

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del D. Lgs. 8 giugno 2001 n. 231 e successive modifiche e integrazioni



**approvato per la prima volta con delibera del Consiglio di Amministrazione del 11/07/2019
Rev. 6 del 16/09/2026**

INPOWER GROUP S.C.P.A.
CONSORZIO
STABILE

A handwritten signature in black ink, appearing to be "M. S.", is written over the text "CONSORZIO STABILE".

Sommario

Il Codice Etico di INPOWER GROUP – CONSORZIO STABILE S.C.P.A.

PARTE GENERALE

PARTE SPECIALE

Parte speciale A – Reati contro la Pubblica Amministrazione e ai danni dello Stato

Parte speciale B – Reati societari

Parte speciale C – Reati contro la personalità individuale

Parte speciale D – Reati in materia di salute e sicurezza sui luoghi di lavoro

Parte speciale E – Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza
Illecita e autoriciclaggio

Parte speciale F – Reati informatici e trattamento illecito di dati

Parte speciale G – Reati contro l'industria e il commercio

Parte speciale H – Reati di criminalità organizzata e reati transnazionali

Parte speciale I – Reati ambientali

Parte speciale J – Reati in materia di violazione del diritto d'autore

Parte speciale K – Reati tributari

Parte speciale L – Reati di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria

Parte Speciale M – Reati contro le fede pubblica

Parte Speciale N – Reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Parte Speciale O – Reati in materia di violazione Misure Restrittive UE

Parte Speciale P - Reati contro Patrimonio Culturale

Attività Sensibili

ALLEGATI

Allegato 1 – Sistema sanzionatorio

Allegato 2 – Struttura organizzativa e sistema di deleghe e poteri

Allegato 3 - Organigramma

Altri allegati – Procedure adottate

Altri allegati – *Risk assessment*

PARTE GENERALE

1. IL QUADRO NORMATIVO

In data 4 luglio 2001 è entrato in vigore il decreto legislativo 8 giugno 2001 n. 231 (di seguito: “D.Lgs. 231/01” o anche “Decreto”) il quale ha introdotto la disciplina della responsabilità delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica per i reati commessi nel loro interesse o vantaggio da coloro che rivestono funzioni di rappresentanza, di amministrazione o di direzione (cosiddetti “apicali” quali, a titolo esemplificativo, amministratori, procuratori, direttori generali) ma anche da coloro che sono sottoposti alla direzione e alla vigilanza dei primi (a titolo esemplificativo dipendenti, collaboratori, consulenti, etc.).

Tale forma di responsabilità amministrativa è equiparabile di fatto alla responsabilità penale, poiché viene accertata nell’ambito di un processo penale (art. 36 D. Lgs. 231/01) a seguito dell’iniziativa del Pubblico Ministero (artt. 55 e 56 D. Lgs 231/01). La responsabilità amministrativa della Società va ad aggiungersi alla responsabilità della persona fisica che ha materialmente commesso determinati reati nell’interesse o vantaggio dell’ente (c.d. reati presupposto).

L’accertamento potrà avere due conclusioni:

- a. l’illecito amministrativo contestato all’ente non sussiste, o la prova è insufficiente o contraddittoria, il giudice lo dichiara con sentenza, indicandone la causa nel dispositivo (art. 66 D.Lgs. 231/2001);
- b. se invece l’ente risulta responsabile dell’illecito amministrativo contestato (i presupposti di responsabilità, oggettivi e soggettivi, sono stati accertati), il giudice applica le sanzioni previste dalla legge, di cui si dirà di più nei paragrafi successivi, e lo condanna al pagamento delle spese processuali (art. 69 D.Lgs. 231/2001).

