è confermata dalla circostanza che, qualora esse vengano attuate oltre i termini di cui all'art. 17 (i.e., dopo l'apertura del dibattimento di primo grado), l'ente può richiedere nel corso del giudizio – e persino dopo il passaggio in giudicato della sentenza che ne accerta la responsabilità, purché entro 20 giorni dalla notifica del relativo estratto – la conversione delle sanzioni interdittive eventualmente applicate in sanzione pecuniaria, allegando la documentazione comprovante l'avvenuta esecuzione degli adempimenti di cui al menzionato art. 17 ([19]) (art. 78, commi 1 e 2 D. Lgs. 231/2001). Disposizioni analoghe sono previste anche dall'art. 31, per il caso di fusione o scissione dell'ente, cui sia stata applicata una sanzione interdittiva (cfr. *infra*, par. 1.5).

Con il D.L. 5.1.2023 n. 2 (convertito in Legge 3.3.2023 n. 17) il legislatore ha inserito un ulteriore ipotesi di inapplicabilità delle sanzioni interdittive, prevedendo che tali sanzioni "*non possono essere applicate quando pregiudicano la continuità dell'attività svolta in stabilimenti industriali o parti di essi dichiarati di interesse strategico nazionale*", qualora l'ente abbia eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi.

A tal fine, il modello organizzativo si considera "*sempre idoneo*" a prevenire reati della specie di quello verificatosi, quando nell'ambito della procedura di riconoscimento dell'interesse strategico

[19] In tal caso, l'art. 78 del Decreto prevede che il Giudice dell'esecuzione fissi – entro 10 giorni dalla richiesta – udienza per l'esame della richiesta e possa sospendere – se la richiesta non sia manifestamente infondata – l'esecuzione della sanzione. In caso di accoglimento della richiesta, le sanzioni interdittive sono convertite in sanzione pecuniaria, in misura non inferiore a quella già applicata in sentenza e non superiore al doppio di questa (art. 78, commi 3 e 4 D. Lgs. 231/2001).

nazionale sono stati adottati provvedimenti diretti a realizzare – anche attraverso l'adozione di modelli organizzativi – il necessario bilanciamento tra le esigenze di continuità dell'attività produttiva e di salvaguardia dell'occupazione e la tutela della sicurezza sul luogo di lavoro, della salute, dell'ambiente e degli altri eventuali beni giuridici lesi dagli illeciti commessi (art. 17, comma 1-bis D. Lgs. 231/2001).

La **confisca** è una sanzione principale, prevista dal Decreto come obbligatoria, che deve essere sempre disposta dal Giudice con la sentenza di condanna o di applicazione della pena ([20]).

La confisca ha ad oggetto il prezzo o il profitto del reato (salvo che per la parte che possa essere restituita al danneggiato dal reato e salvi i diritti dei terzi di buona fede) e può essere disposta anche per equivalente (art. 19 D. Lgs. 231/2001) ([21]).

La **pubblicazione della sentenza di condanna** è una sanzione eventuale, che può essere disposta quando all'ente venga applicata una sanzione interdittiva e viene eseguita con le modalità previste dall'art. 36 del codice penale, nonché mediante affissione nel Comune ove l'ente abbia la sede principale (art. 18 D. Lgs. 231/2001).

1.5 Le vicende modificative dell'ente

Gli articoli 28 – 33 del Decreto disciplinano l'incidenza e gli effetti sulla responsabilità dell'ente delle vicende modificative connesse ad operazioni di trasformazione, fusione o scissione ed alla cessione di azienda.

Come si legge nella Relazione governativa, le disposizioni del Decreto mirano ad impedire che tali operazioni si risolvano in modalità di elusione della responsabilità e – insieme – ad "*escludere effetti eccessivamente penalizzanti, tali da porre remore anche ad interventi di riorganizzazione*" legittimi e privi di finalità elusive o, addirittura, miranti ad eliminare le carenze organizzative che abbiano consentito la commissione dell'illecito.

[20] Secondo un recente orientamento della giurisprudenza di legittimità, ai fini dell'applicazione della confisca con la sentenza di applicazione della pena è irrilevante che essa non abbia formato oggetto dell'accordo tra le parti in quanto, trattandosi di confisca obbligatoria, "*essa deve essere disposta anche nel caso in cui non sia preventivamente entrata nell'accordo delle parti, posto che, al momento della richiesta di patteggiamento, l'imputato era comunque nelle condizioni di prevederne l'applicazione*" (Cass., Sez. VI, 11.5.2022 n. 18652).

[21] La confisca del profitto del reato è prevista (oltre che nel caso di accertata responsabilità dell'ente) anche nel caso di reato presupposto realizzato da un soggetto apicale – attraverso l'elusione fraudolenta del Modello di organizzazione – e di cui l'ente non debba rispondere (art. 6, comma 5 D. Lgs. 231/2001), in quanto, come esplicitato nella Relazione governativa "*la circostanza che, nel caso di elusione fraudolenta del modello senza colpa dell'ente, non sia ravvisabile alcuna responsabilità dello stesso, nulla toglie all'inopportunità che la persona giuridica si giovi dei profitti economici che abbia comunque tratto dall'operato del c.d. amministratore infedele*".

In questa prospettiva, il Decreto prevede, anzitutto, che in caso di trasformazione (i.e. di un mero mutamento della natura o tipologia di ente o società) resta ferma la responsabilità dell'ente per i reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto (art. 28 D. Lgs. 231/2001).

A seguire, in caso di fusione, il Decreto prevede che l'ente che risulta dalla fusione (anche per incorporazione) risponde dei reati di cui erano responsabili gli enti partecipanti alla fusione (art. 29 D. Lgs. 231/2001).

L'art. 30 del Decreto regola, invece, gli effetti della scissione, prevedendo che, nel caso di scissione parziale, l'ente scisso rimane responsabile per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto (art. 30, comma 1).

Gli enti beneficiari della scissione (sia totale che parziale) sono a loro volta solidalmente obbligati al pagamento delle sanzioni pecuniarie dovute dall'ente scisso per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto, nel limite del valore del patrimonio netto trasferito al singolo ente, salvo che all'ente beneficiario della scissione sia stato trasferito – anche solo in parte – il ramo di attività nell'ambito del quale è stato commesso il reato (art. 30, comma 2).

Le sanzioni interdittive relative ai reati commessi anteriormente alla data in cui la scissione ha avuto effetto si applicano agli enti cui è rimasto (o è stato trasferito), anche solo in parte, il ramo di attività nell'ambito del quale il reato è stato commesso (art. 30, comma 3).

L'art. 31 del Decreto detta, poi, specifiche disposizioni – comuni alla fusione ed alla scissione – riferite alla determinazione della sanzione pecuniaria ed all'eventuale conversione delle sanzioni interdittive, per il caso in cui fusione o scissione siano intervenute prima della conclusione del giudizio avente ad oggetto l'accertamento della responsabilità dell'ente.

In tal caso, l'art. 31, comma 1 prevede che il Giudice penale – nel determinare la misura della sanzione pecuniaria a norma dell'art. 11, comma 2 – debba tenere conto delle condizioni economiche e patrimoniali dell'ente originariamente responsabile (e non di quelle dell'ente risultante dalla fusione o scissione).

Inoltre, nel caso di sanzioni interdittive, l'ente risultante dalla fusione o l'ente cui sarebbe applicabile la sanzione interdittiva in caso di scissione, ne possono chiedere al Giudice la conversione in sanzione pecuniaria, qualora – a seguito della fusione o della scissione – ricorrano

le condizioni di cui all'art. 17 del Decreto ([22]). In tal caso, il Giudice, se accoglie la richiesta, sostituisce la sanzione interdittiva con una sanzione pecuniaria di importo pari da 1 a 2 volte quello della sanzione pecuniaria inflitta all'ente in relazione al medesimo reato (art. 31, commi 2 e 3 D. Lgs. 231/2001).

L'art. 32 del Decreto disciplina, infine, la rilevanza della fusione o della scissione ai fini della reiterazione dell'illecito, consentendo al Giudice di tenere conto – ai fini della reiterazione di cui all'art. 20 del Decreto – delle condanne già inflitte agli enti partecipanti alla fusione o all'ente scisso, rispetto agli illeciti ascrivibili all'ente risultante dalla fusione o beneficiario della scissione.

A tal fine, il Decreto statuisce, tuttavia, che per gli enti beneficiari della scissione, la reiterazione può essere ritenuta solo se ad essi sia stato trasferito – anche solo in parte – il ramo di attività nell'ambito del quale erano stati commessi gli illeciti per cui erano state emesse le precedenti condanne (art. 32, commi 1 e 3 D. Lgs. 231/2001).

Da ultimo, il Decreto disciplina anche gli effetti della cessione o del conferimento di azienda. In particolare, il Decreto prevede che il cessionario dell'azienda nella cui attività è stato commesso il reato, sia solidalmente obbligato al pagamento della sanzione pecuniaria comminata al cedente, salvo il beneficio della preventiva escussione dell'ente cedente e nei limiti del valore dell'azienda ceduta. La responsabilità del cessionario è, inoltre, circoscritta alle sanzioni pecuniarie che risultano dai libri contabili obbligatori, ovvero dovute per illeciti amministrativi dei quali era, comunque, a conoscenza (art. 33, commi 1 e 2 D. Lgs. 231/2001). Le medesime disposizioni si applicano anche alle ipotesi di conferimento di azienda ((art. 33, comma 3 D. Lgs. 231/2001).

1.6 Reati commessi all'estero

In forza dell'art. 4 del Decreto, gli enti che abbiano in Italia la sede principale possono essere chiamati a rispondere secondo la legge italiana (beninteso, purché ricorrano le condizioni oggettive e soggettive di ascrizione della responsabilità di cui agli artt. 5, 6 e 7) anche di reati presupposto commessi all'estero, sempreché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il reato e purché sussistano le condizioni di procedibilità previste dagli artt. 7 – 10 del codice penale (i.e. le condizioni cui è subordinata l'applicabilità della legge penale italiana, per i reati commessi all'estero dal cittadino o dallo straniero).

[22] La richiesta può essere formulata dall'ente risultante dalla fusione o da quello cui sarebbe applicabile la sanzione interdittiva, in caso di scissione, anche qualora fusione o scissione siano intervenute dopo la conclusione del giudizio (art. 31, comma 4 D. Lgs. 231/2001).

Nel caso in cui anche solo una parte della condotta illecita realizzata dall'autore del reato sia avvenuta in Italia si applicherà in ogni caso la legge penale italiana (ed il D. Lgs. 231/2001), dal momento che ai sensi dell'art. 6 del codice penale "*il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione*".

Analogamente, secondo l'orientamento espresso dalla giurisprudenza di legittimità ed in forza di questi stessi principi, anche una Società che abbia sede all'estero potrà essere chiamata a rispondere di un reato, per il quale sussista (ai sensi dell'art. 6 c.p.) la giurisdizione italiana, commesso da soggetti della cui attività debba rispondere, dal momento che "*l'ente è soggetto all'obbligo di osservare la legge italiana e, in particolare, quella penale, a prescindere dalla sua nazionalità o dal luogo ove esso abbia la propria sede legale ed indipendentemente dall'esistenza o meno nel paese di appartenenza di norme che disciplino in modo analogo la medesima materia anche con riguardo alla predisposizione e all'efficace attuazione di modelli di organizzazione e gestione atti ad impedire la commissione di reati fonte di responsabilità amministrativa dell'ente stesso*" (Cass., Sez. VI, 11.2.2020 n. 11626; nello stesso senso Cass., Sez. IV, 6.9.2021 n. 32899).

1.7 Procedimento di accertamento dell'illecito (cenni)

Come accennato, la responsabilità dell'ente per gli illeciti amministrativi dipendenti da reato prevista dal Decreto deve essere accertata nell'ambito di un procedimento penale e con l'osservanza delle forme e delle garanzie previste dal codice di procedura penale.

L'art. 34 del Decreto prevede, infatti, che per il procedimento relativo all'accertamento degli illeciti amministrativi dipendenti da reato si debbano osservare le disposizioni dettate dal Decreto "*nonché, in quanto compatibili, le disposizioni del codice di procedura penale*".

Mentre l'art. 36 del Decreto prevede che la competenza a conoscere degli illeciti amministrativi dell'ente "*appartiene al giudice penale competente per i reati dai quali gli stessi dipendono*".

In proposito, il principio generale stabilito dal Decreto è quello secondo il quale ordinariamente "*il procedimento per l'illecito amministrativo dell'ente è riunito al procedimento penale instaurato nei confronti dell'autore del reato da cui l'illecito dipende* (art. 38, comma 1 D. Lgs. 231/2001)

Si procede separatamente per l'illecito amministrativo solo quando è stata ordinata la sospensione del procedimento nei confronti della persona fisica ai sensi dell'art. 71 c.p.p. (i.e., in caso di incapacità dell'imputato a partecipare al processo), quando il procedimento nei confronti dell'imputato è stato definito con rito alternativo (giudizio abbreviato/patteggiamento) o

mediante decreto penale di condanna, ovvero quando lo impongono altre disposizioni processuali (art. 38, comma 2 D. Lgs. 231/2001).

Inoltre, il procedimento prosegue autonomamente contro l'ente anche in tutti i casi in cui il reato presupposto sia estinto nei confronti della persona fisica, per causa diversa dall'amnistia (ad es., per prescrizione, morte dell'imputato o per oblazione, nei casi in cui questa è consentita).

Va tuttavia precisato che – sebbene la responsabilità dell'ente costituisca "*un titolo autonomo di responsabilità*" – il Decreto prevede che non si proceda all'accertamento dell'illecito amministrativo, quando l'azione penale non possa essere iniziata o proseguita nei confronti dell'autore del reato presupposto, per mancanza di una condizione di procedibilità (art. 37 D. Lgs. 231/2001).

Ciò in quanto l'illecito amministrativo di cui l'ente può essere chiamato a rispondere presuppone, pur sempre, la realizzazione da parte di una persona fisica di un fatto costituente reato, il cui accertamento è precluso dall'assenza (originaria o sopravvenuta) di una condizione di procedibilità.

Nel caso di trasformazione, fusione o scissione dell'ente originariamente responsabile, il procedimento prosegue nei confronti degli enti risultanti dalle vicende modificative o beneficiari della scissione, che partecipano al processo nello stato in cui si trovava l'ente originariamente responsabile (art. 42 D. Lgs. 231/2001).

Ai sensi dell'art. 35 del Decreto, all'ente si applicano le disposizioni processuali – e le garanzie – relative all'imputato, in quanto compatibili.

L'ente partecipa al procedimento con il proprio rappresentante legale, salvo che questi sia imputato del reato da cui dipende l'illecito amministrativo; quando il legale rappresentante non compare, l'ente costituito è rappresentato dal difensore (art. 39, commi 1 e 4, del D. Lgs. n. 231/2001).

Alla luce di quanto precede e tenuto conto dei principi enunciati dalla Corte di Cassazione, Sezione III Penale, nelle sentenze 13.5.2022 n. 35387 e 25.7.2023 n. 32110, nelle quali è stato affermato che il Modello organizzativo dell'ente deve prevedere regole cautelari per le possibili situazioni di conflitto di interesse del legale rappresentante, che sia indagato per il reato presupposto, idonee a munire l'ente di un difensore, nominato da soggetto munito dei necessari poteri, che assicuri la tutela degli interessi della Società, Sòlergys S.p.A. ha previsto che:

- qualora sia indagato il Presidente del Consiglio di Amministrazione o l'Amministratore delegato, entrambi titolari di poteri di rappresentanza legale della Società anche in giudizio e degli opportuni poteri per la nomina di un difensore dell'ente, la nomina potrà essere effettuata dal legale rappresentante non indagato;
- qualora siano simultaneamente indagati il Presidente del Consiglio di Amministrazione e l'Amministratore delegato (ed eventualmente altri Consiglieri di Amministrazione), i Consiglieri estranei al fatto per cui si procede, provvedono a deliberare – con la necessaria astensione dei Consiglieri indagati – il conferimento di apposito mandato ad uno di essi affinché provveda nelle forme dell'art. 39 D. Lgs. 231/2001;
- qualora siano indagati tutti i componenti del Consiglio di Amministrazione, l'Assemblea dei Soci provvederà a deliberare l'individuazione di un Procuratore della Società affinché provveda nelle forme dell'art. 39 D. Lgs. 231/2001.

1.8 Le Linee Guida di Confindustria

L'art. 6, comma 3 del Decreto ha previsto che "*i modelli di organizzazione e di gestione possono essere adottati… sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati*".

Nel 2002, Confindustria ha pubblicato la prima versione delle "*Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del Decreto legislativo 8 giugno 2001 n. 231*", che sono state approvate dal Ministero della Giustizia con D.M. 4.12.2003, che le ha giudicate idonee al raggiungimento delle finalità previste dal Decreto.

In seguito Confindustria ha più volte aggiornato le Linee Guida: l'ultimo aggiornamento è stato pubblicato da Confindustria a giugno 2021 ed approvato anch'esso dal Ministero della Giustizia.

Nella costruzione del Modello, CER S.r.l. ha adottato e fatto propri i principi espressi nelle Linee Guida di Confindustria (aggiornate a giugno 2021). Gli aspetti salienti di tali "Linee Guida" possono essere così sintetizzati:

a) identificazione dei rischi, ossia analisi del contesto aziendale per evidenziare in quale area o settore di attività e secondo quali modalità potrebbero verificarsi i reati previsti dal D. Lgs. 231/2001 e degli *standard* di controllo esistenti (i.e., identificazione e verifica del sistema di controllo esistente all'interno dell'ente e valutazione del suo grado di allineamento ai requisiti richiesti dal Decreto);

b) progettazione del sistema di controllo, ovvero di protocolli finalizzati a programmare sia la formazione che l'attuazione delle decisioni dell'ente, in relazione ai reati da prevenire. In funzione della realizzazione di tali obiettivi, le Linee Guida delineano un sistema di controllo, le cui componenti di maggior rilievo sono:

   i. adozione di un Codice Etico, con indicazione di principi etici e di chiare regole comportamentali;
   ii. un sistema organizzativo aggiornato, chiaro e formalizzato, con attribuzione di responsabilità, linee di dipendenza gerarchica, descrizione dei compiti e specifica previsione dei principi di controllo adottati;
   iii. procedure che regolamentino lo svolgimento delle attività prevedendo opportuni punti di controllo;
   iv. poteri autorizzativi e di firma, coerenti con le responsabilità organizzative e gestionali attribuite, con puntuale indicazione, ove opportuno, di limiti di spesa;
   v. un sistema di controllo integrato che, avuto riguardo ai diversi rischi operativi, sia in grado di segnalare tempestivamente eventuali criticità;
   vi. informazione e comunicazione al personale chiara e sufficientemente dettagliata e adeguato programma di formazione del personale, modulato in funzione dei livelli dei destinatari.

c) individuazione di un Organismo di controllo (Organismo di Vigilanza) della Società, dotato di autonomia e adeguata professionalità, con il compito di vigilare sull'applicazione, l'efficacia e l'adeguatezza del Modello di organizzazione, con indicazione dei suoi compiti e poteri e dei flussi informativi da e verso la società;

d) introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;

e) disciplina delle modalità di effettuazione delle segnalazioni cd. "whistleblowing";

f) sistema integrato di gestione dei rischi.

Le Linee Guida di Confindustria precisano, inoltre, che le componenti del sistema di controllo devono conformarsi ad una serie di principi quali:

− applicazione del principio di separazione delle funzioni e segregazione dei compiti;

− verificabilità, tracciabilità e congruità di ogni operazione e transazione;

− documentazione dell'attività di controllo sui processi e sulle attività a rischio di reato.