Ai sensi dell’art. 4 D. Lgs. 231/01 tale forma di responsabilità si configura anche in relazione a **reati commessi all’estero**, nei casi ed alle condizioni previste dagli artt. 7,8,9,10 c.p., a condizione che il reato sia commesso da un soggetto funzionalmente legato all’ente, che la società abbia la propria sede principale nel territorio dello Stato italiano e che nei suoi confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

Giova, altresì, ricordare che la responsabilità dell’ente sussiste anche se l’autore del reato non è stato identificato o il reato sia estinto nei confronti del reo per una causa diversa dall’amnistia o dalla prescrizione.

1.1. I criteri di imputazione della responsabilità

I presupposti oggettivi della responsabilità dell’ente si articolano nei seguenti elementi:

- a) la realizzazione di una fattispecie di reato rientrante tra quelle espressamente previste dal D.Lgs. 231/2001, come individuate dagli artt. 24 e seguenti fino all’art. 25-quinquiesdecies e ulteriori disposizioni integrative (c.d. reati presupposto);
- b) la commissione del reato nell’interesse o a vantaggio dell’ente;

- c) la commissione del fatto di reato da parte di uno o più soggetti qualificati, ossia soggetti apicali ovvero soggetti sottoposti alla direzione o vigilanza di questi ultimi.

Il primo presupposto fondamentale della fattispecie normativa della responsabilità delle Società consiste quindi nella commissione dei reati previsti dal D.Lgs. 231/01.

I reati presupposto:

Il primo presupposto fondamentale della responsabilità dell'ente consiste, dunque, nella commissione di uno dei reati presupposto espressamente previsti dal D.Lgs. 231/2001. I reati dai quali può derivare la responsabilità amministrativa dell'ente sono quelli espressamente e tassativamente indicati dal Decreto (principio di legalità)

In particolare, la responsabilità dell'ente può conseguire alla commissione di uno dei seguenti riconducibili alle diverse categorie di reato previste dal D.Lgs. 231/2001:

- Art. 24 - Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico;
- Art. 24-bis - Delitti informatici e trattamento illecito di dati;
- Art. 24-ter - Delitti di criminalità organizzata;
- Art. 25 - Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità e corruzione;
- Art. 25-bis - Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;
- Art. 25-bis.1 - Delitti contro l'industria e il commercio;
- Art. 25-ter - Reati societari;
- Art. 25-quater - Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali;
- Art. 25-quater.1 - Pratiche di mutilazione degli organi genitali femminili;
- Art. 25-quinquies - Delitti contro la personalità individuale (ivi incluso il delitto di intermediazione illecita e sfruttamento del lavoro ex art. 603-bis c.p., c.d. caporalato);
- Art. 25-sexies - Abusi di mercato;
- Art. 25-septies - Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme a tutela della salute e sicurezza sul lavoro;
- Art. 25-octies - Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;
- Art. 25-octies.1 - Reati in materia di mezzi di pagamento diversi dai contanti;
- Art. 25-octies.2 - Reati in materia di violazione di misure restrittive dell'Unione europea;
- Art. 25-novies - Delitti in materia di violazione del diritto d'autore;
- Art. 25-decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- Art. 25-duodecies - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
- Art. 25-terdecies - Razzismo e xenofobia;
- Art. 25-quaterdecies - Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati;
- Art. 25-undecies - Reati ambientali;
- Art. 25-quinquiesdecies - Reati tributari;
- Art. 25-sexiesdecies - Delitto di contrabbando;
- Art. 25-septiesdecies - Delitti contro il patrimonio culturale;

- Art. 25-duodevices - Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggisti;
- Art. 25-undevices - Delitti contro gli animali;
- Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013) [Costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva].

Si precisa che non tutte le famiglie di reato risultano potenzialmente incidenti sulle attività aziendali di Inpower Group.

Interesse e/o vantaggio

Il secondo presupposto oggettivo della responsabilità dell'ente è rappresentato dalla commissione del reato nell'interesse o a vantaggio dell'ente, secondo i criteri alternativi e non cumulativi delineati dall'art. 5 del D.Lgs. 231/2001.