2. GOVERNANCE E ASSETTO ORGANIZZATIVO DI C.E.R. S.r.l.

La Società C.E.R. S.r.l. ha per oggetto:

- lo studio, la produzione, l'installazione e la gestione di impianti per la produzione di energia elettrica a mezzo dello sfruttamento dell'energia eolica e di altre fonti rinnovabili, in proprio e per conto di terzi;
- la produzione e la vendita dell'energia prodotta, ad Enel S.p.A., nonché alle altre aziende ed enti pubblici o privati che per legge siano interessati od autorizzati all'acquisto, distribuzione ed utilizzo di tale energia.

La Società altresì può operare anche nel più ampio settore della realizzazione di impianti alternativi per lo sfruttamento di risorse naturali ai fini di produzione elettrica che, per ragioni tecniche o commerciali, possono essere di ausilio e completamento a fini produttivi di impianti eolici realizzati e da realizzare.

A tale scopo la Società potrà promuovere e realizzare iniziative commerciali, stipulare accordi, assumere interessenze, quote e partecipazioni azionarie in altre Società, di qualsiasi tipo, aventi scopi analoghi o affini, concernenti la produzione e/o utilizzazione e distribuzione di energia elettrica su base locale, nonché la produzione ed installazione di impianti eolici impiegati per la produzione di energia da fonti alternative ed accessorie.

La società può compiere tutte le operazioni finanziarie, commerciali, industriali, mobiliari ed immobiliari che verranno reputate dagli Amministratori necessarie o utili per il conseguimento dell'oggetto sociale, compresa la prestazione di garanzie reali e personali, anche a favore di terzi; può, inoltre, ricevere finanziamenti da Soci, da società controllanti, controllate, collegate, purché nei limiti e sotto l'osservanza dell'art. 106, del Testo Unico delle leggi in materia bancaria e creditizia.

2.1. Corporate governance e sistema di controllo interno

C.E.R. S.r.l. adotta un assetto di governance di tipo tradizionale, nel quale la gestione è affidata ad un Consiglio di Amministrazione, composto da tre membri mentre le funzioni di controllo sono attribuite ad un Sindaco, per quanto attiene ai controlli di legalità ed alla verifica dell'adeguatezza dell'assetto organizzativo e del sistema amministrativo/contabile.

Avuto riguardo al sistema di amministrazione e controllo adottato da C.E.R. S.r.l., si indicano di seguito i principali organi che svolgono funzioni di direzione e controllo nel sistema organizzativo e di controllo interno, specificandone i ruoli e le interrelazioni, anche tramite il rinvio a specifici documenti.

Assemblea dei soci

Le decisioni dei soci vengono assunte in forma assembleare. Sono di competenza dell'Assemblea ordinaria ai sensi dell'art. 2364 del codice civile:

- l'approvazione del bilancio;
- la nomina e revoca degli amministratori, dei sindaci, nonché del soggetto incaricato di effettuare la revisione legale dei conti;
- la determinazione del compenso degli amministratori e dei sindaci, se non è stabilito dallo statuto;
- le deliberazioni riguardanti la responsabilità di amministratori e sindaci;
- le altre deliberazioni sugli oggetti attribuiti dalla legge alla competenza dell'assemblea, nonché sulle autorizzazioni eventualmente richieste dallo statuto per il compimento di atti degli amministratori, ferma in ogni caso la responsabilità di questi per gli atti compiuti.

Ai sensi dell'art. 2365 del codice civile sono, inoltre, di competenza dell'Assemblea straordinaria:

- le modificazioni dello Statuto;
- la nomina, sulla sostituzione e sulla determinazione dei poteri dei liquidatori;
- ogni altra materia espressamente attribuita dalla legge o dallo Statuto alla sua competenza.

Consiglio di Amministrazione

Il Consiglio di Amministrazione (di seguito, anche "C.d.A.") della Società è attualmente composto da 3 membri ed è dotato dei più ampi poteri di ordinaria e straordinaria amministrazione per la gestione della Società, nonché di tutte le facoltà necessarie per l'attuazione ed il raggiungimento degli scopi sociali, salvo che non siano per legge riservate all'Assemblea dei soci.

Gli aspetti relativi alle modalità di nomina degli amministratori, i loro requisiti di onorabilità, professionalità e indipendenza, il funzionamento (convocazioni, deliberazioni), nonché le

modalità di remunerazione sono disciplinate dallo Statuto della Società e, ove questo non disponga, dalle norme del codice civile.

La rappresentanza sociale di fronte ai terzi ed in giudizio è attribuita al Presidente del Consiglio di Amministrazione, così come il potere di firma o ai consiglieri delegati, nell'ambito dei poteri loro conferiti e agli amministratori nei limiti dei poteri previsti di amministrazione.

Con delibera adottata dal Consiglio di Amministrazione nella riunione del 28.4.2025 sono stati conferiti al Presidente del Consiglio di Amministrazione – oltre ai poteri che gli sono attribuiti dallo Statuto – poteri di rappresentanza e specifici poteri di gestione della Società, a firma singola o congiunta ([23]).

Sempre con delibera del 28.4.2025, il Consiglio di Amministrazione ha, inoltre, provveduto a conferire agli altri due amministratori poteri di firma congiunta con il Presidente del Consiglio di Amministrazione per autorizzare operazioni di valore fino a 1.000.000,00 Euro o operazioni di stipula, modifica o risoluzione di contratti di mutuo.

Il Consiglio di Amministrazione è investito di tutti i poteri per la gestione ordinaria e straordinaria della società.

In particolare ad esso sono attribuiti tutti i poteri per la realizzazione dell'oggetto sociale che non siano per legge specificamente riservati all'Assemblea dei Soci. Ai sensi dell'articolo 2381, 6° comma del codice civile, gli Amministratori sono tenuti ad agire in modo informato e ciascun Amministratore può chiedere agli Organi Delegati, se nominati, che in Consiglio siano fornite informazioni relative alla gestione della società.

---

[23] In particolare, con delibera del C.d.A. del 28.4.2025 sono stati attribuiti al Presidente del C.d.A.: poteri contratti di acquisto di servizi, di acquisto di beni mobili e immobili, di costituzione di diritti reali, di locazione, anche ultranovennale, di terreni e fabbricati:

- A firma singola del Presidente del Consiglio di Amministrazione per operazioni dal valore fino a Euro 50.000,00 per singola operazione.
- A firma congiunta del Presidente del Consiglio di Amministrazione e di uno dei due Amministratori per operazioni entro il limite massimo di Euro 1.000.000,00 per singola operazione, oltre ad operazioni aventi ad oggetto la modifica o la risoluzione di mutui e prestiti a breve, medio o lungo termine con istituti bancari, finanziari e creditizi, con l'espresso potere di consentire le relative iscrizioni ipotecarie;
- A firma congiunta con il dott. Alberto Maria Chiarini per operazioni superiore al valore di Euro 1.000.000,00 per singola operazione avente ad oggetto anche contratti per la fornitura o lo smantellamento o la realizzazione di turbine eoliche e di opere civili ed elettriche.

Inoltre il Presidente del Consiglio di Amministrazione ha il potere – a firma singola – di stipulare o sciogliere contratti con la Pubblica Amministrazione fino al valore di 50.000,00 Euro per singola operazione; aprire e chiudere conti correnti; richiedere fideiussioni o altre garanzie bancarie; girare, emettere o incassare assegni; esigere crediti a qualsiasi titolo; intervenire e concorrere in aste; svolgere e sottoscrivere operazioni con enti assicurativi, rappresentare la Società con pienezza di poteri in pratiche relative ad imposte, in procedure fallimentari o concorsuali e comunque in ogni stato e grado di giudizio di fronte ad ogni giurisdizione anche per controversie in materia di lavoro; assumere, nominare e licenziare personale dipendente.

Il Consiglio ha la facoltà di nominare dirigenti e procuratori per singoli atti o categorie di atti in applicazione delle norme vigenti, determinando l'estensione dei poteri attribuiti e fissando del caso i relativi compensi.

Il Consiglio, qualora non vi abbia provveduto l'Assemblea, può nominare un Direttore Generale ai sensi dell'articolo 2396 del codice civile fissandone il compenso.

Il Presidente del Consiglio di Amministrazione ha la rappresentanza della società, e l'uso della firma sociale in giudizio e nei rapporti con i terzi, per dare esecuzione alle delibere consiliari e delle Assemblee dei Soci, ed ha quindi la potestà di agire in nome della società in ogni procedimento giudiziale od amministrativo, a qualsiasi livello o stadio.

Il Consiglio potrà attribuire la rappresentanza per specifici atti o categorie di atti ad altri Amministratori fermo quanto previsto all'articolo 17.

Sindaco unico

In conformità a quanto previsto dallo Statuto, la Società ha provveduto a nominare un Sindaco Unico quale organo di controllo della società.

Ai sensi dell'art. 2403 del codice civile al Sindaco Unico è attribuito il compito di vigilare "*sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione e in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento*".

Al Sindaco Unico spetta, pertanto, il controllo sull'amministrazione della Società secondo quanto previsto dalle disposizioni del codice civile e la verifica – sulla base delle informazioni ricevute o di quelle acquisite nell'adempimento dei suoi compiti – dell'adeguatezza e del corretto funzionamento (avuto riguardo alle dimensioni ed alle attività svolte dalla Società) dell'assetto organizzativo e del sistema amministrativo/contabile della Società ([24]).

[24] In riferimento a quanto previsto dalla legge e dallo Statuto, il Sindaco Unico, pertanto, deve: vigilare sull'osservanza della legge e dello Statuto sociale; verificare che gli amministratori agiscano in modo informato e che, in particolare, prima di ogni riunione del consiglio, siano fornite a tutti i consiglieri adeguate informazioni sulle materie all'ordine del giorno (art. 2381, co. 1, c.c.); verificare che gli Amministratori delegati riferiscano al C.d.A. e al Collegio, con la periodicità fissata dallo Statuto, sul generale andamento della gestione e sulle operazioni di maggior rilievo; valutare l'adeguatezza dell'assetto organizzativo, amministrativo e contabile della Società; accertare che siano rispettate le previsioni di cui all'art. 2391 c.c., nell'ipotesi in cui un amministratore abbia, per conto proprio o di terzi, interesse in una determinata operazione della Società; vigilare sull'esecuzione delle delibere assembleari; acquisire informazioni dall'O.d.V. sul funzionamento del Modello ex D.lgs. n. 231/2001 e provvedere ad uno scambio informativo con l'O.d.V. in merito agli aspetti rilevanti ed alle eventuali criticità rilevate; vigilare sul corretto funzionamento del sistema amministrativo-contabile, nei termini delle procedure e dei metodi adottati (schemi adottati, deposito e pubblicazione), ovvero della completezza e chiarezza delle

Organismo di Vigilanza

La Società, nel conformare il proprio sistema di organizzazione e controllo alle disposizioni del D. Lgs. 8.6.2001 n. 231 ha provveduto ad istituire un organo collegiale (Organismo di Vigilanza), cui è attribuito il compito di vigilare sul funzionamento e l'osservanza del Modello di organizzazione gestione e controllo, garantendone nel tempo l'adeguatezza e il funzionamento, e di curarne l'aggiornamento.

Per le caratteristiche, i compiti ed il funzionamento dell'Organismo di Vigilanza si rinvia a quanto riportato *infra* (cfr. par. 4).

La Funzione di Internal Audit

Al fine di assicurare il monitoraggio delle attività operative, nonché il miglioramento dei processi di controllo e di gestione dei rischi, C.E.R. S.r.l. si avvale della funzione Internal Audit del Gruppo.

I principali obiettivi di tale funzione possono essere così riassunti:

- nel controllo del regolare svolgimento delle attività operative;
- nel controllo dell'andamento dei rischi aziendali (stima e valutazione dei principali rischi, loro gestione e monitoraggio);
- nella valutazione dell'affidabilità complessiva del sistema dei controlli interni.

Le attività della funzione Internal Audit si esplicano nel monitoraggio sulla corretta gestione dei processi aziendali e nella rimozione delle anomalie riscontrate in merito all'operatività e nel funzionamento dei presidi di controllo.

La funzione Internal Audit espleta, inoltre, verifiche e controlli anche con riguardo a specifiche richieste formulate da parte dell'Organismo di Vigilanza e/o del Sindaco unico e mantiene specifici flussi informativi con gli stessi, inviando loro il Piano annuale di audit e i rapporti di audit, per quanto di competenza.

La Funzione Internal Audit svolge, inoltre, il ruolo di segreteria dell'Organismo di Vigilanza.

---

informazioni fornite nella nota integrativa e nella relazione sulla gestione, e che i singoli processi del ciclo aziendale siano correttamente riflessi nel sistema amministrativo-contabile stesso.

Data Protection Officer - DPO

Ai sensi dell'art. 37 del Regolamento 2016/679/UE, il Consiglio di Amministrazione ha nominato un Data Protection Officer (DPO), che provvede, fra l'altro, a controllare la corretta esecuzione del Modello di Organizzazione Gestione e Controllo della privacy integrato con il Modello 231, segnalando eventuali inadeguatezze e/o malfunzionamenti nonché necessità di aggiornamento.

I compiti del DPO sono dettagliatamente specificati al paragrafo 3.5.9.

La Funzione Compliance Integrata

La Capogruppo operativa Italiana Petroli S.p.A. ha istituito una Funzione di Compliance Integrata, che rafforza i presidi organizzativi ed operativi delle Società del Gruppo, al fine di assicurare la piena osservanza della normativa applicabile, nonché la conformità dell'attività aziendale alle procedure interne.

Tra i compiti ad essa attribuiti si annoverano i controlli di secondo livello finalizzati a consentire che la Società persegua i propri obiettivi di business nel rispetto della legge, preservando il buon nome dell'ente e la fiducia dei clienti.

3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI C.E.R. S.r.l.

C.E.R. S.r.l., in linea con i valori ed i principi che regolano l'attività del Gruppo, ritiene che l'integrità e la legalità costituiscano presupposti fondamentali ed irrinunciabili dell'attività d'impresa, consapevole che l'obiettivo di creare valore economico non possa mai essere disgiunto dal rispetto delle regole.

L'adozione di un Modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 8.6.2001 n. 231 si iscrive, pertanto, nel quadro di una politica d'impresa volta a prevenire, isolare e rimuovere qualsiasi comportamento anomalo, in violazione dei valori e della cultura d'impresa del Gruppo.

3.1. Finalità del Modello

Il presente Modello di Organizzazione, gestione e controllo (di seguito, anche "il Modello" o "il Modello di Organizzazione") ha la finalità di:

a) prevenire la commissione dei reati presupposto di cui al Decreto 231/2001;

b) promuovere e valorizzare una cultura etica orientata alla legalità, integrità, correttezza e trasparenza nell'esercizio delle attività d'impresa;

c) determinare in tutti coloro che operano in nome e/o per conto di C.E.R. S.r.l. la consapevolezza di poter incorrere, nel caso di violazione delle disposizioni normative vigenti e del Modello di organizzazione, in un illecito passibile di sanzioni penali, amministrative e disciplinari e che tale violazione potrebbe comportare conseguenze dirette anche nei confronti della Società;

d) determinare in tutti coloro che operano in C.E.R. S.r.l. e/o in ogni altro soggetto che abbia rapporti con la Società la consapevolezza che tali forme di comportamento illecito sono fortemente condannate dalla Società, in quanto (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono, comunque, contrarie alle disposizioni di legge ed ai principi e valori cui C.E.R. S.r.l. ed il Gruppo ispirano la loro attività e intendono attenersi nell'espletamento della propria missione aziendale e di cui viene richiesta l'osservanza;

e) istituire un processo permanente di analisi delle attività aziendali, volto a individuare le aree nel cui ambito possano astrattamente essere commessi i reati indicati dal Decreto;

f) introdurre presidi di controllo che consentano alla Società di prevenire il rischio di commissione dei reati indicati dal Decreto nelle specifiche attività potenzialmente a rischio reato e/o di reagire tempestivamente per impedirne la commissione;

g) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto dei principi e presidi di controllo e, in particolare, delle misure indicate nel presente Modello di organizzazione;

h) istituire un Organismo di Vigilanza, con il compito di vigilare sul corretto funzionamento e l'osservanza del Modello e di curarne l'aggiornamento.

Nell'ottica della progressiva responsabilizzazione della persona giuridica e della dilatazione degli adempimenti richiesti alle Società dalle diverse normative di settore e in coerenza con le Linee Guida di Confindustria – che raccomandano alle imprese il passaggio ad un "sistema integrato" di gestione dei rischi, attraverso "*una visione integrata delle diverse esigenze di compliance*" – C.E.R. S.r.l. adotta un sistema di *compliance integrata*, dentro il quale il Modello è volto non solo alla prevenzione dei reati presupposto previsti dal D. Lgs. 8.6.2011 n. 231, ma ad assicurare la conformità ad altre normative di settore applicabili e che rivestono particolare rilevanza rispetto all'attività svolta dalla Società (come la normativa a tutela della salute e della sicurezza nei luoghi di lavoro, la normativa riguardante la protezione dei dati personali, la normativa Antitrust o quella prevista dal D. Lgs. 262/2005 a tutela del consumatore), a prescindere dalla circostanza che non siano direttamente richiamate dal Decreto.

Il presente Modello è, pertanto, integrato con le Linee Guida Anticorruzione, le Linee Guida Antitrust (comprensive anche della disciplina a tutela del consumatore) e con il Sistema di gestione della privacy.

3.2. Destinatari del Modello

Le disposizioni contenute nel presente Modello si applicano a tutti coloro che svolgono (anche di fatto ed indipendentemente dall'attribuzione di qualifiche formali) funzioni di gestione, amministrazione, direzione o controllo in C.E.R. S.r.l.., consulenti, agenti, partners commerciali e finanziari, fornitori e, in genere, a tutti coloro che (indipendentemente da vincoli di subordinazione) agiscano per conto della Società nell'ambito di attività considerate "a rischio reato".

I soggetti ai quali si rivolge il Modello (di seguito, "i destinatari del Modello") sono tenuti, pertanto, a rispettarne puntualmente le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con la Società.

3.3. Metodologia di predisposizione del Modello

Come già accennato, l'art. 6, comma 2, lett. a) del Decreto stabilisce che il Modello debba "individuare le attività nel cui ambito possono essere commessi i reati". L'identificazione dei processi societari "sensibili" alla realizzazione degli illeciti indicati nel Decreto ha rappresentato, pertanto, il punto di partenza per la definizione del Modello di C.E.R. S.r.l.

A tal fine, si è provveduto ad effettuare un'accurata ricognizione e verifica delle attività poste in essere dalla Società, delle sue strutture organizzative, dei ruoli e delle responsabilità assegnate e della relativa documentazione interna, nonché dei processi aziendali e delle attività sensibili, anche attraverso interviste con le figure apicali, per identificare le aree ed i processi a "rischio reato" e l'idoneità dei presidi di controllo esistenti a prevenirne la realizzazione.

Ad esito di questa ricognizione ed analisi dei processi aziendali è stata elaborata una "mappatura delle aree a rischio", che identifica le aree astrattamente esposte al rischio di commissione di (almeno uno dei) reati presupposto (che viene allegato al presente Modello, **Allegato 2 – Mappatura Aree a Rischio**).