Il criterio dell'**interesse** attiene alla dimensione finalistico-soggettiva della condotta e richiede una valutazione ex ante, consistente nella verifica della idoneità della stessa a perseguire, anche solo in via potenziale, un'utilità per l'ente, a prescindere dal concreto conseguimento del risultato.

Il criterio del **vantaggio**, di contro, si configura secondo una valutazione ex post e postula l'effettiva produzione di un beneficio in capo all'ente, anche non immediatamente patrimoniale, quale conseguenza causale della realizzazione del reato.

I due criteri, pur ontologicamente distinti, sono tra loro alternativi e non cumulativi, essendo sufficiente la ricorrenza anche di uno solo di essi ai fini dell'integrazione del presupposto di imputazione oggettiva della responsabilità dell'ente. Resta fermo che la loro eventuale compresenza costituisce elemento rafforzativo dell'addebitabilità della responsabilità medesima.

Interesse e/o vantaggio nei reati colposi

L'introduzione dell'art. 25-septies del D.Lgs. 231/2001, relativo ai reati colposi in materia di salute e sicurezza sui luoghi di lavoro, introdotto dalla legge 3 agosto 2007, n. 123 e successive modifiche e integrazioni, ha tuttavia posto in rilievo la centralità del tema relativo alla compatibilità tra la natura colposa del reato e i criteri di imputazione dell'ente fondati sull'interesse o sul vantaggio.

Sul punto, la giurisprudenza ha chiarito che, anche con riferimento ai reati colposi, la responsabilità dell'ente può configurarsi allorché la condotta omissiva o commissiva, violativa di norme cautelari poste a tutela della salute e sicurezza sul lavoro, si traduca in un risparmio di costi o di risorse organizzative, suscettibile di essere qualificato ex post quale vantaggio per l'ente. In tale prospettiva, si pensi, a titolo esemplificativo, alla mancata fornitura di dispositivi di protezione individuale ovvero all'omessa manutenzione o revisione di attrezzature aziendali, ove determinate da esigenze di contenimento dei costi.

Autori del reato: soggetti apicali e sottoposti

In forza dell'art. 5 del D.Lgs. 231/2001 l'illecito penale deve essere stato realizzato da uno o più soggetti qualificati, ovvero:

- da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale» o da coloro che «esercitano, anche di fatto, la gestione e il controllo dell'ente (soggetti in c.d. «posizione apicale»);
- o da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali di cui alla lettera a) (c.d. «sottoposti»).

Qualora più soggetti partecipino alla commissione del reato (ipotesi di concorso di persone nel reato ex art. 110 c.p.), non è necessario che il soggetto “qualificato” ponga in essere l’azione tipica prevista dalla legge penale. È sufficiente che fornisca un contributo consapevolmente causale alla realizzazione del reato.

La colpa di organizzazione

La colpa di organizzazione costituisce il criterio soggettivo di imputazione della responsabilità dell’ente ai sensi del D.Lgs. 231/2001 ed è il vero fulcro sistematico dell’intero modello di responsabilità amministrativa.

Sul piano dogmatico, essa non coincide con la colpa in senso penalistico riferibile alla persona fisica, ma si configura come rimproverabilità dell’ente per inadeguatezza del proprio assetto organizzativo, gestionale e di controllo, rispetto all’esigenza di prevenire la commissione dei reati presupposto.

In altri termini, la responsabilità dell’ente non discende automaticamente dalla commissione del reato da parte del soggetto apicale o subordinato, ma presuppone che tale fatto sia reso possibile da una carenza organizzativa imputabile all’ente stesso, consistente nella mancata adozione ovvero nell’inefficace attuazione di modelli idonei a prevenire reati della specie di quello verificatosi.

La colpa di organizzazione si sostanzia, quindi, nella violazione del dovere di auto-organizzazione efficiente e conforme ai principi di prevenzione del rischio-reato, che trova espressione nella mancata predisposizione o nell’inadeguata attuazione del Modello di Organizzazione, Gestione e Controllo ex artt. 6 e 7 del D.Lgs. 231/2001.

Ne consegue che il Modello 231 assume una funzione non meramente formale, ma sostanziale di criterio esimente della responsabilità dell’ente, laddove risulti idoneo ed efficacemente attuato prima della commissione del reato, e costantemente vigilato attraverso un organismo dotato di autonomi poteri di controllo.

In tale prospettiva, la colpa di organizzazione rappresenta il necessario elemento di collegamento tra il fatto-reato della persona fisica e l’imputazione all’ente, qualificando la responsabilità 231 come una responsabilità autonoma, fondata su un deficit organizzativo prevenzionistico.

1.3. Le sanzioni

L’art. 9 D. Lgs. 231/01 prevede l’irrogazione di sanzioni in caso di accertata responsabilità dell’ente. Il catalogo sanzionatorio è così strutturato:

a. sanzioni amministrative pecuniarie, sempre irrogate dall’autorità giudiziaria in caso di accertata responsabilità dell’ente. Calcolate in quote, di numero non inferiore a 100 né superiore a 1000, con un importo unitario della quota oscillante tra euro 258,23 ed euro 1.549,37. Il giudice determina la sanzione pecuniaria tenendo conto della gravità del fatto, del grado di responsabilità della Società, nonché dell’attività svolta da questa per eliminare o attenuare le conseguenze del fatto e/o per prevenire la commissione di ulteriori illeciti.

Le sanzioni pecuniarie sono ridotte nel caso in cui:

- l’autore del reato abbia commesso il fatto nel prevalente interesse proprio o di terzi e la società non ne abbia ricavato vantaggio o ne abbia ricavato vantaggio minimo;
- il danno patrimoniale cagionato è di particolare tenuità;
- la società ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;

- la società abbia adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

b. **sanzioni interdittive**, si applicano solo in relazione ai reati per i quali espressamente previsto, nonché in presenza delle seguenti circostanze:

- la società ha tratto dal reato commesso da un apicale/subordinato un profitto di rilevante entità e la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; 2 in caso di reiterazione degli illeciti.

Le sanzioni interdittive sono le seguenti:

- interdizione dall'esercizio dell'attività;
- sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- divieto di contrattare con la pubblica amministrazione;
- esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

c. **confisca del prezzo o profitto del reato**. Nei confronti dell'ente è sempre disposta, con la sentenza di condanna, la confisca del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato. Sono fatti salvi i diritti acquisiti dai terzi in buona fede.

La confisca si può concretizzare anche per "equivalente", vale a dire che laddove la confisca non possa essere disposta in relazione al prezzo o al profitto del reato, la stessa potrà avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

d. **pubblicazione della sentenza** di condanna può essere disposta quando nei confronti della Società viene applicata una sanzione interdittiva.

Qualora sussistano i presupposti per l'applicazione di una sanzione interdittiva che determina l'interruzione dell'attività della società, il giudice, in luogo dell'applicazione della sanzione, dispone la prosecuzione dell'attività della società da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni: a) la società svolge un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività; b) l'interruzione dell'attività della società può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

Il profitto derivante dalla prosecuzione dell'attività viene confiscato.

Le sanzioni interdittive possono essere applicate anche in via definitiva.

L'interdizione definitiva dall'esercizio dell'attività può essere disposta se la società ha tratto dal reato un profitto di rilevante entità ed è già stata condannata, almeno tre volte negli ultimi sette anni, alla interdizione temporanea dall'esercizio dell'attività.

Il giudice può applicare alla società, in via definitiva, la sanzione del divieto di contrattare con la Pubblica Amministrazione ovvero del divieto di pubblicizzare beni o servizi quando è già stata condannata alla stessa sanzione almeno tre volte negli ultimi sette anni.

Se la società o una sua unità organizzativa viene stabilmente utilizzata allo scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità è sempre disposta l'interdizione definitiva dall'esercizio dell'attività.