Tra i reati presupposto rientranti nell'ambito di applicazione del D. Lgs. 231/2001 sono state individuate 10 "famiglie di reato", che ricomprendono fattispecie astrattamente suscettibili di essere realizzate nell'ambito dell'attività aziendale ([25]):

---

[25] Rispetto all'elenco delle famiglie di reato previste dal Decreto e indicate alle pagine 22 - 23 non sono state considerate applicabili alla società quelle di cui al n. 6 (*Delitti contro l'industria e il commercio* – Art. 25-bis.1); al n. 5 *Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento* (Art. 25-bis)n. 9 (*Pratiche di mutilazione degli organi genitali femminili* – Art. 25-quater.1); al n. 10 (*Delitti contro la personalità individuale* – Art. 25-quinquies); al n. 11. *Reati di abuso di mercato* (Art. 25-sexies)al n. 19 (*Reati di razzismo e xenofobia* – Art. 25-terdecies); al n. 20 (*Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati* – Art. 24-quaterdecies); al n. 22 (*Contrabbando* – art. 25-sexiesdecies); al n. 23 (*Delitti contro il patrimonio culturale* – Art. 25-septiesdecies); al n. 24 (*Riciclaggio di beni culturali e devastazione o saccheggio di beni culturali e paesaggistici* – Art. 25-duodevicies) ed al n. 25 (*Reati contro gli animali – Art.* 25-undevicies);

Sono state, inoltre accorpate all'interno dei "Reati con finalità di terrorismo ed eversione dell'ordine democratico e di criminalità organizzata" (n. 10) le "famiglie di reati" di cui ai numeri 3 (*Delitti di criminalità organizzata* – Art. 24-ter) e 8 (*Delitti con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali* – Art. 25-quater) 6 (*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria* – Art. 25-decies) e il n. 25 (*Reati transnazionali L. 146/2006*)dell'elenco riportato alle pagine 18 e 19.

1) Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture;
2) Reati contro la Pubblica Amministrazione;
3) Reati societari;
4) Reati informatici e di trattamento illecito di dati;
5) Reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio;
6) Reati con finalità di terrorismo ed eversione dell'ordine democratico e di criminalità organizzata;
7) Reati di omicidio e lesioni colpose commessi con violazione della normativa a tutela della salute e sicurezza nei luoghi di lavoro;
8) Reati ambientali;
9) Reati tributari;
10) Delitti in materia di strumenti di pagamento diversi dal contante.

3.4. Struttura del Modello

In conformità alle *best practices* adottate nell'elaborazione dei modelli ed a quanto raccomandato dalle Linee Guida di Confindustria, il presente Modello di organizzazione, gestione e controllo è articolato:
(i) in una Parte Generale, che descrive il quadro normativo di riferimento, il processo di definizione del Modello ed i principi generali di funzionamento complessivo del sistema di organizzazione, gestione e controllo adottato volto a prevenire la commissione dei reati presupposto;

(ii) ed in una serie di Parti Speciali, volte ad integrare il contenuto della Parte Generale con la descrizione delle fattispecie di reato e dei processi/attività sensibili che la Società ha individuato come rilevanti in relazione alle fattispecie di reato previste dal Decreto e delle correlate misure di prevenzione e riduzione del rischio, tra cui standard di controllo.

Sono parte integrante del Modello anche la Mappatura delle Aree a Rischio ed il Codice Etico del Gruppo, adottato dalla Società (e recentemente aggiornato), nel quale sono espressi i valori e la cultura d'impresa del Gruppo (cfr. *infra*, par. 3.5.15).

3.5. Elementi e principi generali del Modello

Il Modello si fonda su un insieme integrato di elementi e principi generali, che sono a fondamento del complessivo funzionamento del sistema di organizzazione, gestione e controllo volto a prevenire la commissione di reati presupposto e, più in generale, ad assicurare la legalità dell'attività di impresa, qui di seguito indicati:

1. Adozione e aggiornamento del Modello ed aggiornamento della mappatura delle aree a rischio e delle funzioni coinvolte;
2. Sistema organizzativo e autorizzativo;
3. Principi generali di controllo relativi alle attività a rischio;
4. Sistema di gestione delle risorse finanziarie;
5. Prestazioni di servizi da o verso altre società;
6. Rapporti infragruppo;
7. Linee guida anticorruzione;
8. Linee guida antitrust;
9. Sistema di gestione della privacy;
10. Sistema di flussi informativi da e verso il Data Protection Officer (DPO);
11. Organismo di Vigilanza e sistema di flussi informativi da e verso l'O.d.V. (rinvio);
12. Comunicazione del Modello;
13. Informativa ai Collaboratori esterni ed ai partners;
14. Codice Etico e protocollo per il suo aggiornamento;
15. Sistema disciplinare e sanzionatorio (rinvio).

3.5.1. Adozione e aggiornamento del Modello ed aggiornamento della mappatura delle aree a rischio e dei controlli

L'approvazione del Modello costituisce prerogativa e responsabilità esclusiva del Consiglio di Amministrazione di C.E.R. S.r.l.

Analogamente, anche l'aggiornamento del Modello è responsabilità esclusiva del Consiglio di Amministrazione, anche su segnalazione dell'Organismo di Vigilanza.

In particolare, il Modello dovrà essere integrato ed aggiornato ogniqualvolta siano scoperte significative violazioni delle sue prescrizioni, ovvero quando intervengano rilevanti mutamenti nell'organizzazione o nell'attività della Società o, ancora, quando sopravvengano novità normative per effetto delle quali vengano identificate nuove attività a rischio reato, ovvero aree sensibili non adeguatamente coperte dai presidi di controllo esistenti.

L'individuazione degli ambiti in cui può sussistere il rischio di commissione dei reati e la "mappatura delle aree a rischio" costituisce, infatti, un presupposto fondamentale non solo per l'elaborazione, ma anche per il funzionamento del Modello. Di conseguenza, la "mappatura delle aree a rischio" deve essere aggiornata, al verificarsi di evoluzioni o modifiche dell'attività o dell'organizzazione aziendale o dell'introduzione di nuove fattispecie penalmente rilevanti.

È attribuito all'Organismo di Vigilanza il compito e la responsabilità di monitorare le circostanze che potrebbero determinare la necessità di una revisione e/o di un aggiornamento della mappatura delle aree a rischio reato o del Modello, valutandone la rilevanza, nonché di segnalarle al C.d.A. nella Relazione semestrale – o quando ne ravvisi comunque l'opportunità – per l'adozione da parte dell'Organo amministrativo delle opportune determinazioni.

3.5.2. Il Sistema organizzativo e autorizzativo

Il Sistema organizzativo

Come chiarito dalla Linee Guida di Confindustria, il Sistema organizzativo deve essere adeguatamente formalizzato e chiaro, soprattutto in riferimento all'attribuzione di poteri e responsabilità, alle linee di dipendenza gerarchica ed alla descrizione dei compiti.

Allo stato, la Società non ha dipendenti, né personale proprio e le attività operative vengono svolte avvalendosi di un contratto di *service* sottoscritto con la Capogruppo operativa Italiana Petroli S.p.A. e di servizi offerti da ditte terze contrattualizzate.

Il Sistema autorizzativo

Il sistema autorizzativo è adeguatamente formalizzato, attraverso la divisione ed il conferimento di specifici poteri agli esponenti aziendali che operano per conto della Società. Alla distribuzione dei poteri autorizzativi è data adeguata pubblicità, mediante la pubblicazione nel Registro delle imprese.

In conformità alle Linee Guida di Confindustria, la Società provvede:

- ad aggiornare l'articolazione dei poteri a seguito di modifiche e/o integrazioni intervenute nella struttura organizzativa;
- ad istituire ed alimentare un flusso informativo, al fine di garantire la tempestiva comunicazione dei poteri e dei relativi cambiamenti;
- e ad effettuare verifiche periodiche sul rispetto dei poteri di firma.

3.5.3. Principi generali di controllo relativi alle aree a rischio

Ad integrazione dei principi e presidi di controllo previsti nell'ambito di ciascuna sezione della Parte Speciale del Modello, in riferimento ai processi aziendali identificati come "a rischio reato" ed ai reati presupposto astrattamente suscettibili di realizzazione, C.E.R. S.r.l. ha previsto una serie di principi di controllo e di regole generali di comportamento, trasversali a tutti i processi aziendali, cui deve uniformarsi la condotta degli esponenti aziendali.

In particolare, i principi di controllo e le regole di comportamento di cui dovrà essere garantita l'osservanza in tutte le attività "a rischio reato" sono i seguenti:

- garantire integrità ed etica nello svolgimento dell'attività, tramite la previsione di opportune regole di comportamento volte a disciplinare ogni specifica attività a rischio;
- definire compiti e responsabilità di ciascun esponente aziendale coinvolto nelle attività a rischio;
- attribuire poteri decisionali in modo commisurato al grado di responsabilità e autorità conferito;
- definire, assegnare e comunicare i poteri autorizzativi e di firma, prevedendo, quando richiesto, l'indicazione delle soglie di approvazione delle spese, in modo che a nessun soggetto siano attribuiti poteri discrezionali illimitati;

- garantire la separazione dei ruoli nella gestione dei processi, provvedendo ad assegnare a soggetti diversi le varie fasi di cui si compone il processo e, in particolare, quella dell'autorizzazione, dell'esecuzione e del controllo;
- assicurare la verificabilità, la documentabilità, la coerenza e la congruità di ogni operazione o transazione. A tal fine, dovrà essere garantita la tracciabilità dell'attività attraverso un adeguato supporto documentale, su cui si possa procedere in ogni momento all'effettuazione di controlli. La tracciabilità delle operazioni potrà essere assicurata anche dall'utilizzo di sistemi informatici, che consentano il rispetto dei requisiti sopra descritti;
- assicurare la documentabilità dei controlli effettuati al fine di garantire la possibilità di ripercorrere l'attività di controllo e valutare la metodologia adottata e la correttezza dei risultati emersi;
- garantire l'affidabilità del reporting al vertice aziendale;

Nella Parte Speciale sono individuate, in relazione a ciascuna area a rischio reato, le modalità con le quali i principi di controllo sopra descritti vengono declinati ed attuati.

3.5.4. Sistema di gestione delle risorse finanziarie

L'art. 6, comma 2, lett. c) del Decreto richiede che i Modelli prevedano "*modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati*".

Le Linee Guida di Confindustria raccomandano, a tal fine, l'adozione di meccanismi di procedimentalizzazione delle decisioni che, rendendo documentate e verificabili le varie fasi del processo decisionale, impediscano la gestione impropria delle risorse finanziarie dell'ente.

Al fine di assicurare la corretta gestione delle risorse finanziarie C.E.R. S.r.l. ha provveduto a regolamentare i principali processi amministrativo-contabili nell'ambito dei protocolli previsti dal presente Modello ed è, altresì, previsto che le fasi del processo decisionale – che conduce all'impiego di risorse finanziarie – siano documentate, così da renderle verificabili e tracciabili.

3.5.5. Prestazione di servizi da o verso altre società

Le prestazioni di servizi svolte dalla Capogruppo operativa Italiana Petroli S.p.A. e/o da altre società appartenenti al Gruppo a beneficio della Società vengono disciplinate da un contratto scritto. Il contratto di servizi prevede:

- ruoli, responsabilità e tempistiche, riguardanti la gestione delle attività che formano oggetto della prestazione di servizi;
- l'obbligo da parte della società che presta il servizio in favore di C.E.R. S.r.l. di attestare la veridicità e completezza della documentazione prodotta e/o delle informazioni comunicate alla Società ai fini dello svolgimento dei servizi richiesti;
- l'obbligo da parte della società che presta il servizio in favore di C.E.R. S.r.l. di rispettare, nello svolgimento del servizio richiesto, il Codice etico del gruppo, nonché l'impegno al rispetto dei principi del Modello volti a prevenire la commissione degli illeciti di cui al D. Lgs. 231/2001.

Analogamente, qualora C.E.R. S.r.l. presti servizi in favore di società appartenenti al Gruppo, la prestazione viene disciplinata da un contratto scritto, che prevede:

- l'obbligo da parte di C.E.R. S.r.l. di attestare la veridicità e la completezza della documentazione prodotta e/o delle informazioni comunicate alla società beneficiaria del servizio;
- l'obbligo da parte di C.E.R S.r.l. di rispettare nello svolgimento del servizio prestato il Codice etico e il presente Modello. Qualora i servizi erogati rientrino nell'ambito di attività sensibili non contemplate dal presente Modello, la Società dovrà dotarsi di regole e procedure idonee a prevenire la commissione dei reati previsti dal Decreto.

3.5.6. Rapporti infragruppo

Italiana Petroli S.p.A., in qualità di socio unico di C.E.R. S.r.l. e di Capogruppo operativa, esercita attività di direzione e coordinamento (ai sensi degli artt. 2497 e seguenti del c.c.) nei confronti della Società (e delle altre società del Gruppo), al fine di garantire il coordinamento dell'attività della Società nell'interesse complessivo del Gruppo e per una valorizzazione delle possibili sinergie tra le varie società.

Nell'ambito dell'attività di direzione e coordinamento, Italiana Petroli S.p.A. eroga alle Società del Gruppo una serie di servizi, sulla base di apposito contratto di servizio in forma scritta, che prevede ruoli e responsabilità riguardanti la gestione delle attività *in service*, nonché le caratteristiche essenziali dei servizi ed i criteri.

Le attività svolte in forza del contratto di servizio sono oggetto di monitoraggio da parte dell'Organismo di Vigilanza della Società.

3.5.7. Linee Guida Anticorruzione

C.E.R. S.r.l. svolge la propria attività in conformità ai principi e valori espressi nel Codice Etico ed a quanto previsto dal Modello, secondo criteri di trasparenza, integrità, correttezza e lealtà nei rapporti con le Autorità pubbliche e nel rispetto delle normative vigenti, contrastando ogni forma di corruzione, pubblica o privata.

C.E.R. S.r.l. richiede, pertanto, a tutti i propri stakeholder di operare in conformità ad ogni normativa applicabile per prevenire e contrastare ogni fenomeno di corruzione ed è impegnata a rispettare i principi e le regole di comportamento di seguito indicate

A – Regole di comportamento nei rapporti con la Pubblica Amministrazione

- È vietato a tutti gli esponenti aziendali offrire, promettere e corrispondere, direttamente o indirettamente, denaro o qualsiasi altra utilità, di qualsivoglia natura, a pubblici ufficiali o incaricati di pubblico servizio, al fine di influenzare o remunerare un atto del loro ufficio e/o di indurli a omettere o ritardare un atto del loro ufficio, ovvero a compiere un atto contrario ai loro doveri d'ufficio e/o a remunerare il compimento di un atto contrario ai loro doveri d'ufficio;
- È vietato a tutti gli esponenti aziendali influenzare, anche per interposta persona, il pubblico ufficiale o l'incaricato di un pubblico servizio nello svolgimento delle sue funzioni o per indurlo a compiere, omettere o ritardare un atto d'ufficio o contrario ai suoi doveri d'ufficio;
- È vietato a tutti gli esponenti aziendali effettuare o offrire somme di denaro (o qualsiasi altra utilità) a persone, società o qualunque altra entità, che vantino relazioni asserite o esistenti con pubblici ufficiali o incaricati di pubblico servizio, per conseguire benefici di qualsivoglia natura nei rapporti della Società con la pubblica amministrazione;
- È vietato a tutti gli esponenti aziendali effettuare o promettere, anche per interposta persona, erogazioni a beneficio di partiti politici, movimenti e organizzazioni politiche e sindacali o a loro rappresentanti e candidati;
- È vietato a tutti gli esponenti aziendali offrire regali o altre liberalità a funzionari o dipendenti della Pubblica Amministrazione. Sono consentiti esclusivamente, nel rispetto delle procedure interne e salvo che siano finalizzati ad influenzare l'operato del funzionario pubblico, omaggi di modico valore e comunque tali da non compromettere l'integrità, l'imparzialità e la reputazione delle parti e da non poter essere interpretati come finalizzati ad acquisire vantaggi in modo improprio;

Le disposizioni ed i divieti appena indicati si applicano anche nei confronti delle persone indicate nell'art. 322-bis del codice penale ([26]).

È fatto obbligo a tutti gli esponenti aziendali di segnalare ogni possibile violazione della normativa anticorruzione secondo le modalità previste al paragrafo 4, nonché di partecipare alla formazione in materia anticorruzione nel rispetto dei programmi e dei contenuti predisposti dalle competenti Funzioni aziendali.

B – Regole di comportamento nei rapporti con i privati

- È vietato a tutti gli esponenti aziendali sollecitare e/o ricevere denaro (o qualsiasi altra utilità di qualsivoglia natura) per compiere o per omettere un atto in violazione degli obblighi del loro ufficio/funzione o degli obblighi di fedeltà;
- È vietato a tutti gli esponenti aziendali offrire o promettere denaro (o qualsiasi altra utilità di qualsivoglia natura) – anche per interposta persona – ad amministratori, direttori generali, dirigenti, dipendenti, sindaci o liquidatori di società o enti privati, affinché compiano od omettano un atto in violazione degli obblighi del loro ufficio e/o della loro funzione o degli obblighi di fedeltà su di essi incombenti;
- È vietato a tutti gli esponenti aziendali praticare favoritismi o porre in essere comportamenti collusivi, anche attraverso promesse di vantaggi personali di qualsiasi natura

[26] E cioè, nei confronti a) dei membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee; b) dei funzionari e degli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee; c) delle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee; d) dei membri e degli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee; e) di coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio; f) dei giudici, del procuratore, dei procuratori aggiunti, dei funzionari e degli agenti della Corte penale internazionale, delle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, dei membri e degli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale; g) delle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di pubblico servizio nell'ambito di organizzazioni pubbliche internazionali; h) dei membri delle assemblee parlamentari internazionali o di un'organizzazione internazionale o sovranazionale e dei giudici e funzionari delle corti internazionali; i) delle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di pubblico servizio nell'ambito di Stati non appartenenti all'Unione europea, quando il fatto offende gli interessi finanziari dell'Unione; l) delle persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali.

- È fatto obbligo a tutti gli esponenti aziendali di segnalare, anche in forma anonima, ogni possibile violazione della normativa anticorruzione secondo le modalità previste al paragrafo 4.

C.E.R. S.r.l. adotterà i provvedimenti disciplinari, secondo le previsioni del presente Modello, in caso di violazione delle indicate regole di comportamento.

Nessun esponente aziendale potrà essere oggetto di sanzioni disciplinari o subire conseguenze personali per essersi rifiutato di compiere atti in violazione delle presenti Linee Guida, anche qualora tale rifiuto abbia determinato conseguenze pregiudizievoli per il *business* aziendale.

Tutti gli esponenti aziendali devono, inoltre, evitare – e comunque segnalare – ogni situazione che possa costituire o determinare un conflitto di interesse tra le attività economiche personali e/o familiari e le mansioni che ricoprono all'interno della Azienda.

I contratti con i Partner, Fornitori, Consulenti e Collaboratori esterni devono prevedere l'inserimento e l'accettazione di clausole contrattuali specifiche che li impegnino all'osservanza della normativa anticorruzione e, in generale, di ogni altra normativa al cui rispetto è improntata l'attività di C.E.R. S.r.l.

3.5.8. Linee Guida Antitrust

In conformità ai principi e valori espressi nel Codice Etico ed a quanto previsto dal Modello, C.E.R. S.r.l. svolge la propria attività nel rispetto delle regole poste a tutela della concorrenza e del mercato e dei consumatori.

La legge 10 ottobre 1990 n. 287, recante norme per la tutela della concorrenza e del mercato, vieta alle imprese:

- le intese restrittive della concorrenza, ossia quelle che abbiano per oggetto o per effetto di impedire, restringere o falsare in maniera consistente la concorrenza all'interno del mercato nazionale o in una sua parte rilevante (art. 2 Legge 287/1990).