1.4. Le misure cautelari interdittive e reali

Nei confronti della società sottoposta a procedimento può essere applicata, in via cautelare, una misura cautelare interdittiva o reale.

Le misure cautelari interdittive – che consistono nell'applicazione temporanea di una sanzione interdittiva – sono disposte in presenza di due requisiti:

- a. quando risultano gravi indizi per ritenere la sussistenza della responsabilità della società per un illecito amministrativo dipendente da reato (i gravi indizi sussistono ove risulti una delle condizioni previste dall'art. 13 del Decreto: la società ha tratto dal reato – compiuto da un suo dipendente o da un soggetto in posizione apicale – un profitto di rilevante entità e la commissione del reato è stata determinata o agevolata da gravi carenze organizzative; in caso di reiterazione degli illeciti;
- b. quando vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede.

Le misure cautelari reali consistono, invece, nel sequestro preventivo e nel sequestro conservativo.

Il sequestro preventivo ha ad oggetto il prezzo o il profitto del reato, laddove il fatto di reato sia attribuibile alla società, non importando che sussistano gravi indizi di colpevolezza a carico della società stessa.

Il sequestro conservativo ha ad oggetto beni mobili o immobili della società nonché somme o cose alla stessa dovute, qualora vi sia fondato motivo di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento e di ogni altra somma dovuta all'erario dello Stato.

1.5. Le azioni esimenti dalla responsabilità amministrativa

Gli artt. 6 e 7 del D. Lgs. 231/01 prevedono forme di esonero da responsabilità differenti a seconda che il reato presupposto sia stato commesso da soggetti in posizione apicale o subordinata.

L'art. 6 co. 1 del Decreto prevede una forma specifica di esimente dalla responsabilità amministrativa qualora il reato sia stato commesso da soggetti in c.d. «posizione apicale» e la Società provi che:

1. l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto illecito, un modello idoneo a prevenire la realizzazione degli illeciti della specie di quello verificatosi;
2. ha affidato ad un organo interno, c.d. Organismo di Vigilanza (OdV) - dotato di autonomi poteri di iniziativa e di controllo – il compito di vigilare sul funzionamento e sull'efficace osservanza del modello in questione, nonché di curarne l'aggiornamento;
3. i soggetti in c.d. «posizione apicale» hanno commesso il reato eludendo fraudolentemente il modello;
4. non vi è stato omesso o insufficiente controllo da parte dell'Organismo di Vigilanza.

L'art. 7 del Decreto prevede una forma specifica di esimente dalla responsabilità amministrativa qualora il reato sia stato commesso dai c.d. «sottoposti» ma sia accertato che la Società, prima della commissione del reato, abbia adottato un modello idoneo a prevenire reati della stessa specie di quello verificatosi (la Società è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza).

È bene precisare, quindi, che l'onere della prova cambia a seconda che i reati siano stati commessi da soggetti in posizione apicale o da coloro che sono sottoposti all'altrui direzione.

Infatti, nel caso di reati commessi da soggetti in posizione apicale, la Società dovrà provare che il reo abbia sostanzialmente agito contro il divieto di commettere reati impostogli dalla Società violando (con frode) il Modello predisposto dalla Società stessa.

In altri termini, nel caso del reato commesso dal soggetto apicale, l'invocabilità dell'esimente postula che non sia sufficiente la sola idoneità del Modello ad escludere l'inosservanza degli obblighi di direzione e vigilanza, ma altresì che il Modello adottato sia tale per cui possa essere eluso soltanto fraudolentemente.

Nel caso invece dei reati commessi da soggetti che sono sottoposti all'altrui direzione è sufficiente perché sia invocabile l'esimente l'aver adottato ed efficacemente attuato un Modello idoneo spettando al magistrato la prova della sua eventuale inidoneità.

Risulta a questo punto agevole comprendere che, al di là delle esimenti invocabili dalla Società a seconda che il reato sia stato commesso dai soggetti in posizione apicale o meno con relativa inversione dell'onere della prova, il fulcro centrale della disciplina per l'esonero della responsabilità della Società previsto dal D.Lgs. 231/2001 sta nell'adozione di un Modello di organizzazione, gestione e controllo che non costituisce solo un valido strumento di adeguamento alla normativa, ma altresì un'occasione per ribadire e diffondere principi etici comportamentali a cui ispirarsi nell'esercizio delle attività aziendali.

L'art. 6 co. 2 del Decreto dispone, inoltre, che il modello debba rispondere alle seguenti esigenze:

- individuare i rischi aziendali ovvero le attività nel cui ambito possono essere commessi i reati;
- escludere che un qualunque soggetto operante all'interno della Società possa giustificare la propria condotta adducendo l'ignoranza delle discipline aziendali ed evitare che, nella normalità dei casi, il reato possa essere causato dall'errore – dovuto anche a negligenza o imperizia – nella valutazione delle direttive aziendali;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- prevedere un sistema di controlli preventivi tali da non poter essere aggirati se non intenzionalmente;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza deputato a controllare sul funzionamento e l'osservanza del modello.

In concreto è possibile affermare che la Società, per poter essere esonerata dalla responsabilità amministrativa, deve dotarsi di presidi etico-comportamentali ai quali ispirarsi nello svolgimento delle attività aziendali. A tal fine risulta necessaria l'adozione di un Codice Etico che statuisca principi generali di comportamento. Risulta, altresì, necessario definire una struttura organizzativa in grado di garantire una chiara ed organica attribuzione dei compiti, di attuare una segregazione delle funzioni, nonché di ispirare e controllare la correttezza dei comportamenti. Ed ancora, formalizzare procedure aziendali manuali ed informatiche destinate a regolamentare lo svolgimento delle attività (una particolare efficacia preventiva riveste lo strumento di controllo rappresentato dalla "segregazione dei compiti" tra coloro che svolgono fasi cruciali di un processo a rischio), assegnare poteri autorizzativi e di firma in coerenza con le responsabilità organizzative e gestionali definite, nonché, infine, comunicare al personale in modo capillare, efficace, chiaro e dettagliato tutti siffatti presidi.

Su tale sistema vigila l'Organismo di Vigilanza, caratterizzato da sostanziale autonomia, indipendenza e professionalità, valutando l'adeguatezza del modello e vigilando sul suo funzionamento, operando con continuità di azione.

2. L'ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

2.1. La società INPOWER GROUP CONSORZIO STABILE SCPA

Inpower Group - Consorzio Stabile Scpa (anche "Inpower Group") è una società consortile per azioni con sede legale in Roma, costituita nel 2009, che opera come realtà strutturata nel settore delle infrastrutture tecnologiche, delle telecomunicazioni e degli impianti elettrici ed elettromeccanici.

Nel corso degli anni la società ha consolidato un ruolo di primo piano nella realizzazione di opere complesse, nella gestione di servizi tecnici avanzati e nello sviluppo di progetti specialistici per committenti pubblici e privati.

L'attività si fonda su un modello operativo che integra competenze tecniche, capacità organizzative e una rete di imprese consorziate altamente qualificate. Tale assetto consente a Inpower Group di assumere ed eseguire appalti, partecipare a gare, coordinare attività di progettazione, installazione, manutenzione e gestione di impianti, nonché di operare in ambiti specialistici quali reti di telecomunicazione, infrastrutture energetiche, sistemi di sicurezza, opere civili e servizi di global service.

La struttura organizzativa, articolata in *Business Unit* dedicate (Networking, Delivery & Assurance, Impianti Speciali, Fibra) e in funzioni centrali di coordinamento (*Compliance*, Qualità-Sicurezza-Ambiente, Controllo di Gestione, Amministrazione, Risorse Umane), consente alla società di garantire un presidio costante dei processi operativi e di assicurare elevati *standard* di qualità, sicurezza e affidabilità.