Sono considerati intese gli accordi e/o le pratiche concordati tra imprese nonché le deliberazioni, anche se adottate ai sensi di disposizioni statutarie o regolamentari, di consorzi, associazioni di imprese ed altri organismi similari (art. 2, comma 1 Legge 287/1990)

In particolare, costituiscono intese restrittive della concorrenza gli accordi fra più imprese volti (i) a concertare, direttamente o indirettamente, le condizioni economiche di vendita o di acquisto dei prodotti o le condizioni contrattuali (ii) a impedire o limitare la produzione, gli sbocchi o gli

accessi al mercato, gli investimenti, lo sviluppo tecnico o il progresso tecnologico; (iii) a ripartire mercati o fonti di approvvigionamento (iv) ad applicare, nei rapporti commerciali con altri contraenti, condizioni oggettivamente diverse per prestazioni equivalenti, così da determinare per essi ingiustificati svantaggi nella concorrenza; (v) a subordinare la conclusione di contratti all'accettazione, da parte degli altri contraenti, di prestazioni supplementari che, per loro natura o secondo gli usi commerciali, non abbiano alcun rapporto con l'oggetto dei contratti stessi.

Detti accordi sono da considerarsi nulli ad ogni effetto. Se le intese sono idonee a pregiudicare il commercio tra gli Stati membri, l'Autorità antitrust applicherà la normativa comunitaria (articolo 101 del Trattato sul funzionamento dell'Unione Europea).

- l'abuso di posizione dominante, intendendosi per posizione dominante quella dell'impresa che può comportarsi in modo significativamente indipendente dai concorrenti, dai fornitori e dai consumatori (art. 3 Legge 287/1990).

La posizione dominante deve essere valutata nel tempo e sulla base della posizione occupata dall'impresa nell'ambito del mercato di riferimento in cui opera. La circostanza che un'impresa raggiunga grandi dimensioni o detenga quote significative di mercato non distorce, di per sé, il mercato, così come la capacità dell'impresa di imporre determinate condizioni in uno specifico rapporto contrattuale non determina, di per sé, una posizione dominante. La legge non vieta, insomma, che un'impresa raggiunga una "posizione dominante" in uno specifico mercato, ma ne vieta l'abuso, che si concretizza quando l'impresa sfrutta il proprio potere a danno dei consumatori ovvero impedisce ai concorrenti di operare sul mercato, causando, conseguentemente, un danno ai consumatori.

L'art. 3 della Legge 287/1990 vieta, pertanto, alle imprese a) di imporre direttamente o indirettamente prezzi di acquisto, di vendita o altre condizioni contrattuali ingiustificatamente gravose; b) di impedire o limitare la produzione, gli sbocchi o gli accessi al mercato, lo sviluppo tecnico o il progresso tecnologico, a danno dei consumatori; c) di applicare nei rapporti commerciali con altri contraenti condizioni oggettivamente diverse per prestazioni equivalenti, così da determinare per essi ingiustificati svantaggi nella concorrenza; d) e di subordinare la conclusione dei contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari che, per loro natura e secondo gli usi commerciali, non abbiano alcuna connessione con l'oggetto dei contratti.

Quando l'abuso determina un pregiudizio per il commercio tra più Stati membri dell'UE, l'Autorità applica la normativa comunitaria (articolo 102 del Trattato sul funzionamento dell'Unione Europea).

- le operazioni di concentrazione – così come definite dall'art. 5 della Legge 287/1990 - restrittive della libertà di concorrenza, ossia le operazioni che abbiano l'effetto di ostacolare in modo significativo la concorrenza effettiva nel mercato nazionale o in una sua parte rilevante, in particolare a causa della costituzione o del rafforzamento di una posizione dominante (art. 6 Legge 287/1990).

Tale situazione deve essere valutata in ragione della necessità di preservare e sviluppare la concorrenza effettiva, tenendo conto della struttura di tutti i mercati interessati e della concorrenza (attuale o potenziale), nonché della posizione sul mercato delle imprese partecipanti, del loro potere economico e finanziario, delle possibilità di scelta dei fornitori e degli utilizzatori, del loro accesso alle fonti di approvvigionamento o agli sbocchi di mercato, dell'esistenza di diritto o di fatto di ostacoli all'entrata, dell'andamento dell'offerta e della domanda dei prodotti e dei servizi in questione, degli interessi dei consumatori intermedi e finali, nonché del progresso tecnico ed economico, purché esso sia a vantaggio del consumatore e non costituisca impedimento alla concorrenza.

Sono operazioni di concentrazione soggette all'applicazione della Legge 287/1990 (i) la fusione di due o più imprese; (ii) l'acquisizione, da parte di una o più imprese (o di uno o più soggetti che abbiano il controllo di almeno un'impresa), del controllo diretto o indiretto dell'insieme o di parti di una o più imprese, mediante acquisto di azioni o di elementi del patrimonio, contratto o con qualsiasi altro mezzo; (iii) la costituzione, da parte di due o più imprese, di un'impresa comune che esercita stabilmente tutte le funzioni di un'entità autonoma (art. 4 Legge 287/1990).

Le operazioni di concentrazione devono essere preventivamente comunicate all'Autorità Garante della Concorrenza e del Mercato secondo quanto previsto dall'art. 16 della Legge 287/1990 qualora il fatturato totale realizzato a livello nazionale dall'insieme delle imprese interessate sia superiore a determinate soglie.

Al termine dell'istruttoria, qualora l'Autorità Garante ritenga che un'operazione di concentrazione abbia (o possa avere) l'effetto di ostacolare in modo significativo la concorrenza nel mercato, determinando la costituzione o il rafforzamento di una posizione dominante, ne vieta l'esecuzione, ovvero l'autorizza prescrivendo le misure necessarie ad impedire tali effetti restrittivi o distorsivi della concorrenza.

Pratiche commerciali scorrette

Sono, altresì, vietate le pratiche commerciali scorrette nei confronti dei consumatori, ossia le pratiche commerciali in contrasto con il principio della diligenza professionale, falsa o idonea a falsare in misura apprezzabile il comportamento economico del consumatore medio che raggiunge o al quale è diretta o del membro medio di un gruppo, quando sia diretta a un determinato gruppo di consumatori (art. 20 D. Lgs. 6.9.2005 n. 206 – Codice del Consumo).

In particolare il Codice del Consumo considera scorrette e vieta tassativamente le pratiche commerciali ingannevoli e aggressive, così come definite negli artt. 21 – 26 del D. Lgs. 206/2005 ([27]).

Tutta la popolazione aziendale è tenuta al rispetto delle regole di condotta di seguito indicate, che hanno come obiettivo quello di prevenire la commissione di qualsivoglia illecito in violazione della normativa *antitrust* sopra richiamata.

Programma di compliance antitrust e regole di comportamento

Al fine di assicurare che l'attività della Società si svolga in conformità alla normativa antitrust ed a quella posta a protezione del consumatore, C.E.R. S.r.l. adotta un programma di compliance e protocolli operativi conformi alla normativa di riferimento ed alle Linee Guida adottate dall'Autorità Garante della Concorrenza e del Mercato (di seguito, AGCM).

In particolare, C.E.R. S.r.l. riconosce il valore della concorrenza come parte integrante della propria cultura e politica aziendale, provvedendo all'identificazione e valutazione degli eventuali rischi antitrust ed implementando processi decisionali e gestionali idonei a ridurre il rischio che siano poste in essere condotte in violazione della concorrenza e pratiche commerciali scorrette,

---

[27] Rinviando agli artt. 21 e ss. del Codice del Consumo per la descrizione dettagliata delle caratteristiche e dei requisiti delle pratiche commerciali ingannevoli e aggressive, può ritenersi – in sintesi – "pratica commerciale ingannevole" quella che contiene informazioni non rispondenti al vero o che comunque, in qualsiasi modo ed anche nella sua presentazione complessiva, è idonea ad indurre in errore il consumatore medio, falsandone il processo decisionale. È considerata ingannevole anche la pratica commerciale che omette informazioni rilevanti di cui il consumatore medio ha bisogno per prendere una decisione consapevole di natura commerciale.

L'Autorità Garante considera ingannevoli ed illecite anche le pratiche che inducono il consumatore a trascurare le normali regole di prudenza o vigilanza relativamente all'uso di prodotti pericolosi per la salute e la sicurezza o che possano, anche indirettamente, minacciare la sicurezza di bambini o adolescenti.

Costituisce, invece, "pratica commerciale aggressiva" quella che, mediante molestie, coercizione o indebito condizionamento, è idonea a limitare considerevolmente la libertà di scelta o di comportamento del consumatore medio in relazione al prodotto e, pertanto, lo induce (o è idonea ad indurlo) ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso.

Il Codice del consumo elenca, peraltro, negli artt. 23 e 26 le pratiche commerciali che devono essere considerate in ogni caso ingannevoli o aggressive.

nonché monitorando l'osservanza della normativa antitrust e predisponendo specifici canali per l'eventuale segnalazione della sua violazione (piattaforma whistleblowing; cfr. par. 4.7). C.E.R. S.r.l. provvede, altresì, ad erogare agli esponenti aziendali una specifica formazione antitrust (cfr. par. 3.5.12).

La Società si avvale di un Compliance Officer Antitrust che svolge la propria attività *in service* nell'interesse di tutte le Società del Gruppo.

Al Compliance Officer Antitrust – che riporta al vertice aziendale – è attribuita la verifica preventiva della compatibilità con la disciplina antitrust di delibere societarie, accordi o pratiche commerciali potenzialmente rilevanti ai fini della concorrenza o per la tutela del consumatore, l'istruttoria di eventuali segnalazioni aventi ad oggetto possibili violazioni della normativa antitrust (o di pratiche commerciali scorrette), la pianificazione, in accordo con le competenti funzioni aziendali, delle attività di formazione in materia antitrust, nonché il monitoraggio dell'evoluzione della normativa antitrust (anche con riferimento alle determinazioni dell'AGCM).

Al fine di assicurare l'osservanza della normativa antitrust e del programma di compliance aziendale, tutti gli esponenti aziendali sono tenuti al rigoroso rispetto delle seguenti regole minime di condotta:

- È fatto divieto di porre in essere qualsiasi condotta che integri o possa integrare gli illeciti più sopra descritti (intese restrittive della concorrenza; abuso di posizione dominante; operazioni di concentrazione restrittive della libertà di concorrenza), nonché pratiche commerciali scorrette;
- È fatto divieto di scambiare con i concorrenti informazioni sensibili ai fini della normativa antitrust e di concludere o partecipare a intese (formale o informali) con concorrenti, che possano incidere o limitare la strategia commerciale della Società o del Gruppo;
- È fatto obbligo a tutti gli esponenti aziendali di coinvolgere preventivamente la Funzione Compliance ed il Compliance Officer Antitrust per la valutazione di conformità normativa di ogni iniziativa di business, che possa integrare un comportamento potenzialmente idoneo a realizzare una violazione della normativa *antitrust*, secondo quanto precedentemente descritto;
- È fatto obbligo a tutti gli esponenti aziendali di segnalare, anche in forma anonima, ogni possibile violazione della normativa antitrust mediante il portale per le segnalazioni *whistleblowing*, utilizzando il link disponibile sul sito www.gruppoapi.com (cfr. par. 4.7); le

segnalazioni verranno gestite dall'Antitrust Compliance Officer, in conformità alle procedure interne di Sòlergys S.p.A.;

- È fatto obbligo a tutti gli esponenti aziendali di partecipare alla formazione in materia Antitrust nel rispetto dei programmi e dei contenuti predisposti dalle competenti Funzioni aziendali.

Allo scopo di assicurare un proficuo scambio di informazioni sono, inoltre, previsti incontri e flussi informativi fra il Compliance Officer Antitrust e l'Organismo di Vigilanza (cfr. par. 4.6).

C.E.R. S.r.l. adotta i provvedimenti disciplinari, secondo quanto previsto nel presente Modello, in caso di violazione delle suddette regole di comportamento.

3.5.9. Sistema di gestione della privacy

Il Regolamento 27 aprile 2016 "*General Data Protection Regulation*" (di seguito, "GDPR"), pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016 – operativo ed applicabile, in via diretta, in tutti i Paesi membri dell'Unione Europea dal 25 maggio 2018 – persegue l'obiettivo di rafforzare la protezione dei dati personali delle persone fisiche e di armonizzare le regole privacy degli Stati membri.

Il GDPR è fondato su tre principi ispiratori, che permeano e sostengono l'intero impianto normativo, la cui violazione determina l'applicabilità delle sanzioni delineate dagli artt. 83 e ss., cui si aggiungono le sanzioni penali previste dal D. Lgs 10 agosto 2018 n. 101 (entrato in vigore il 19.9.2018).

In particolare, i principi essenziali su cui si fonda il GDPR sono:

- *l'accountability*, ossia il principio di responsabilizzazione del titolare (art. 32 GDPR). Viene attribuito al Titolare il compito di definire autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative ed alla luce di alcuni criteri indicati nel Regolamento. Ciò impone un approccio integrato, che interessi tutte le aree aziendali, concreto e *risk-based* e che dia luogo a comportamenti proattivi.
- *la privacy by design*, che impone l'adozione di misure di protezione fin dalla fase di progettazione del trattamento (art. 25 GDPR).

- *la privacy by default*, che prescrive un utilizzo che si limiti, per impostazione predefinita, ai dati personali necessari (e sufficienti) a rispondere alle finalità specifiche della gestione dei dati e per il periodo strettamente necessario a tali fini (art. 25 GDPR).

Tali principi ispiratori si riflettono negli adempimenti richiesti del GDPR, che rappresentano una delle principali novità ivi previste, ovvero:

- l'istituzione del Registro delle attività di trattamento (art. 30 GDPR);
- la designazione del Responsabile della protezione dei dati (RDP o DPO - *Data Protection Officer*) (art. 37-39 GDPR);
- il processo di data breach (artt. 33 e 34 GDPR).

Registro delle attività di trattamento

In linea con quanto previsto dal GDPR, la Società ha istituito il Registro delle attività di trattamento dei dati personali.

L'istituzione e la tenuta Registro costituisce uno degli adempimenti principali richiesti al titolare ed al responsabile del trattamento e costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività di trattamento.

Il Registro delle attività di trattamento aziendale è compilato in relazione a ciascuna area dalle figure aziendali specificamente individuate dai referenti interni del titolare. È articolato in sezioni e deve contenere le seguenti informazioni:

- l'area o la struttura aziendale di riferimento;
- le finalità del trattamento;
- la descrizione delle categorie di interessati e delle categorie di dati personali;
- il termine ultimo previsto per la cancellazione delle diverse categorie di dati;
- le operazioni di trattamento (es: raccolta, estrazione, elaborazione, ecc.);
- le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- il tipo di supporto in cui sono contenuti (se informatico, cartaceo o entrambi);
- input (raccolta dati): se presso l'interessato, oppure no;

- la descrizione degli strumenti elettronici usati;
- le banche dati contenenti i dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative;
- il luogo di custodia dei supporti di memorizzazione;
- le strutture che concorrono al trattamento dei dati;
- il nominativo del Privacy contact o coordinator, nonché di eventuali responsabili esterni, amministratori di sistema e contitolari;
- le istruzioni specifiche per le persone autorizzate al trattamento.

Responsabile della protezione dati (Data Protection Officer – DPO)

Il Consiglio di Amministrazione ha nominato il Responsabile della Protezione Dati (Data Protection Officer, di seguito anche DPO) ai sensi dell'art. 37 Regolamento 2016/679/UE, attribuendogli i compiti indicati nell'art. 39 del Regolamento e nello specifico:

- informare e fornire consulenza al Titolare del trattamento o al responsabile interno del trattamento, nonché a coloro che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati Membri relative alla protezione dei dati;
- sorvegliare l'osservanza del Regolamento, nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione di responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del Regolamento;
- cooperare con l'Autorità di Controllo (Garante Privacy) e fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 ed effettuare, se del caso, consultazioni relativamente alle leggi in materia di privacy presenti nell'ordinamento giuridico italiano.

Il Data Protection Officer cura, inoltre, la diffusione della cultura della protezione dei dati all'interno dell'azienda, monitora l'evoluzione della normativa (anche di natura tecnica) attinente alla privacy e supporta l'Organo amministrativo ed il management aziendale nella valutazione –

per gli aspetti con rilevanza sulla privacy – di eventuali nuove iniziative e progetti, che abbiano (o possano avere) impatto sulla protezione dei dati personali.

Il DPO provvede, altresì, a promuovere – in collaborazione le competenti funzioni aziendali – attività di formazione in materia di protezione dei dati personali e funge da punto di contatto per gli interessati, per tutte le tematiche attinenti al trattamento e alla protezione dei loro dati personali, ivi incluso l'esercizio dei diritti loro spettanti.

In conformità a quanto previsto dal GDPR, per garantire l'adempimento dei compiti che gli sono attribuiti, al DPO – nello svolgimento delle proprie mansioni – sono garantite le risorse necessarie in termini di struttura e budget.

Il DPO riporta direttamente all'Amministratore delegato e non è soggetto a direttive e/o istruzioni gerarchiche nello svolgimento delle attività e dei compiti che gli sono attribuiti, che possano influenzare la sua autonomia ed il suo giudizio.

I dati di contatto del DPO sono pubblicati sul sito web del gruppo (con istituzione di una casella PEC dedicata), sono inseriti nelle informative privacy e sono portati a conoscenza dell'organizzazione aziendale, mediante pubblicazione sul sito web del gruppo www.ip.gruppoapi.com , nonché comunicati al Garante.

Il Responsabile della Protezione Dati di C.E.R. S.r.l. svolge funzioni di DPO anche per la controllante Italiana Petroli S.p.A. (e per le altre società del Gruppo controllate da Italiana Petroli S.p.A.).

Tutti i pareri e le indicazioni forniti dal DPO sono documentati. Analogamente, in caso di disaccordo, sono documentate le ragioni che abbia indotto il management aziendale a non conformarsi alle indicazioni del Responsabile della Protezione Dati.

Procedura di data breach

Per *data breach* (violazione dei dati personali) si intende la violazione di sicurezza, che comporta – accidentalmente o in modo illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Secondo il GDPR, la notifica di eventuali violazioni di dati deve avvenire senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui si è venuti a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.

Le eventuali ipotesi di *data breach* sono gestite in conformità a quanto previsto dalla specifica procedura adottata e implementata da

Titolare, responsabili, referenti interni e persone autorizzate al trattamento sotto l'autorità diretta del Titolare del trattamento.

Il Regolamento definisce caratteristiche soggettive e le responsabilità del Titolare e Responsabile del trattamento. Inoltre, pur non prevedendo espressamente la figura dell'«incaricato del trattamento», il regolamento non ne esclude la presenza, in quanto fa comunque riferimento a "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*" (art. 4, n. 10 del GDPR).

In adempimento di queste disposizioni, C.E.R. S.r.l. ha, pertanto, provveduto ad individuare le seguenti figure:

- il Titolare del trattamento (la Società, in persona dell'Amministratore delegato);
- il referente interno del Titolare ai sensi del GDPR;
- gli istruiti al trattamento;
- i responsabili esterni;
- gli amministratori di sistema.

Titolare del trattamento

Titolare del trattamento, ai sensi dell'art. 4 n. 7) e art. 24 del Regolamento, è la Società – nella persona del Presidente del Consiglio di Amministrazione – cui spetta l'adozione delle misure tecniche e organizzative adeguate a garantire che i trattamenti di dati personali effettuati sono conformi al Regolamento.

C.E.R. S.r.l., titolare del trattamento, con apposita nomina dei referenti ha distribuito le istruzioni sui trattamenti al personale aziendale e assimilato che gestisce dati.

Le istruzioni vengono formalizzate in apposito documento e contengono precise indicazioni in ordine alle modalità del trattamento nel rispetto della finalità di raccolta, in ottemperanza a quanto previsto sul piano normativo e in conformità alla Policy interna sul corretto utilizzo dei sistemi informatici aziendali.

Amministratori di sistema

In conformità al provvedimento del Garante in data 27.11.2008 i sistemi informativi hanno un proprio Amministratore di Sistema nominato e verificato ognuno per le proprie competenze che riporta al Responsabile della Funzione Tecnologico.