Nel tempo, Inpower Group ha sviluppato un modello di crescita basato sull'ampliamento delle competenze tecniche, sull'adozione di sistemi di gestione certificati e sull'integrazione di procedure organizzative orientate alla trasparenza, alla tracciabilità e alla prevenzione dei rischi. L'attenzione alla compliance, alla sostenibilità operativa e alla tutela degli stakeholder rappresenta un elemento centrale della strategia aziendale.

In questa prospettiva, l'adozione del Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001 rappresenta un elemento centrale del sistema di governance della Società. Il presente aggiornamento del Modello si inserisce nel percorso di costante evoluzione e rafforzamento dei presidi organizzativi e di controllo, al fine di assicurare che tutte le attività sensibili siano disciplinate da regole chiare, procedure formalizzate e controlli efficaci, in coerenza con la struttura organizzativa, con il Codice Etico e con il sistema di gestione interno.

L'impegno della Società è orientato a garantire un ambiente operativo improntato ai principi di legalità, integrità, correttezza e responsabilità, promuovendo comportamenti conformi ai valori aziendali e prevenendo ogni possibile forma di illecito. L'aggiornamento del Modello 231 conferma la volontà della Società di mantenere un sistema di controllo interno efficace e costantemente allineato all'evoluzione normativa, organizzativa e operativa, nell'ottica del miglioramento continuo e della tutela della Società, dei soci, dei clienti, dei partner commerciali e di tutti gli stakeholder coinvolti nelle attività aziendali.

2.2. Lo scopo di adozione e aggiornamento del Modello di organizzazione, gestione e controllo

Inpower Group - Consorzio Stabile Scpa., in coerenza con i propri principi etico-comportamentali e al fine di assicurare condizioni di correttezza, trasparenza e integrità nella conduzione degli affari e delle attività aziendali, ha adottato il proprio Codice Etico e il Modello di Organizzazione, Gestione e Controllo (di seguito, il "Modello") ai sensi del D.Lgs. 231/2001, quale parte integrante del sistema di *governance* e di controllo interno della Società.

Il presente aggiornamento del Modello si inserisce nel processo di costante verifica e adeguamento dei presidi organizzativi e di controllo, volto a garantire l'efficacia del sistema di prevenzione dei rischi e la sua coerenza con l'evoluzione del contesto normativo, organizzativo e operativo della Società.

Inpower Group - Consorzio Stabile Scpa ritiene che il Modello costituisca, oltre che un fondamentale strumento di prevenzione dei reati rilevanti ai sensi del D.Lgs. 231/2001, un efficace mezzo di diffusione della cultura della legalità e dei valori aziendali, promuovendo la consapevolezza e la responsabilizzazione di tutti i destinatari, dipendenti, collaboratori, partner commerciali e, più in generale, di tutti i soggetti con i quali la Società intrattiene rapporti a qualsiasi titolo.

Il modello, al fine di strutturare un sistema preventivo e di controllo, individua le attività maggiormente sensibili al “rischio-reato” e le modalità operative per farvi fronte.

Le finalità del Modello sono, pertanto, di:

- prevenire e ragionevolmente limitare i possibili rischi connessi all’attività aziendale con particolare riguardo ai rischi collegati alle condotte illecite;
- fare acquisire a tutti coloro che operano in nome e per conto di Inpower Group nelle aree di attività a rischio, la consapevolezza dell’eventualità di porre in essere, ove risultino violate le disposizioni riportate nel modello, condotte passibili di sanzioni penali e/o amministrative non solo nei loro confronti, ma anche nei confronti di Inpower Group stessa;
- ribadire che Inpower Group non ammette comportamenti illeciti;
- informare in ordine alle gravose conseguenze che potrebbero derivare alla Società (e, dunque, indirettamente a tutti i portatori di interesse) dall’applicazione delle sanzioni pecuniarie e interdittive previste dal Decreto e della possibilità che esse siano disposte anche in via cautelare;
- consentire alla società un costante controllo ed un’attenta vigilanza sulle attività, in modo da poter intervenire tempestivamente ove si manifestino profili di rischio ed eventualmente applicare le misure disciplinari previste dallo stesso Modello.