La nomina degli amministratori di sistema deve avvenire in conformità alla vigente normativa e devono essere indicati i soggetti terzi cui è affidato il trattamento dei dati in out-sourcing con incarico di Amministratore di sistema, con indicazione della tipologia di dati trattati e del referente interno di C.E.R. S.r.l.

Responsabili esterni del trattamento

Sono designati Responsabili esterni del trattamento di dati personali i soggetti (esterni), cui siano affidate attività che implicano il trattamento, per conto e nell'interesse di C.E.R. S.r.l., di banche dati nella disponibilità della Società medesima.

I Responsabili esterni del trattamento devono essere nominati dal titolare con specifica indicazione della tipologia di dati trattati e del referente interno di C.E.R. S.r.l.

Titolare autonomo del trattamento

I titolari autonomi del trattamento con i quali la società ha rapporti rilasciano autocertificazione ai sensi dell'art. 47 del D.P.R. 445/2000 in ordine alle corrette modalità di gestione del trattamento.

Contitolare del trattamento

Quando due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento, entrambi sono contitolari del trattamento. In tal caso, gli stessi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza del regolamento.

Informative e Consensi

Ai sensi del GDPR, l'interessato ha il diritto di conoscere preventivamente per quali finalità e con quali modalità vengano trattati dal Titolare i dati che lo riguardano.

L'informativa deve essere fornita all'interessato, prima di effettuare la raccolta dei dati (ove raccolti direttamente presso l'interessato). Se i dati non sono raccolti direttamente presso

l'interessato, l'informativa deve essere fornita entro un termine ragionevole e, comunque entro 1 mese o, nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato oppure, qualora sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali e deve comprendere le categorie di dati personali oggetto di trattamento (art. 14 GDPR).

Come previsto dagli artt. 13 e 14 del Regolamento, nell'informativa il Titolare deve in ogni caso specificare:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del DPO, ove applicabile;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- qualora il trattamento si basi su un legittimo interesse del titolare del trattamento o di terzi, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l'eventuale intenzione del titolare del trattamento di trasferire dati personali ad un Paese terzo o ad un'organizzazione internazionale
- il periodo di conservazione dei dati, ovvero i criteri utilizzati per determinare tale periodo;
- i diritti degli interessati ([28])
- quando la comunicazione di dati personali sia un obbligo legale o contrattuale, ovvero un requisito necessario per la conclusione di un contratto e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, in questi casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

[28] E, in particolare, (i) il diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la loro cancellazione o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; (ii) qualora il trattamento sia basato sul perseguimento di un interesse legittimo del Titolare del trattamento o di terzi, oppure sull'art. 9, comma 2 lett. a) del regolamento, il diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; (iii) il diritto di proporre reclamo a un'Autorità di controllo.

Le informative per la raccolta del consenso al trattamento dei dati sono redatte dalla Società in conformità alle previsioni del GDPR. È prevista un'apposita procedura relativa alla gestione delle richieste di esercizio dei diritti dell'interessato.

3.5.10. Sistema di flussi da e verso il Data Protection Officer (DPO)

In conformità a quanto previsto dal GDPR, la Società ha istituito e implementato un sistema strutturato di flussi informativi da e verso il Data Protection Officer, qui di seguito descritti.

Allo scopo di assicurare un proficuo scambio di informazioni sono, inoltre, previsti incontri e flussi informativi fra il DPO e l'Organismo di Vigilanza.

Flussi verso il Data Protection Officer

Come richiesto dal GDPR, il DPO deve essere coinvolto in tutte le questioni che potrebbero incidere sul corretto trattamento dei dati.

Il Titolare del trattamento assicura, pertanto, che il DPO:

- partecipi alle riunioni tenute dal vertice aziendale, ove si prospetti la trattazione di questioni o vengano assunte decisioni che incidano (o potrebbero incidere) sul trattamento e/o la protezione dei dati personali o, comunque, ne venga tempestivamente informato. A tal fine, al DPO devono essere trasmesse tutte le informazioni riguardanti eventuali modifiche organizzative o riguardanti le attività svolte dalla Società e/o eventuali iniziative o progetti, che potrebbero impattare sulle modalità o finalità di trattamento dei dati personali, affinché gli sia consentito di fornire un'adeguata consulenza al management aziendale;
- sia tempestivamente consultato qualora vi sia un dubbio, si verifichi una violazione dei dati personali o qualsiasi altro incidente che possa incidere sugli stessi (data breach);
- riceva con cadenza almeno semestrale tutte le informazioni afferenti alle modalità del trattamento dei dati da parte dei referenti interni di Sòlergys S.p.A. In particolare, i referenti interni sono tenuti a fornire al DPO informazioni tempestive sulle modalità del trattamento, per garantirne l'effettività e la continuità d'azione.

Inoltre, indipendentemente e ad integrazione dell'informativa periodica di cui sopra, il DPO deve essere tempestivamente informato:

- di ogni violazione di dati personali e di qualunque comportamento in violazione della normativa in materia di protezione dei dati personali;

- di ogni provvedimento dell'Autorità giudiziaria e/o di organi di polizia giudiziaria o di qualsiasi altra Autorità, dai quali risulti o possa evincersi la commissione di reati informatici o, comunque, una violazione delle disposizioni in materia di protezione dei dati personali o del Modello privacy;
- delle richieste di assistenza legale pervenute dal personale in caso di avvio di procedimento penale a loro carico in relazione a reati informatici o, comunque, a reati previsti dal D. Lgs 10.8.2018 n. 101, commessi nello svolgimento dell'attività lavorativa,
- degli esiti di attività di controllo svolte da Autorità pubbliche, dal Sindaco unico o da esponenti aziendali, dalle quali risulti una violazione di dati personali o, comunque, la mancata osservanza delle norme in materia di protezione dei dati personali o del Modello privacy;
- di ogni eventuale violazione del Modello privacy e degli illeciti disciplinari di cui la funzione Risorse Umane (o altra funzione aziendale) sia venuta a conoscenza e che possano integrare anche una violazione della normativa in materia di protezione dei dati personali e/o del Modello privacy.

L'Organismo di Vigilanza provvede, inoltre, ad informare il DPO di ogni eventuale violazione del Modello di Organizzazione, gestione e controllo di cui al D. Lgs. 231/2001, che possa integrare anche una violazione di dati personali (o, comunque, una possibile violazione della normativa in materia di privacy), nonché qualsiasi dato, informazione e notizia di cui sia venuto a conoscenza nell'esercizio delle proprie funzioni e che evidenzi la possibile commissione (o il rischio di commissione) di condotte critiche sotto il profilo privacy, ad esempio recanti un rischio di *data breach.*

Tutti gli esponenti aziendali che siano venuti a conoscenza di una violazione di dati personali e/o di qualsiasi altra violazione alla normativa privacy, ovvero abbiano motivo di ritenere che tale normativa sia stata violata, sono tenuti a darne senza ritardo comunicazione al Data Protection Officer. Analogamente, qualsiasi soggetto esterno alla Società, che abbia motivo di ritenere che sia stata commessa (o sia venuto a conoscenza di) una violazione della normativa privacy, può segnalarla al Data Protection Officer.

Al fine di facilitare i flussi di comunicazione verso il DPO, la Società ha istituito uno specifico canale di segnalazione e comunicazione, rappresentato da una casella di posta elettronica dedicata (dpocer@pec.gruppoapi.com), al quale è assicurata adeguata pubblicità, mediante pubblicazione nel sito web del gruppo.

In alternativa, al DPO di C.E.R. S.r.l. possono essere inviate anche segnalazioni e comunicazioni in forma scritta presso la sede della Società all'indirizzo C.E.R. S.r.l. – Via Salaria 1322 – 00138 ROMA, anch'esso pubblicato sul sito web del Gruppo.

Flussi dal Responsabile della Protezione Dati (DPO) verso la Società e l'Organismo di Vigilanza

Coerentemente con quanto previsto dal Regolamento, il DPO deve provvedere a fornire all'Organo amministrativo le informazioni e gli elementi conoscitivi utili per definire le scelte gestionali opportune ad assicurare la protezione dei dati personali.

Sono, pertanto, previsti specifici obblighi di informazione periodica e ad evento del DPO verso il Consiglio di Amministrazione, secondo le cadenze e con le modalità di seguito descritte. Gli obblighi di informazione sono estesi anche nei confronti del Collegio Sindacale, per l'esercizio delle funzioni di controllo a lui demandate.

In particolare, il DPO predispone ed invia al Consiglio di Amministrazione ed al Sindaco unico un'informativa annuale sull'osservanza del Regolamento e delle politiche aziendali in materia di privacy, sull'attuazione del Modello di organizzazione, gestione e controllo della privacy (di seguito, per brevità, anche "Modello privacy") e sugli esiti dell'attività di vigilanza svolta, con indicazione di eventuali interventi per l'implementazione e il miglioramento del Modello privacy. L'informativa contiene almeno le seguenti informazioni:

- la descrizione dei controlli sul trattamento dei dati che hanno impatto sul corretto funzionamento e sull'adeguata osservanza del Modello privacy adottato da C.E.R. S.r.l.;
- la descrizione della regolarità e della completezza dei flussi informativi;
- l'indicazione di eventuali modifiche normative in materia di protezione dei dati rilevanti, al fine di agevolare l'aggiornamento del Modello privacy;
- la descrizione generale delle misure di sicurezza tecniche e organizzative implementate, anche in ottica di prevenzione dei reati informatici;
- l'osservanza del Modello privacy e le eventuali violazioni o carenze riscontrate;
- i controlli espletati in relazione alle violazioni riscontrate ed i relativi esiti, nonché le misure adottate per l'eliminazione delle carenze che hanno determinato tali violazioni;
- l'indicazione di eventuali controversie insorte con privati in ordine al trattamento dei dati;
- la rendicontazione sull'utilizzo delle risorse assegnate;

- l'elencazione dei rapporti intervenuti nel periodo di riferimento con l'Autorità Garante in relazione
  - ✓ alle eventuali richieste preliminari effettuate ai sensi dell'art. 17 del Codice Privacy (rischi specifici rispetto al trattamento dati), ovvero ai sensi della analoga previsione di cui all'art. 36 del GDPR (consultazione preventiva nel caso in cui il RDP abbia indicato al Titolare un rischio specifico rispetto ad un determinato trattamento dei dati);
  - ✓ alle eventuali informazioni trasmesse ai sensi dell'art. 157 del Codice Privacy (richiesta di informazioni da parte del Garante);
  - ✓ agli adempimenti ex art. 33 del GDPR (data breach);
  - ✓ alle autorizzazioni richieste ai sensi degli artt. 46 e 47 del GDPR (trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali).

Il DPO riferisce, inoltre, senza ritardo, al Consiglio di Amministrazione ed al Sindaco unico di ogni eventuale violazione di dati personali di cui venga a conoscenza nell'esercizio delle sue attività o che gli sia stata segnalata, nonché di ogni comportamento non conforme alla vigente normativa ed al Modello privacy, che comporti o possa comportare una violazione o un trattamento illecito di dati personali e, comunque, ogniqualvolta lo ritenga opportuno, in ordine a circostanze e fatti che ritenga rilevanti per il funzionamento e l'osservanza del Modello privacy.

Il DPO può essere convocato in qualsiasi momento dal Consiglio di Amministrazione e, a sua volta può richiedere al C.d.A. di essere sentito qualora ravvisi l'opportunità di riferire su questioni inerenti al funzionamento del Modello privacy, il trattamento dei dati e/o l'osservanza del Regolamento.

Il DPO comunica, inoltre, all'Organismo di Vigilanza ogni elemento e informazione utile per l'adempimento dei compiti ad esso spettanti, nonché qualsiasi dato, informazione e notizia che evidenzi la possibile commissione (o il rischio di commissione) di reati rilevanti ai sensi del D. Lgs. 231/2001 e, in particolare, di reati informatici.

3.5.11. Organismo di Vigilanza e sistema di flussi informativi

Come accennato, l'art. 6, comma 1 lett. b) del Decreto prevede, tra i presupposti per l'esonero dalla responsabilità in caso di commissione di un reato presupposto, che l'ente o la società abbia provveduto ad istituire un organismo, dotato di autonomi poteri di iniziativa e controllo, con il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento.

A sua volta, l'art. 6, comma 2 lett. d) del Decreto impone che il Modello di organizzazione, gestione e controllo preveda "*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza*" del Modello stesso.

C.E.R. S.r.l. ha provveduto ad istituire e nominare un Organismo di Vigilanza monocratico, composto di tre membri, ed a definire ed implementare flussi informativi strutturati verso l'Organismo, per assicurare un efficace esercizio dei suoi compiti di vigilanza sull'osservanza ed il funzionamento del presente Modello.

Per la descrizione delle caratteristiche, delle funzioni e dei compiti dell'Organismo di Vigilanza e del sistema dei flussi informativi da e verso l'Organismo, si rinvia *infra* al paragrafo 4.

3.5.12. Piano di formazione

La formazione costituisce uno strumento imprescindibile per un'efficace implementazione del Modello di organizzazione e per una diffusione capillare dei principi di comportamento e di controllo adottati da C.E.R. S.r.l., al fine della prevenzione dei reati di cui al D. Lgs. 231/2001 e, più in genere, con comportamenti contrastanti con il sistema dei principi e di valori cui è ispirata l'attività del Gruppo e/o con le normative di settore che la Società è tenuta ad applicare.

Il programma di formazione rispetta ed attua i seguenti requisiti:

- ✓ il programma deve essere adeguato alla posizione ricoperta dai soggetti all'interno dell'organizzazione;
- ✓ la periodicità dell'attività di formazione deve essere calibrata in funzione delle modifiche intervenute nell'organizzazione e/o nell'attività aziendale e del grado di cambiamento cui è soggetto l'ambiente esterno, nonché della capacità di apprendimento del personale;
- ✓ i soggetti che erogano la formazione devono essere autorevoli e dotati di specifica competenza in relazione alle tematiche da trattare, al fine di assicurare la qualità dei contenuti trattati, nonché di rendere esplicita l'importanza che la formazione in oggetto riveste per C.E.R. S.r.l. e per le strategie che essa intende perseguire;
- ✓ la partecipazione al programma di formazione è resa obbligatoria per tutta la popolazione aziendale.

La formazione è svolta al fine di consentire a ciascun esponente aziendale di:

- conoscere le finalità ed i principali contenuti del D. Lgs. 231/2001, acquisendo altresì consapevolezza che C.E.R. S.r.l. intende assicurarne l'osservanza e renderle parte integrante della cultura aziendale;
- acquisire conoscenza del Modello e del Codice Etico e dei suoi contenuti (comprensivi delle Linee Guida Anticorruzione e Antitrust e del Sistema di gestione della privacy), delle sue finalità e delle sue prescrizioni, nonché degli obiettivi che la Società si prefigge di raggiungere tramite l'implementazione del Modello;
- acquisire consapevolezza del proprio ruolo e responsabilità all'interno del sistema di controllo interno presente C.E.R. S.r.l.;
- conoscere quali sono i comportamenti attesi e quelli vietati o ritenuti comunque non accettabili da C.E.R. S.r.l. e delle conseguenze e sanzioni correlate alla violazione del Modello e del Codice Etico;
- conoscere i canali di reporting adeguati al tipo di informazione che si vuole comunicare ed al soggetto cui si vuole far pervenire la comunicazione: a tal fine, la formazione deve comprendere l'indicazione e delle modalità con le quali segnalare eventuali violazioni del Modello nello svolgimento delle attività aziendali ed essere estesa all'illustrazione dei principali contenuti del D. Lgs. 24/2023 ed al funzionamento dei canali di segnalazione *whistleblowing*;
- conoscere i poteri e i compiti dell'Organismo di Vigilanza e gli obblighi informativi nei confronti di tale Organismo.

3.5.13. Comunicazione del Modello

In linea con quanto disposto dal Decreto e dalle Linee Guida di Confindustria, C.E.R. S.r.l. provvede a dare comunicazione del Modello e del Codice Etico e di loro eventuali modifiche o integrazioni, al fine di assicurare che gli esponenti aziendali siano a conoscenza dei suoi elementi.

In particolare, al fine di assicurare la diffusione del Modello nel contesto aziendale, il Modello ed il Codice Etico sono resi disponibili nel sito web del gruppo (www.ip.gruppoapi.com).

3.5.14. Informativa ai Collaboratori esterni ed ai Partner

C.E.R. S.r.l. promuove, altresì, la conoscenza e l'osservanza dei principi, dei valori e delle regole di condotta previsti dal Modello e dal Codice Etico anche da parte dei soggetti esterni

all'organizzazione aziendale che svolgono attività nell'interesse della Società (procuratori speciali e/o consulenti), nonché da parte dei partner commerciali e finanziari e dei fornitori.

A tali soggetti vengono, pertanto, resi disponibili il Modello (Parte Generale) ed il Codice Etico nelle modalità ritenute più opportune, ad esempio tramite pubblicazione (integrale o per estratto) dei medesimi nel sito internet aziendale o del Gruppo.

Sono, inoltre, predisposti meccanismi per l'inserimento e l'accettazione di clausole contrattuali specifiche che le Funzioni competenti, sentita la funzione Compliance, provvedono ad introdurre nelle procure speciali e negli schemi contrattuali di riferimento, in virtù delle quali procuratori speciali, consulenti, partners commerciali e finanziari e fornitori dovranno impegnarsi ad accettare ed osservare il Modello ed il Codice Etico.

3.5.15. Codice Etico e protocollo per il suo aggiornamento

C.E.R. S.r.l. ha adottato il Codice Etico del Gruppo **(Allegato n. 3 del presente Modello)** con l'obiettivo di garantire il rispetto dei principi, dei valori e delle regole di condotta cui le Società del Gruppo ispirano la propria attività d'impresa e dei quali è richiesta l'osservanza a tutti gli stakeholder (soci, amministratori, partners commerciali e finanziari, consulenti, fornitori).

Il Codice Etico costituisce parte integrante del Modello, dettando una serie di principi e di regole di condotta, che contribuiscono alla prevenzione dei reati previsti dal Decreto, nonché all'osservanza delle regole di comportamento previste dalle Linee Guida Anticorruzione e Antitrust e dalla normativa a protezione dei dati personali.

Al Codice Etico è assicurata ampia diffusione, anche mediante pubblicazione sul sito web del Gruppo, in modo da assicurarne la conoscenza da parte di tutti i destinatari.

L'Organismo di Vigilanza è deputato al controllo circa l'osservanza del Codice Etico e deve comunicare tempestivamente ogni eventuale necessità di modifica o di aggiornamento al Consiglio di Amministrazione.

Eventuali problematiche inerenti all'applicazione del Codice Etico devono essere tempestivamente segnalate all'Organismo di Vigilanza. È fatto obbligo a chiunque venga a conoscenza di violazioni al Codice Etico o di eventi suscettibili di alterarne la portata e l'efficacia, di darne pronta segnalazione all'O.d.V.

3.5.16. Sistema disciplinare e sanzionatorio (rinvio)

Gli artt. 6, comma 2 e 7, comma 4 del Decreto richiedono – per l'efficace attuazione del Modello – che l'ente provveda ad introdurre un adeguato sistema disciplinare "*idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*".

Dando attuazione a queste disposizioni, C.E.R. S.r.l. ha previsto un sistema autonomo di sanzioni disciplinari, finalizzato a rafforzare l'osservanza e l'efficace attuazione del Modello e destinato a colpire le violazioni del Modello e del Codice Etico.

Il sistema disciplinare, la tipologia delle sanzioni ed i meccanismi per la loro irrogazione sono descritti nel paragrafo 5, al quale si fa rinvio.

4. L'ORGANISMO DI VIGILANZA

Come esposto, l'art. 6, comma 1, lett. b) del Decreto indica, tra i presupposti indispensabili per l'esonero dalla responsabilità, che l'ente provveda ad affidare ad un Organismo (l'Organismo di Vigilanza), dotato di autonomi poteri di iniziativa e controllo, il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento.

Come evidenziato dalla Linee Guida di Confindustria, il conferimento di questi compiti all'Organismo di Vigilanza (nel seguito, anche O.d.V.) e il loro corretto ed efficace svolgimento costituiscono, quindi, adempimenti indispensabili per l'esonero dalla responsabilità.

È necessario, inoltre, che l'Organismo sia posto nelle condizioni di assolvere realmente ai complessi e delicati compiti di cui la legge lo investe, attraverso un sistema di flussi informativi e la dotazione delle necessarie risorse finanziarie.

4.1. Requisiti dell'Organismo di Vigilanza

Sulla base di quanto disposto dal D. Lgs. 231/2001 e dalle Linee Guida di Confindustria (e tenuto conto degli orientamenti giurisprudenziali), affinché il Modello spieghi efficacia esimente l'Organismo di Vigilanza deve soddisfare una serie di requisiti, di seguito indicati.

Autonomia e indipendenza

Come precisato dalle Linee Guida di Confindustria l'Organismo di Vigilanza deve essere dotato di autonomi poteri di iniziativa e di controllo e risultare indipendente.

L'autonomia va intesa nel senso che la posizione dell'Organismo di Vigilanza all'interno dell'ente deve essere tale da garantirgli "*autonomia dell'iniziativa di controllo da ogni forma di interferenza o condizionamento da parte di qualunque componente dell'ente e, in particolare, dell'organo dirigente*".

Al requisito dell'autonomia si affianca quello dell'indipendenza, che richiede che i membri dell'Organismo non risultino condizionati a livello economico e/o personale e non versino in situazioni di incompatibilità o conflitto di interesse (anche solo potenziale).

L'Organismo di Vigilanza, pertanto, pur essendo strutturalmente inserito all'interno dell'ente, non deve dipendere da alcun organo aziendale, ma deve risultare del tutto autonomo nell'esercizio della sua attività, "riportando" (in termini informativi) al vertice aziendale, e deve essere dotato di un budget annuale per l'esercizio delle attività di verifica necessarie per lo svolgimento dei compiti affidatigli.

Inoltre, al fine di garantirne la necessaria autonomia di iniziativa e indipendenza, "*è indispensabile che all'OdV non siano attribuiti compiti operativi che, rendendolo partecipe di decisioni e attività operative, ne minerebbero l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello*".

Allo scopo di assicurare l'effettiva sussistenza dei requisiti di autonomia e indipendenza si richiede, infine, che siano previste cause di ineleggibilità o decadenza dei membri dell'Organismo di Vigilanza e che i suoi membri debbano soddisfare requisiti soggettivi di onorabilità.

In conformità a queste indicazioni, l'Organismo di Vigilanza di C.E.R. S.r.l. nell'esercizio delle sue funzioni, è autonomo e indipendente dagli Organi Societari e dagli altri organismi di controllo interno e dispone di autonome risorse finanziarie e di autonomi poteri di spesa, che può utilizzare a supporto delle attività di verifica necessarie per lo svolgimento dei compiti ad esso affidati. Le attività poste in essere dall'Organismo di Vigilanza di C.E.R. S.r.l. non possono essere sindacate da alcun altro organismo o struttura aziendale.

All'Organismo di Vigilanza sono, inoltre, riconosciuti, nel corso delle verifiche ed ispezioni, i più ampi poteri, per svolgere efficacemente i compiti affidatigli. A tal fine, l'Organismo di Vigilanza di C.E.R. S.r.l. può avvalersi delle diverse funzioni aziendali per svolgere le verifiche ed i controlli che ritiene opportuni.

Il presente Modello, inoltre, prevede – a garanzia dell'autonomia ed indipendenza dei membri dell'Organismo di Vigilanza – cause di ineleggibilità e decadenza dei suoi componenti, nonché i requisiti di onorabilità che gli stessi devono soddisfare per l'assunzione della carica (cfr. *infra* par. 4.3).

Professionalità

Questo requisito si riferisce alle competenze tecniche specialistiche di cui deve essere dotato l'Organismo di Vigilanza, per poter svolgere efficacemente le attività che la norma gli attribuisce.

Per un effettivo esercizio delle funzioni ad esso affidate, è opportuno che l'Organismo possieda conoscenze e competenze specifiche connesse alle attività di verifica e controllo che dovrà svolgere.

C.E.R. S.r.l. ha, pertanto, provveduto a selezionare e nominare quale componente dell'Organismo di Vigilanza un soggetto dotato delle richieste competenze specialistiche.

L'Organismo di Vigilanza può avvalersi, per l'esecuzione di attività connesse allo svolgimento delle funzioni di controllo, che richiedano conoscenze tecniche di natura specialistica, anche di

consulenti esterni. In tal caso, i consulenti dovranno riferire i risultati del loro operato esclusivamente all'Organismo di Vigilanza.

Continuità di azione

Questo requisito deve connotare l'attività dell'Organismo di Vigilanza per garantire l'efficace attuazione del Modello organizzativo e richiede che l'O.d.V. assicuri un esercizio senza soluzione di continuità delle funzioni che gli sono attribuite.

In conformità alle indicazioni delle Linee Guida di Confindustria, per l'Organismo di Vigilanza di C.E.R. S.r.l. – a composizione monocratica – il requisito della continuità di azione è soddisfatto attraverso il supporto del personale della Società.

4.2. Composizione, nomina, durata e revoca dell'Organismo di Vigilanza

In attuazione di quanto previsto dal Decreto e dalle Linee Guida di Confindustria e nel rispetto dei requisiti di autonomia, indipendenza, professionalità e continuità d'azione, C.E.R. S.r.l. ha istituito un Organismo di Vigilanza monocratico, composto da un membro, individuato in ragione delle competenze professionali maturate e delle caratteristiche personali di indipendenza di giudizio ed integrità morale.

Nomina e durata dei componenti dell'Organismo di Vigilanza

L'Organismo di Vigilanza è nominato dal Consiglio d'Amministrazione con provvedimento motivato, scelto esclusivamente sulla base dei requisiti di professionalità, onorabilità, competenza, indipendenza e autonomia funzionale.

Il componente dell'Organismo di Vigilanza rimane in carica sino alla scadenza del Consiglio d'Amministrazione che ha provveduto alla sua nomina.

L'Organismo di Vigilanza si intende decaduto se viene a mancare, per dimissioni o per altre cause, il suo membro unico. In tal caso, il Consiglio di Amministrazione provvede tempestivamente a nominare un nuovo Organismo. L'Organismo di Vigilanza decade, altresì, in caso di decadenza o cessazione del Consiglio di Amministrazione che lo ha nominato.

Revoca, dimissioni e sostituzione dei componenti dell'Organismo di Vigilanza.

Il componente dell'Organismo di Vigilanza può essere revocato solo dal Consiglio di Amministrazione, previa informativa al Collegio Sindacale, quando ricorra una giusta causa di revoca.

Costituisce giusta causa di revoca del componente dell'Organismo di Vigilanza:

a) il sopravvenire di una delle ipotesi di ineleggibilità o di decadenza previste dallo Statuto dell'Organismo di Vigilanza o la perdita dei requisiti di onorabilità richiesti (cfr. par. 4.3);

b) la condanna ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici ovvero l'incapacità ad esercitare uffici direttivi presso persone giuridiche;

c) l'avere riportato condanna, anche non definitiva, o di applicazione della pena per uno dei reati previsti dal D. Lgs. 231/2001;

d) l'inadempimento agli obblighi afferenti all'incarico affidato;

e) la mancanza di buona fede e di diligenza nell'esercizio dell'incarico;

f) l'inattività ingiustificata che abbia comportato l'applicazione di sanzioni interdittive per la Società.

A tali cause di revoca si aggiungono anche le seguenti applicabili al membro dell'O.d.V. in quanto non appartenente al personale della Società, ossia che:

a) sia legato alla Società o a società del Gruppo da un rapporto di natura patrimoniale che ne possa ragionevolmente compromettere l'indipendenza;

b) l'intrattenere o l'aver intrattenuto, anche indirettamente con la Società o con soggetti legati ad essa, relazioni tali da condizionarne l'autonomia di giudizio.

Qualora il membro sia interno, costituisce causa di revoca dell'Organismo di Vigilanza, l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e di "continuità di azione" propri dell'Organismo.

Il componente dell'Organismo di Vigilanza può rassegnare in qualunque momento le dimissioni e cessa dall'incarico nel momento in cui le dimissioni vengano accettate dal Consiglio di Amministrazione, ovvero venga nominato altro componente in sostituzione

A seguito della cessazione, il Consiglio di Amministrazione provvede a nominare un nuovo Organismo di Vigilanza.

Temporaneo impedimento dei componenti dell'Organismo di Vigilanza

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea, al membro dell'Organismo di Vigilanza di svolgere le proprie funzioni, ovvero di svolgerle con la necessaria continuità, egli è tenuto a dare notizia al Consiglio di Amministrazione.

A titolo esemplificativo, costituisce causa di temporaneo impedimento una malattia, infermità o infortunio che impediscano di svolgere l'attività dell'Organismo di Vigilanza per un periodo prolungato.

4.3. Cause di ineleggibilità e di decadenza e requisiti di onorabilità dei membri dell'Organismo di Vigilanza

Il componente dell'Organismo di Vigilanza deve possedere competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere.

A tal fine, viene scelto tra soggetti dotati di specifiche competenze e professionalità riguardanti le tecniche e attività ispettive, le tecniche di analisi, valutazione e contenimento dei rischi, i sistemi di controllo dei rischi, di organizzazione aziendale, la tutela della salute e della sicurezza nei luoghi di lavoro, la tutela dell'ambiente, nonché di specifiche competenze di tipo giuridico (e, in particolare, di carattere penalistico).

Il componente dell'Organismo di Vigilanza deve, inoltre, possedere all'atto dell'assunzione della carica i requisiti di onorabilità previsti dal D.M. 30 marzo 2000 n. 162 per i membri del Collegio Sindacale di società quotate.

Fermi restando i requisiti di cui sopra, non può essere nominato come membro dell'Organismo di Vigilanza e, se nominato, decade dalla carica:

a) colui che sia stato condannato ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici ovvero l'incapacità ad esercitare uffici direttivi presso persone giuridiche;

b) colui che sia stato condannato con sentenza passata in giudicato per aver commesso uno dei reati presupposti previsti dal D.lgs. 231/2001;

c) colui che sia sottoposto a misure cautelari personali per uno dei reati previsti dal D. Lgs. 8.6.2011 n. 231;

d) colui che sia sottoposto, anche in via provvisoria, a misure di prevenzione ai sensi della legge 27 dicembre 1956 n. 1423 o della Legge 31 maggio 1965 n. 575;

e) colui nei confronti del quale sia stata pronunciata sentenza di condanna al risarcimento del danno o, comunque, sentenza civile che abbia accertato l'inadempimento o il carente adempimento degli obblighi incombenti sui componenti dell'Organismo di Vigilanza in riferimento a società cui siano state applicate sanzioni ai sensi del D. Lgs. 8.6.2001 n. 231;

f) colui che si trovi nelle condizioni di cui all'art. 2382 del codice civile;

g) il coniuge, i parenti e gli affini entro il quarto grado degli amministratori di SIGEA S.p.A. e di società controllate o partecipate da SIGEA S.p.A.

h) colui nei confronti del quale sia intervenuto un provvedimento di sospensione o radiazione da albi, ovvero cancellazione (adottata a titolo di provvedimento disciplinare) da elenchi e ordini professionali irrogati dalle Autorità competenti.

Agli effetti dell'applicazione delle disposizioni di cui sopra, alla sentenza penale di condanna è equiparato il decreto penale di condanna, anche non irrevocabile.

Risulta inoltre ineleggibile:

a) colui che abbia svolto nei tre anni antecedenti alla nomina a componente unico dell'O.d.V. funzioni di amministratore in imprese che siano state dichiarate fallite o che siano soggette a liquidazione giudiziale, ovvero ad altre procedure concorsuali o a liquidazione coatta amministrativa;

b) colui che abbia ricoperto, nei tre anni antecedenti all'assunzione della carica di componente dell'Organismo, cariche pubbliche presso amministrazioni centrali o periferiche dello Stato, Agenzie pubbliche, Regioni, Comuni o altri Enti locali, ovvero presso Enti pubblici economici e/o non economici controllati dallo Stato, dalle Regioni, dai Comuni o da altri Enti locali;

c) colui che sia stato, nei tre anni antecedenti all'assunzione della carica di componente dell'Organismo, dirigente o dipendente di amministrazioni centrali o periferiche dello Stato, di Agenzie pubbliche, delle Regioni, di Comuni o altri Enti locali, nonché amministratori, dirigenti o dipendenti di Enti pubblici economici e/o non economici controllati dallo Stato, dalle Regioni o da altri Enti locali;

d) colui che sia legato alla Società da interessi economici rilevanti (quali, rapporti continuativi di collaborazione, consulenza o di prestazione d'opera retribuita di rilevante valore economico) che ne possa compromettere l'autonomia e l'indipendenza.

Decade, inoltre, automaticamente dalla carica colui nei confronti del quale siano venuti meno i requisiti di onorabilità previsti dal D.M. 30 marzo 2000 n. 162 per i membri del Collegio Sindacale di società quotate.

Il membro unico dell'Organismo di Vigilanza deve, inoltre, avere cura di evitare qualsiasi situazione suscettibile di integrare un conflitto di interesse (anche solo potenziale) con SIGEA S.p.A. tale da compromettere la sua autonomia e indipendenza e l'adempimento dei compiti a lui attribuiti.

All'atto dell'accettazione della carica, egli sottoscrive una dichiarazione, con la quale attesta:

1. il possesso dei requisiti di onorabilità richiesti e l'assenza di ragioni ostative all'assunzione dell'incarico e l'impegno a comunicare immediatamente al Consiglio di Amministrazione l'eventuale sopravvenire di circostanze idonee incidere sul mantenimento dei requisiti richiesti;
2. di essere stato adeguatamente informato sulle regole comportamentali ed etiche che la Società ha adottato, ivi comprese quelle contenute nel presente Modello e nel Codice Etico, e l'impegno a farle proprie nello svolgimento dell'incarico;
3. l'impegno a svolgere le funzioni attribuite con diligenza e professionalità, garantendo la necessaria continuità di azione.

4.4. Funzioni e poteri dell'Organismo di Vigilanza. Segreteria tecnica dell'O.d.V.

L'Organismo di Vigilanza dispone – come previsto dal Decreto – di autonomi poteri di iniziativa, intervento e controllo, che si estendono all'intera Società, al fine di svolgere efficacemente e tempestivamente le funzioni previste nel Modello, per assicurare un'effettiva ed efficace vigilanza sul funzionamento e sull'osservanza del Modello e di curare il suo aggiornamento, così come previsto dall'art. 6 del D. Lgs. n. 231/2001.

In adempimento di tali funzioni l'Organismo di Vigilanza dovrà svolgere attività di vigilanza ogniqualvolta ne ravvisi l'opportunità e, comunque, almeno ogni 3 mesi. Le riunioni dell'Organismo dovranno essere verbalizzate ed i verbali saranno conservati presso la Segreteria tecnica dell'Organismo.

Nell'espletamento dei propri compiti, l'Organismo di Vigilanza svolge ogni attività necessaria e/o opportuna a vigilare sul funzionamento e l'osservanza del Modello, esercitando in piena autonomia i propri poteri di iniziativa e di controllo e, in particolare, sarà chiamato a svolgere le attività di seguito indicate (a titolo esemplificativo e non tassativo):

- verificare il rispetto e l'osservanza del Modello, delle regole di comportamento e degli standards di controllo previsti dal Modello e rilevare eventuali scostamenti comportamentali, anomalie o criticità che dovessero emergere dall'analisi dei flussi informativi o dalle segnalazioni pervenute e adottare le iniziative conseguenti, secondo quanto previsto nel Modello;
- predisporre ed attuare un programma di verifiche periodiche, per accertare l'applicazione degli standard di controllo nelle attività a rischio e la loro efficacia, in coerenza con i principi contenuti nel Modello;
- svolgere attività ispettiva e di controllo, anche a sorpresa, sui diversi settori di attività aziendale e le attività sensibili identificate, al fine di evidenziare eventuali debolezze o esigenze di miglioramento dei presidi di controllo;
- effettuare una periodica ricognizione dell'attività aziendale, ai fini dell'aggiornamento della mappatura delle attività a rischio e dei relativi processi sensibili nell'ambito del contesto aziendale;
- effettuare, in caso di presunte violazioni del Modello, i necessari approfondimenti e le opportune indagini interne finalizzate al loro accertamento, anche in vista dell'adozione delle misure sanzionatorie previste dal Modello;
- verificare, nel caso in cui siano riscontrate anomalie o criticità, esigenze di miglioramento dei presidi di controllo, ovvero allorché vengano accertate violazioni del Modello, l'effettiva implementazione da parte della Società delle azioni rimediali o di miglioramento necessarie, anche attraverso l'effettuazione di periodici *follow up* per accertare lo stato di avanzamento di tali azioni;
- promuovere l'aggiornamento del Modello allorché siano identificate significative violazioni delle prescrizioni, ovvero quando intervengono significativi mutamenti nella struttura organizzativa o nell'attività o sopravvengano rilevanti modifiche normative;
- verificare il rispetto delle Codice Etico, nonché delle Linee Guida Anticorruzione, delle Linee Guida e della normativa Antitrust e del Sistema di gestione della privacy, segnalando alla Società eventuali inadempienze o violazioni, per l'adozione dei provvedimenti di competenza, nonché per l'irrogazione delle relative sanzioni;
- promuovere idonee iniziative per la formazione del personale in ambito 231, nonché per la diffusione della conoscenza e della comprensione del Modello, anche attraverso il supporto

delle apposite strutture interne o di consulenti esterni, nonché verificare la realizzazione e promuovere l'aggiornamento della formazione, nel caso di sopravvenute modifiche del Modello o di rilevanti novità normative;

- verificare e monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello nei confronti degli organi sociali, dei procuratori, collaboratori esterni, consulenti, fornitori e partners commerciali e finanziari, secondo quanto previsto dal presente Modello;
- fornire, ove ne sia richiesto, ai membri degli Organi sociali ed ai soggetti che operano in nome e per conto della Società chiarimenti in merito al significato delle previsioni contenute nel Modello, nonché alla corretta interpretazione/applicazione del presente Modello, degli standard di controllo e del Codice Etico;
- segnalare tempestivamente al Consiglio di Amministrazione, per gli opportuni provvedimenti, le eventuali violazioni del Modello, che l'Organismo abbia accertato (anche a seguito di segnalazione pervenuta attraverso i canali a ciò deputati) e proporre le relative sanzioni;
- promuovere idonee iniziative per assicurare a tutti coloro che collaborano con la Società, la conoscenza e la comprensione dei contenuti dell'art. 6, comma 2-bis del Decreto e del D. Lgs. 24/2023 in materia di *whistleblowing*, nonché la conoscenza delle condotte che possono formare oggetto di segnalazione e delle modalità di effettuazione delle segnalazioni;
- verificare l'idoneità del sistema disciplinare adottato ai sensi del D. Lgs. 231/2001;
- monitorare il funzionamento del sistema dei flussi informativi, in modo da assicurare che l'Organismo riceva i flussi informativi di competenza delle strutture organizzative aziendali (cfr. par. 4.5) e provvedere ad alle comunicazioni ed alla reportistica verso il Consiglio di Amministrazione, in conformità a quanto previsto nel paragrafo 4.6.

Poteri dell'Organismo di Vigilanza

Ai fini dello svolgimento delle funzioni di vigilanza e controllo e delle attività sopra elencate, all'Organismo sono attribuiti i più ampi poteri di iniziativa, intervento e controllo, che potranno essere esercitati nei confronti di tutte le strutture aziendali in modo autonomo.

In particolare, nell'esercizio delle proprie funzioni e per l'adempimento dei compiti di vigilanza sul funzionamento e l'osservanza del Modello, l'Organismo potrà:

- ✓ svolgere o provvedere a far svolgere, sotta la sua diretta sorveglianza e responsabilità, attività ispettive periodiche;
- ✓ accedere a tutte le informazioni concernenti le attività sensibili della Società;
- ✓ chiedere informazioni o l'esibizione di documenti in merito alle attività sensibili agli amministratori e al Sindaco unico;
- ✓ chiedere informazioni o l'esibizione di documenti in merito alle attività sensibili a collaboratori, consulenti, agenti e rappresentanti esterni della Società e in genere a tutti i soggetti destinatari del Modello sempre che l'obbligo di ottemperare alle richieste dell'O.d.V. sia espressamente previsto nei contratti o nei mandati che legano il soggetto esterno alla Società;
- ✓ ove necessario per lo svolgimento delle proprie funzioni, chiedere informazioni agli Organismi di Vigilanza delle società appartenenti al Gruppo;
- ✓ avvalersi di consulenti esterni per problematiche di particolare complessità o che richiedono competenze specifiche;
- ✓ proporre all'organo titolare del potere disciplinare l'adozione delle sanzioni ove ne ricorrano i presupposti;
- ✓ sottoporre il Modello a verifica periodica e se necessario proporre al Consiglio di Amministrazione modifiche o aggiornamenti;
- ✓ informare il Consiglio di Amministrazione di fatti urgenti e rilevanti emersi nello svolgimento della propria attività;

Nello svolgimento della propria attività, l'Organismo di Vigilanza può avvalersi del supporto delle strutture organizzative aziendali, con specifiche competenze nei settori aziendali di volta in volta sottoposti a controllo. In particolare:

1. della funzione di Internal Audit della capogruppo operativa, per la verifica dei processi gestionali e dell'applicazione delle procedure organizzative emanate in attuazione del presente Modello, nonché per le attività di identificazione, valutazione e controllo dei rischi di commissione di reati previsti dal D.lgs. n. 231/2001;
2. di altre unità organizzative della Capogruppo operativa e o dei soci, in ordine a specifici controlli come ad esempio un controllo dei flussi finanziari);

3. dell'esponente aziendale preposto alla redazione dei documenti contabili societari per quanto di competenza;
4. di opportuni supporti esterni, secondo le valutazioni del caso.

L'O.d.V. può convocare il Presidente del Consiglio di Amministrazione e il DPO al fine di acquisire le opportune informazioni e condividere le tematiche di compliance integrata, nell'ottica di un sistema integrato di gestione dei rischi.

È previsto, inoltre, per il corretto e completo espletamento delle attività di vigilanza, un coordinamento sistematico dell'O.d.V. con tutte le Funzioni aziendali della Società.

Al fine dell'esercizio delle funzioni e dei poteri di cui sopra, all'Organismo di Vigilanza è attribuita piena autonomia operativa e accesso senza limitazioni alle informazioni aziendali. Gli Amministratori e collaboratori sono tenuti a fornire all'Organismo le informazioni richieste.

Per l'esercizio dei propri poteri, all'Organismo sono assegnati autonomi poteri di spesa e risorse finanziarie. A tal fine, l'Organismo indica annualmente al Presidente del Consiglio di Amministrazione un budget di spesa necessario allo svolgimento dei compiti assegnati, affinché egli provveda a dotare l'Organismo delle risorse necessarie.

Al verificarsi di circostanze impreviste, che rendano necessario un incremento del budget originariamente indicato, l'Organismo provvede a segnalarle al Presidente del Consiglio di Amministrazione – unitamente alle ragioni che rendono necessario l'adeguamento – affinché egli assegni all'O.d.V. risorse finanziarie integrative.

Al fine di coadiuvare l'attività dell'Organismo, è istituita una Segreteria tecnica dell'O.d.V., che provvederà a svolgere le attività di supporto tecnico e di segreteria. L'attività di segreteria dell'O.d.V. è assegnata alla Funzione Internal Audit, la quale provvederà ad ogni adempimento necessario al fine di poter dare concreta attuazione a quanto previsto dal presente Modello in capo a tale organismo.

4.5. Flussi informativi verso L'Organismo di Vigilanza

L'art. 6, comma 2 lett. d) del Decreto richiede che il Modello preveda "obblighi di informazione" nei confronti dell'Organismo di Vigilanza, allo scopo di garantire l'effettività e l'efficacia dell'attività vigilanza svolta dall'O.d.V. sul funzionamento e l'osservanza del Modello.

In attuazione di questi principi, il presente Modello prevede un sistema di flussi informativi strutturati verso l'Organismo di Vigilanza. Le informazioni che devono essere veicolate

all'O.d.V. mirano a rendere più efficace le sue attività di vigilanza e la pianificazione dei controlli, consentendo una verifica sistematica di tutte le aree di attività aziendali.

In linea generale, l'Organismo di Vigilanza deve essere informato di ogni circostanza rilevante e di ogni dato utile per l'esercizio dell'attività di vigilanza.

In particolare, all'Organismo di Vigilanza devono essere trasmesse su base periodica le informazioni, i dati e le notizie concordate con l'O.d.V. (avvalendosi eventualmente di schemi e prospetto riepilogativi definiti d'intesa con l'Organismo), nonché ogni altra informazione rilevanti per l'esercizio dell'attività di vigilanza o per l'applicazione del Modello nelle aree di attività a rischio.

Al fine di assicurare un proficuo e reciproco scambio di informazioni sono, inoltre, previsti incontri con cadenza periodica (almeno annuale) dell'Organismo di Vigilanza con il Data Protection Officer ed il Compliance Officer Antitrust.

Inoltre, indipendentemente dalla (e ad integrazione della) informazione periodica di cui sopra, devono essere tempestivamente trasmesse all'O.d.V. le informazioni concernenti procedimenti disciplinari azionati per violazioni del Modello, dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, dell'applicazione di una sanzione per violazione del Modello o delle procedure stabilite per la sua attuazione; nonché dei provvedimenti e/o delle notizione provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di attività d'indagine per i reati di cui al Decreto 231/2001, avviate anche nei confronti di ignoti.

Il Sindaco unico, il Data Protection Officer ed il Compliance Officer Antitrust comunicano, inoltre, senza ritardo all'Organismo di Vigilanza eventuali carenze organizzative e/o violazioni riscontrate nell'esercizio delle loro funzioni, che integrino o possano integrare una violazione del presente Modello o espongano la Società al rischio di commissione di uno o più dei reati presupposto previsti dal D. Lgs. 231/2001.

Inoltre, in attuazione di quanto previsto dall'art. 6 del Decreto e del D. Lgs. 24/2023, sono stati istituiti specifici canali di segnalazione interna (anche anonima) verso l'Organismo di Vigilanza, per la segnalazione della ritenuta commissione di reati di cui al D. Lgs. 231/2001, nonché di ogni ritenuta violazione del Codice Etico (c.d. segnalazioni Whistleblowing). Sul punto si rinvia al paragrafo 4.7.

4.6. Flussi informativi dall'Organismo di Vigilanza verso la Società

L'Organismo di Vigilanza riferisce al Consiglio di Amministrazione in merito all'attuazione del Modello, alle eventuali criticità riscontrate ed agli interventi correttivi necessari, nonché in merito all'eventuale aggiornamento del Modello. In particolare, sono previsti sia flussi informativi periodici, che ad evento.

Informativa periodica

L'Organismo di Vigilanza predispone e trasmette periodicamente (con periodicità almeno semestrale) al Consiglio di Amministrazione ed al Sindaco unico una Relazione scritta, riepilogativa dell'attività svolta nel periodo di riferimento.

La Relazione è sottoscritta dall'Organismo di Vigilanza e deve contenere almeno i seguenti elementi:

- la sintesi delle attività e dei controlli svolti dall'O.d.V.;
- eventuali problematiche sorte riguardo alle procedure operative di attuazione delle disposizioni del Modello;
- eventuali nuove attività nell'ambito delle quali può essere commesso uno dei reati previsti dal Decreto;
- il resoconto delle segnalazioni ricevute da soggetti interni ed esterni in ordine a presunte violazioni del Modello e l'esito delle verifiche su dette segnalazioni;
- le procedure disciplinari e le sanzioni eventualmente applicate dalla Società, per violazioni al Modello o commesse con riferimento alle attività a rischio;
- una valutazione complessiva sul funzionamento e l'efficacia del Modello con eventuali proposte di integrazioni, correzioni o modifiche;
- eventuali mutamenti del quadro normativo che richiedano un aggiornamento del Modello;
- la sintesi dei fatti rilevanti e delle modifiche di carattere significativo apportate al Modello delle società appartenenti al Gruppo;
- un rendiconto delle spese sostenute

L'Organismo di Vigilanza, inoltre, incontra periodicamente il Sindaco unico, per un reciproco scambio di informazioni, nonché per riferire in merito all'attività svolta ed ai relativi esiti ed alle eventuali carenze riscontrate ed alle attività di vigilanza previste nel successivo periodo di

riferimento. Gli incontri con il Sindaco unico vengono verbalizzati a cura dell'Organismo ed i relativi verbali sono conservati presso la Segreteria tecnica dell'O.d.V.

L'Organismo di Vigilanza può, inoltre, essere convocato in qualsiasi momento dal Consiglio di Amministrazione e potrà a sua volta presentare richiesta in tal senso, al fine di riferire in merito al funzionamento del Modello ed a situazioni specifiche, direttamente o indirettamente inerenti al funzionamento o l'osservanza del Modello e/o l'attuazione del D. Lgs. 231/2001.

L'Organismo di Vigilanza dà, inoltre, informativa al Data Protection Officer o al Compliance Officer Antitrust – nel rispetto degli obblighi di riservatezza previsti dal presente Modello e dalla normativa vigente – di ogni di ogni eventuale violazione del presente Modello di cui abbia avuto o acquisito notizia nell'esercizio delle sue funzioni, che possa integrare anche una violazione della vigente normativa privacy o della normativa antitrust.

Informativa ad evento

In ogni caso, l'O.d.V. riferisce senza ritardo al Consiglio di Amministrazione dell'avvenuta commissione (da parte di uno dei soggetti di cui all'art. 5 del Decreto) di un reato presupposto o di eventuali violazioni significative del Modello e delle segnalazioni ricevute, che rivestano carattere d'urgenza.

Inoltre, l'Organismo riferisce al Consiglio di Amministrazione ed al Sindaco unico ogniqualvolta lo ritenga opportuno, in ordine a circostanze e fatti – accertati o di cui abbia avuto conoscenza nell'esercizio delle sue funzioni – rilevanti per il funzionamento e l'osservanza del Modello.

4.7. Whistleblowing

Ai sensi dell'art. 6 comma 2-*bis* del Decreto, i Modelli di organizzazione – ai sensi del D. Lgs. 10.3.2023 n. 24 attuativo della c.d. Direttiva Whistleblowing – devono prevedere specifici canali di segnalazione interna per le segnalazioni *whistleblowing*, che garantiscano la riservatezza dell'identità della persona segnalante (nonché della persona coinvolta e della persona comunque menzionata nella segnalazione e del contenuto della segnalazione), il divieto di ritorsione e un sistema disciplinare, conforme a quanto previsto dal D.lgs. 24/2023.

In conformità alle disposizioni del Decreto e del D. Lgs. 24/2023, sono stati istituiti specifici canali interni di segnalazione, che consentono di veicolare all'Organismo di Vigilanza le segnalazioni, assicurando la tutela dell'identità del segnalante (nonché della persona coinvolta e della persona menzionata nella segnalazione) e del contenuto della segnalazione.

In particolare, sono stati messi a disposizione dei soggetti che intendano effettuare una segnalazione diversi canali per le segnalazioni all'O.d.V.:

a) un portale per le segnalazioni – anche in forma anonima – *whistleblowing*, tramite link dedicato (segnalazione-whistleblowing@gruppoapi.com) disponibile sul sito www.gruppoapi.com ;

b) un indirizzo specifico ove possono essere indirizzate segnalazioni in forma cartacea all'Organismo di Vigilanza ("C.E.R. S.r.l. via Salaria 1322, 00138 Roma");

c) una segreteria telefonica contattabile al numero pubblicato sul sito istituzionale, che rende possibile effettuare segnalazioni (anche anonime) in forma orale.

La Società, partendo da una lettura combinata di diversi pacchetti normativi, ha adottato un protocollo di whistleblowing dall'utilità multipla e amplificata, perché progettato conformemente al D.lgs. 231/2001, al D. Lgs. 24/2023, alle indicazioni del Garante privacy ed alle Linee guida sulla compliance antitrust emanate dall'Autorità Garante per la Concorrenza ed il Mercato.

La soluzione è originale e creativa: invece di duplicare gli strumenti organizzativi, C.E.R. S.r.l. ha ritenuto di implementare una soluzione che, realizzando una lettura simmetrica ed integrata di quanto richiesto del legislatore, adotta un unico applicativo, di ultima generazione sotto il profilo informatico, progettato in ottica *multicompliant*.

La soluzione si caratterizza per il contesto di dialogo segregato con il potenziale whistleblower, che può segnalare in forma scritta attraverso l'applicativo o esporre oralmente (attraverso un numero telefonico dedicato) il presunto reato o la ritenuta violazione, anche mantenendo l'anonimato. L'applicativo è corredato da formulari progettati ad hoc e profilati sulla base del contesto di riferimento del comportamento denunciato (D. Lgs. 231/2001, D. Lgs. 24/2023, normativa a tutela della concorrenza e/o del consumatore) al fine di guidare il whistleblower ad un'esposizione mirata, che escluda eccessi narrativi non pertinenti rispetto al fatto narrato.

In alternativa ai canali precedentemente indicati, inoltre, il segnalante può avvalersi anche dell'email riservata dell'Organismo di Vigilanza (odvcer@gruppoapi.com) e potrà richiedere di effettuare la segnalazione anche mediante incontro diretto con il membro dell'O.d.V., attraverso comunicazione scritta o orale, ovvero mediante richiesta inviata all'indirizzo e-mail dell'Organismo di Vigilanza.

Le modalità di segnalazione (comprensive del link della piattaforma e degli altri recapiti ove possono essere indirizzate) e le condotte che potrebbero esserne oggetto sono pubblicati sul sito del gruppo www.gruppoapi.com (nella sezione Governance – Whistleblowing).

Le istruttorie delle segnalazioni rilevanti alla luce del D. Lgs. 231/2001 e D.lgs. 24/2023 sono rimesse all'Organismo di Vigilanza, mentre quelle a rilevanza Antitrust rimesse alla valutazione del Compliance Officer Antitrust, che segue la società in service.

C.E.R. S.r.l. ha adottato un protocollo per la "*Gestione Segnalazioni*" (predisposto dalla controllante ed applicabile a tutte le società del Gruppo) nelle quali sono descritte le modalità di ricezione delle segnalazioni, alla loro gestione, alle tutele garantite al segnalante (ed agli altri soggetti indicati nel D. Lgs. 24/2023) ed alle misure che in caso di segnalazioni in mala fede.

Al fine di garantire l'efficacia del sistema di gestione delle segnalazioni in ottemperanza a quanto previsto dal D. Lgs. 24/2023, è vietata qualsiasi forma (diretta o indiretta) di ritorsione o discriminazione o penalizzazione nei confronti del segnalante (nonché degli altri soggetti cui si estende la protezione, di cui all'art. 2 del D. Lgs. 24/2023).

L'Organismo, allorché abbia ricevuto una segnalazione nominativa – o dalla quale sia comunque possibile dedurre univocamente l'identità del segnalante – vigila affinché non siano applicate a quest'ultimo (ovvero agli altri soggetti cui si estende la protezione accordata al segnalante) misure ritorsive, per tali intendendosi quelle indicate all'art. 17 del D. Lgs. 24/2023.

L'adozione di misure discriminatorie nei confronti del segnalante in buona fede può essere altresì comunicata all'Autorità Nazionale Anticorruzione (ANAC) o denunciata all'Ispettorato Nazionale del Lavoro, per i provvedimenti di competenza, dal segnalante stesso o dalle organizzazioni sindacali.

Le misure ritorsive o discriminatorie adottate nei confronti del segnalante (o degli altri soggetti cui si estende la protezione) sono nulle. Si provvederà all'applicazione di congrue sanzioni a carico di coloro che si rendessero responsabili di comportamenti ritorsivi o discriminatori a carico degli autori di segnalazioni (o di altri soggetti cui si estende la protezione accodata al segnalante, ai sensi del D. Lgs. 24/2023).

Ai sensi del D. Lgs. 24/2023, la tutela del segnalante non è garantita nel caso di segnalazioni effettuate con dolo o colpa grave, che si rivelino infondate. Salva l'applicazione delle eventuali sanzioni penali, si provvederà all'applicazione di congrue sanzioni a carico di coloro che abbiano

effettuato segnalazioni false o infondate sulla commissione di illeciti e/o violazioni del Modello di Organizzazione, Gestione e Controllo.

Per il sistema disciplinare adottato si rinvia al successivo paragrafo 5.

5. SISTEMA DISCIPLINARE E SANZIONATORIO

Gli artt. 6, comma 2 e 7, comma 4 del Decreto richiedono – per l'efficace attuazione del Modello – che l'ente provveda ad introdurre un adeguato sistema disciplinare "*idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*".

C.E.R. S.r.l. ha previsto un sistema autonomo di sanzioni disciplinari, finalizzato a rafforzare l'osservanza e l'efficace attuazione del Modello, destinato a colpire le violazioni del Modello e del Codice Etico. L'applicazione delle misure sanzionatorie previste dal Modello non sostituisce eventuali sanzioni di diversa natura (penale, civile o amministrativa), che possano derivare dalla medesima violazione.

Le sanzioni previste dal Modello, inoltre, saranno applicate in riferimento ad ogni violazione – debitamente accertata – delle disposizioni contenute nel Modello, a prescindere dalla commissione di un reato e dall'instaurazione (e dall'esito) di un eventuale procedimento penale conseguente alla sua realizzazione.

5.1. Destinatari

Sono tenuti all'osservanza del Modello e del Codice Etico e destinatari del presente sistema disciplinare e sanzionatorio:

a) i soggetti che rivestono funzioni di rappresentanza, di amministrazione e direzione della Società (quali amministratori muniti di poteri di particolare ampiezza);

b) i soggetti che svolgano attività per conto e/o nell'interesse della Società, i consulenti, i lavoratori autonomi che collaborino con C.E.R. S.r.l., i partners commerciali e finanziari, i fornitori e, più in genere, tutti coloro che svolgano qualsivoglia prestazione per conto e/o nell'interesse della Società;

c) il Sindaco unico e lo stesso Organismo di Vigilanza.

5.2. Violazioni del Modello di organizzazione

Salvo quanto di seguito esposto con riferimento alle misure adottabili nei confronti delle diverse tipologie di Destinatari del sistema disciplinare, integrano in ogni caso una violazione del Modello le seguenti classi di condotte:

- la realizzazione di azioni o comportamenti contrari o, comunque, non conformi alle prescrizioni del Modello o agli standard di controllo ivi previsti, ovvero l'omissione di azioni

o comportamenti prescritti dal Modello, che possano esporre la Società a contestazioni ai sensi del D. Lgs. 231/2001;

- l'inosservanza – nell'espletamento di attività a rischio – dei presidi di controllo e degli strumenti normativi aziendali di riferimento nei quali sono declinati;
- l'inosservanza degli obblighi di informazione nei confronti dell'Organismo di Vigilanza previsti dal Modello, allorché espongano la Società a una situazione oggettiva di rischio di commissione di uno dei reati contemplati dal Decreto, ovvero siano diretti in modo univoco al compimento di uno (o più) dei reati contemplati dal Decreto;
- l'ostacolo all'attività di vigilanza dell'O.d.V., anche attraverso la mancata, incompleta o non veritiera rappresentazione dell'attività svolta nelle comunicazioni o nei report inviati all'Organismo di Vigilanza (o da questo richiesti), ovvero la falsità delle dichiarazioni e attestazioni eventualmente richieste dall'O.d.V. in merito al rispetto del Modello e del Codice Etico;
- la violazione e/o elusione del sistema di controllo poste in essere mediante la sottrazione, la distruzione o alterazione della documentazione, ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti al controllo, ivi incluso l'Organismo di Vigilanza;
- l'omessa segnalazione della commissione di un reato presupposto o di una violazione del Modello commessa da uno dei Destinatari;
- la volontaria mancata partecipazione alle attività di formazione riguardanti il Modello, nonostante l'invito reiteratamente rivolto al Destinatario.

Costituisce, altresì, violazione del Modello – cui consegue l'applicazione delle sanzioni ivi previste – la violazione degli obblighi di riservatezza e tutela dell'identità del segnalante previsti dal D. Lgs. 24/2023, l'adozione di misure ritorsive, discriminatorie o comunque penalizzanti per il segnalante (o per gli altri soggetti cui si estende la protezione accordata al segnalante), nonché l'avere effettuato con dolo o colpa grave segnalazioni false o infondate.

Le sanzioni contemplate per la violazione di disposizioni contenute nel Modello sono applicabili anche alla violazione del Codice Etico, nonché alla violazione delle Linee Guida Anticorruzione, alla violazione delle Linee Guida e della normativa Antitrust ed alla violazione delle norme vigenti in materia di protezione dei dati personali e del Modello privacy.

5.3. Sanzioni e criteri di applicazione

Le sanzioni applicabili dovranno essere diversificate in ragione della natura del rapporto tra l'autore della violazione e la Società, nonché del rilievo e della gravità della violazione e del grado di responsabilità dell'autore.

A tal fine, potranno assumere rilievo elementi sia di natura oggettiva, che soggettiva, quali:

- la tipologia della violazione contestata e le circostanze in cui è stata commessa;
- le modalità di commissione della condotta e la natura e rilevanza degli obblighi violati;
- la reiterazione della condotta nel tempo o la commissione di più violazioni;
- il ruolo e le responsabilità dell'autore, le sue mansioni e grado di autonomia;
- la natura dolosa o colposa della condotta e le sue eventuali finalità;
- l'eventuale concorso di più soggetti nella commissione della violazione;
- l'eventuale recidività dell'autore.

In conformità agli orientamenti espressi dalla giurisprudenza (anche costituzionale) e dalle Linee Guida di Confindustria, l'esercizio del potere disciplinare dovrà, in ogni caso, conformarsi ai principi di:

- proporzionalità, commisurando la sanzione irrogata alla natura e gravità della violazione;
- contraddittorio, assicurando il coinvolgimento del soggetto interessato: formulata la contestazione (che dovrà essere tempestiva e specifica) dell'addebito, occorrerà assicurare all'incolpato la possibilità di controdedurre, a difesa del suo comportamento.

5.4. Misure nei confronti degli Amministratori, del Sindaco unico

Se la violazione riguarda un Amministratore della Società, l'Organismo di Vigilanza deve darne immediata comunicazione al Consiglio di Amministrazione e al Sindaco unico mediante relazione scritta, affinché vengano assunte o promosse le iniziative più opportune, in relazione alla natura e gravità della violazione riscontrata, in conformità a quanto previsto dalla legge e dallo Statuto sociale.

Se la violazione delle disposizioni del Modello è stata commessa dal Consiglio di Amministrazione nella sua interezza, l'Organismo di Vigilanza ne informa il Sindaco unico, affinché provveda a promuovere le conseguenti iniziative.

Analogamente, nel caso di violazione del Modello o del Codice Etico da parte del Sindaco unico, l'Organismo di Vigilanza deve darne immediata comunicazione al Consiglio di Amministrazione mediante relazione scritta, per le opportune valutazioni e l'adozione dei provvedimenti conseguenti.

Nei confronti degli Amministratori che abbiano commesso una violazione del Modello o del Codice Etico, il Consiglio di Amministrazione può applicare ogni idoneo provvedimento consentito dalla legge e dallo Statuto, avuto riguardo alla gravità del fatto, alla natura dolosa o colposa della violazione, nonché alle conseguenze che ne sono derivate alla Società, fra cui le seguenti sanzioni:

a) richiamo formale scritto che dovrà essere inserito nel verbale dell'adunanza del C.d.A.;
b) sanzione pecuniaria pari all'importo da due a cinque volte gli emolumenti calcolati su base mensile;
c) revoca, totale o parziale, delle eventuali deleghe conferite.

Nell'ipotesi in cui si ravvisino violazioni del Modello tali da compromettere il rapporto di fiducia con l'Amministratore responsabile della violazione, si procederà alla convocazione dell'Assemblea per deliberare in merito alla eventuale revoca della carica.

Le stesse disposizioni si applicano, in quanto compatibili, nel caso di violazioni del Modello commesse dal Sindaco unico.

L'eventuale revoca dalla carica di Amministratore o la revoca dalla carica di Sindaco unico per la responsabilità della violazione non precludono l'esercizio di azioni di responsabilità e/o risarcitorie, per l'accertamento della responsabilità dell'Amministratore e/o del Sindaco unico ed il risarcimento dei danni cagionati alla Società.

5.5. Misure nei confronti dei componenti dell'Organismo di Vigilanza

In conformità a quanto previsto al paragrafo 4.3, il Consiglio di Amministrazione, quando accerta la commissione da parte di un componente dell'Organismo di Vigilanza di una violazione delle prescrizioni del Modello o del Codice Etico, previa valutazione delle argomentazioni difensive e/o delle giustificazioni fornite dall'incolpato, provvede – se le ritiene infondate – alla sua revoca.

L'adozione del provvedimento di revoca non preclude l'esercizio nei suoi confronti di azione civile per il risarcimento dei danni che ne siano eventualmente derivati alla Società.

5.6. Misure nei confronti di soggetti esterni alla società (agenti, collaboratori, consulenti, lavoratori autonomi, partners)

Per i soggetti esterni alla Società destinatari del Modello (come indicati al par. 5.1) e tenuti alla sua osservanza, l'Organismo di Vigilanza svolge – con il supporto delle funzioni competenti e del Responsabile dell'area alla quale il contratto o rapporto si riferiscono – gli opportuni accertamenti, all'esito dei quali, se accerta una violazione del Modello o del Codice Etico, propone l'applicazione delle opportune sanzioni.

In particolare, avuto riguardo a quanto previsto nel contratto che regola il contratto di *service* o il rapporto negoziale, potranno essere applicate ai soggetti esterne sanzioni, quali la diffida al puntuale rispetto del Modello e del Codice Etico, penali per la sua violazione o, nei casi più gravi, la risoluzione del contratto.

Resta, inoltre, salvo il diritto della Società di richiedere il risarcimento dei danni conseguenti alla violazione, da parte del terzo che si sia reso autore della violazione, delle disposizioni e delle regole di comportamento previste dal Modello e dal Codice Etico.

5.7. Procedimento di applicazione delle sanzioni

L'Organismo di Vigilanza provvede ad avviare le attività per l'accertamento e l'eventuale applicazione delle sanzioni conseguenti ad una violazione del Modello ogniqualvolta

a) riceva una segnalazione di potenziali violazioni del Modello, attraverso i canali informativi di cui ai paragrafi 4.5 e 4.7;

b) riscontri o accerti direttamente da parte dell'Organismo, nell'esercizio della propria attività di vigilanza e di verifica, una possibile violazione del Modello.

Ogni violazione del Modello, da chiunque commessa, deve essere immediatamente comunicata per iscritto, all'Organismo di Vigilanza. Il dovere di segnalazione grava su tutti i Destinatari del presente Modello.

Ricevuta la segnalazione, l'Organismo di Vigilanza deve dare corso ai necessari accertamenti nel rispetto delle modalità e delle tempistiche eventualmente previste dalla legge, garantendo la riservatezza del soggetto nei cui confronti procede.

5.7.1. Procedimento di applicazione per Amministratori, il Sindaco unico e dell'Organismo di Vigilanze

L'Organismo di Vigilanza, allorché accerti la violazione del Modello da parte di un Amministratore, trasmette al Consiglio di Amministrazione ed al Sindaco unico una relazione contenente la descrizione della condotta accertata e l'indicazione delle disposizioni del Modello che risultano violate; l'indicazione del soggetto responsabile della violazione e gli elementi acquisiti comprovanti la violazione.

Entro 15 giorni dall'acquisizione della relazione dell'Organismo, il Consiglio di Amministrazione convoca un'adunanza del Consiglio stesso, da tenersi non oltre 20 giorni dalla data della convocazione, per l'audizione dell'Amministratore cui venga attribuita la violazione del Modello.

La convocazione deve contenere l'indicazione della condotta contestata e delle previsioni del Modello oggetto di violazione e l'avviso all'Amministratore incolpato della violazione che egli ha facoltà di formulare eventuali rilievi e/o deduzioni, sia scritte che orali. All'Amministratore incolpato deve essere resa disponibile la relazione trasmessa dall'O.d.V.

In occasione dell'adunanza a cui è invitato a partecipare anche il Sindaco unico, si procede all'audizione dell'interessato, all'acquisizione delle eventuali deduzioni da quest'ultimo formulate e può disporre gli eventuali ulteriori accertamenti ritenuti opportuni.

Il Consiglio di Amministrazione può richiedere, se lo ritiene opportuno, che all'adunanza partecipi anche l'Organismo di Vigilanza.

Sulla base degli elementi acquisiti, il Consiglio di Amministrazione delibera – con l'astensione dell'Amministratore incolpato – le misure che ritiene opportune misure e l'eventuale applicazione delle sanzioni di cui al paragrafo 5.4., ovvero provvede a convocare l'Assemblea, per la revoca dell'Amministratore incolpato. Dei provvedimenti adottati, il Consiglio provvede a dare informazione all'O.d.V.

Qualora l'Amministratore incolpato della violazione del Modello sia legato alla Società da un rapporto di lavoro subordinato, nel procedimento sanzionatorio dovrà farsi applicazione delle disposizioni di cui all'art. 7 della Legge 300/1970 e del CCNL. Nel caso in cui, ad esito di tale procedimento, il Consiglio di Amministrazione ritenga di provvedere al licenziamento disciplinare dell'Amministratore incolpato, il C.d.A. dovrà convocare senza indugio l'Assemblea dei soci per deliberare la revoca dell'Amministratore dall'incarico.

Le disposizioni precedenti si applicano – in quanto compatibili – anche al procedimento per l'applicazione di sanzioni conseguenti alla violazione del Modello o del Codice Etico da parte del Collegio Sindacale, di un Componente dell'Organismo di Vigilanza o dei revisori della Società incaricata della revisione contabile.

5.7.2. Procedimento di applicazione per i soggetti esterni alla Società

L'Organismo di Vigilanza, allorché riscontri una violazione del Modello da parte di soggetti esterni alla Società, che ne siano destinatari (come definiti al par. 5.1), trasmette al Presidente del Consiglio di Amministrazione, una relazione contenente

- la descrizione della condotta accertata, l'indicazione delle disposizioni del Modello e del contratto che risultano violate,
- l'indicazione del soggetto responsabile della violazione e gli elementi acquisiti comprovanti la violazione
- e formula una proposta riguardante l'applicazione di eventuali sanzioni al soggetto esterno (destinatario del Modello), che si sia reso responsabile della violazione.

Il Presidente del Consiglio di Amministrazione invia all'interessato una comunicazione scritta, contenente l'indicazione della condotta accertata, le disposizioni del Modello e del contratto che risultano violate e lo invita a fornire le sue deduzioni e giustificazioni.
Degli esiti del procedimento e delle iniziative assunte, anche sul piano contrattuale, nei confronti del soggetto esterno alla Società autore della violazione del Modello è data comunicazione all'O.d.V.

6. PRINCIPI E VALORI ETICI E NORME GENERALI DI COMPORTAMENTO

Fatto salvo quanto previsto dal Codice Etico che esprime i principi e i valori che connotano la cultura d'impresa di tutte le Società del Gruppo, C.E.R. S.r.l. intende ribadire la sussistenza dell'obbligo per tutti gli esponenti aziendali di osservare scrupolosamente le regole di comportamento sotto enucleate. Dette regole hanno una funzione immediatamente precettiva e, per quanto ivi non espressamente normato, integrativa delle procedure interne richiamate nelle Parti Speciali del Modello.

C.E.R. S.r.l. non giustifica alcun comportamento che, seppure compiuto nel suo interesse e/o a suo vantaggio, contrasti con i principi e i valori del Codice Etico e con le regole di seguito esposte, con le procedure che disciplinano le attività aziendali e, in generale, con le previsioni del Modello. In ogni caso la violazione di dette regole determinerà la applicazione delle sanzioni disciplinari in conformità al CCNL e al presente Modello.

C.E.R. S.r.l. nei rapporti con i terzi, darà corso alla immediata risoluzione del contratto qualora gli stessi pongano in essere, nel corso, in ragione o in conseguenza del rapporto, comportamenti contrari alle regole, ai principi e ai valori cui si ispira nell'agire aziendale anche quando il partner o collaboratore ritenga di agire nell'interesse o a vantaggio di C.E.R. S.r.l.

6.1. Norme generali di comportamento nei rapporti con la Pubblica Amministrazione

C.E.R. S.r.l. esige che i propri esponenti tengano comportamenti corretti nei rapporti con la Pubblica Amministrazione. È quindi fatto divieto di praticare qualsivoglia forma di corruzione, favoritismi, comportamenti collusivi, sollecitazioni dirette e/o indirette anche attraverso promesse di vantaggi personali, nei confronti di qualunque soggetto appartenente alla Pubblica Amministrazione.

È fatto divieto di fornire alla Pubblica Amministrazione informazioni e/o documenti falsi o attestanti fatti o circostante non rispondenti al vero, ovvero omettere informazioni rilevanti.

6.2. Norme generali di comportamento nei rapporti commerciali

Nei rapporti commerciali con privati e Partner in genere, è vietato fornire informazioni e/o documenti non rispondenti al vero o che omettano notizie rilevanti secondo la natura dell'affare.

6.3. Norme generali di comportamento nella redazione dei documenti contabili

È fatto obbligo di redigere e tenere le scritture contabili in conformità alle previsioni normative. I bilanci devono contenere informazioni veritiere e corrette ed è fatto obbligo di rispettare i principi contabili. I rapporti con le Autorità Pubbliche di vigilanza, il sindaco unico o il Socio devono essere improntati a criteri di trasparenza, collaborazione e verità.

6.4. Conflitti di interesse

È fatto obbligo a tutti gli esponenti aziendali di rendere noto qualsiasi conflitto di interesse che sia sorto o possa sorgere in relazione ad uno o più affari. Le comunicazioni dovranno essere precise e indicare specificamente la natura, i termini e l'origine della situazione (anche solo potenziale) di conflitto di interesse e del vantaggio (o potenziale vantaggio) che l'esponente aziendale – anche indirettamente e per interposta persona – potrebbe trarne. In attesa delle valutazioni e decisioni societarie sul punto, gli interessati dovranno astenersi dal compiere qualsiasi operazione.

6.5. Tutela del capitale sociale e dei creditori

È vietato a tutti gli esponenti aziendali di compiere atti simulati o fraudolenti al fine di influenzare il Socio falsando il libero formarsi della volontà dell'assemblea in sede deliberante.

È vietato porre in essere condotte finalizzate alla realizzazione di operazioni illecite sulle azioni o quote sociali anche delle altre Società del gruppo.

È fatto divieto agli Amministratori di effettuare operazioni societarie o sul capitale, al fine di procurare un danno ai creditori.

6.6. Norme generali di comportamento nella gestione dei pagamenti

È fatto obbligo di rispettare la normativa vigente e le procedure interne in materia di pagamenti, utilizzo e circolazione di monete, carte di pubblico credito e valori di bollo. È fatto obbligo di garantire la tracciabilità di tutti i pagamenti.

I rapporti e le transazioni infragruppo devono essere adeguatamente regolamentati in forma scritta e i flussi di denaro da o verso altre Società del Gruppo devono essere tracciati e trovare giustificazione nei contratti e nei rapporti negoziali in essere.

6.7. Norme generali di comportamento per il contrasto al terrorismo

È vietata qualsiasi condotta idonea ad integrare atti di terrorismo o di eversione dell'ordinamento ovvero di finanziamento, diretto o indiretto, di associazioni aventi finalità di terrorismo o di eversione dell'ordine democratico.

6.8. Norme generali di comportamento per la salvaguardia dell'ambiente

La tutela dell'ambiente rappresenta uno dei valori primari della cultura d'impresa del Gruppo. È fatto, pertanto, obbligo a tutti gli esponenti aziendali di rispettare le previsioni normative in materia di tutela dell'ambiente e di operare al fine di evitare e di adottare ogni appropriata misura per ridurre l'impatto dell'attività aziendale sull'ambiente.

6.9. Norme generali di comportamento per la tutela della salute e della sicurezza nei luoghi di lavoro

La tutela della salute e della sicurezza nei luoghi di lavoro rappresenta un valore centrale nell'attività d'impresa di C.E.R. S.r.l. e del Gruppo. È fatto obbligo a tutti gli esponenti aziendali di rispettare le norme di legge e le procedure interne finalizzate a garantire la salute e la sicurezza nei luoghi di lavoro nel rispetto dei ruoli, delle mansioni e delle responsabilità a ciascuno assegnate nell'ambito delle misure organizzative adottate dalla Società per una efficace tutela dei lavoratori dai rischi che possano insorgere nello svolgimento delle loro attività.

6.10. Norme generali di comportamento nell'utilizzo delle tecnologie informatiche

È fatto obbligo di utilizzare le tecnologie informatiche e i dispositivi informatici forniti alla popolazione aziendale nel rispetto delle procedure che ne regolamentano gli usi e, comunque, esclusivamente per finalità lecite connesse allo svolgimento dell'attività lavorativa.

6.11. Norme generali di comportamento per il contrasto del riciclaggio

È fatto obbligo di rispettare la normativa e le procedure interne finalizzate alla prevenzione del riciclaggio. Sono vietate le condotte che direttamente o indirettamente possano integrare forme di collaborazione con associazioni criminose in genere e di stampo mafioso. È inoltre vietata ogni operazione che possa concretizzarsi in un utilizzo di denaro, beni o utilità di provenienza illecita nonché qualunque attività e/o forma di riciclaggio.

6.12. Norme generali di comportamento nei rapporti con l'Autorità giudiziaria

È vietato qualunque comportamento che possa rivelarsi di intralcio alla giustizia. I rapporti con l'Autorità Giudiziaria devono essere improntati a criteri di collaborazione, verità e trasparenza.

6.13. Tutela della concorrenza e dei consumatori

È fatto obbligo di gestire gli affari e le operazioni societarie nel rispetto della normativa e delle procedure interne a tutela della libertà di concorrenza, del consumatore e del diritto d'autore.

6.14. Tutela della privacy e della riservatezza

È fatto obbligo di rispettare la normativa e le procedure interne a tutela del diritto alla privacy e alla riservatezza. Le informazioni e i dati anche di carattere non personale devono essere trattati dalle persone a ciò autorizzate nel rispetto della suddetta normativa.

ALLEGATI

1) Elenco dei reati per i quali il D.Lgs 8.6.2001 n. 231 prevede la responsabilità dell'ente;
2) Mappatura delle aree a rischio;
3) Codice Etico di gruppo.
4) Statuto dell'Organismo di Vigilanza