2.3. Il campo di applicazione

I protocolli descritti nella Parte Speciale del Modello si applicano a tutti coloro che intrattengono, a qualsivoglia titolo, rapporti con la Società. Trattasi di coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella Società, i soci e dipendenti, nonché coloro i quali, pur non appartenendo alla Società, operano su mandato della medesima o sono legati contrattualmente alla stessa.

In forza dei rapporti contrattuali instaurati e limitatamente allo svolgimento delle attività sensibili a cui essi eventualmente partecipano, possono essere destinatari di specifici obblighi, strumentali ad un’adeguata esecuzione delle attività di controllo interno previste nella presente Parte Generale, i seguenti soggetti esterni:

- i collaboratori, gli agenti e i rappresentanti, i consulenti e in generale i soggetti che svolgono attività di lavoro autonomo nella misura in cui essi operino nell’ambito delle aree di attività sensibili per conto o nell’interesse della Società;
- i fornitori e i *partner* commerciali (anche sotto forma di associazione temporanea di imprese, nonché di *jointventure*) che operano in maniera rilevante e/o continuativa nell’ambito delle aree di attività cosiddette sensibili per conto o nell’interesse della Società.

Inpower Group divulga il presente Modello attraverso modalità idonee ad assicurarne l’effettiva conoscenza da parte di tutti i soggetti interessati.

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

2.4. Le attività propedeutiche all’aggiornamento del Modello

La Società, anche tramite il supporto di consulenti esterni, ha avviato il progetto finalizzato all’aggiornamento del Modello di Organizzazione, Gestione e Controllo (di seguito “MOGC”) ai sensi dell’art. 6, comma 2, lett. a) del D. Lgs. 231/01 e, in via principale e non esaustiva, delle Linee Guida Confindustria.

Nel corso del progetto, il Gruppo di lavoro 231 ha interagito con le funzioni aziendali competenti con incontri e interviste mirati alla raccolta di informazioni e documentazione relativi alla Società al fine di procedere ad una dettagliata analisi e all'individuazione e valutazione delle aree di rischio.

L'attività di progettazione e aggiornamento di tale Modello è stata finalizzata prioritariamente a presidiare le aree che sono emerse come maggiormente a rischio.

Tale attività è stata strutturata come di seguito indicato:

- organizzazione, pianificazione, comunicazione e avvio del progetto di predisposizione e sviluppo del MOGC;
- raccolta documentazione/informazioni preliminari (norme, procedure, sistema delle deleghe, organigramma etc.);
- analisi dell'azienda e identificazione delle aree di rischio ex D. Lgs. 231/01 ("macro aree" di attività sensibili) e dei relativi processi e ruoli aziendali coinvolti;
- valutazione dei rischi attraverso la mappatura¹ dei processi sensibili in termini di:
 - reati prospettabili ed astrattamente ipotizzabili a cui ciascun processo risulta esposto;
 - potenziali modalità attuative del reato per ciascun processo;
 - funzioni organizzative/ruoli aziendali coinvolti nel processo;
 - grado di rischio associato.

Successivamente si è provveduto ad implementare la formalizzazione e aggiornamento del Modello di Organizzazione, Gestione e Controllo.

Il presente aggiornamento del Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/01 si è reso necessario a seguito sia degli aggiornamenti del catalogo dei reati ex D.Lgs. 231 /2001 che dalle modifiche societarie avvenute. Il Modello è stato presentato al Vertice aziendale e successivamente sottoposto all'approvazione e delibera dell'Organo Amministrativo della Società.

Il presente MOGC è un atto di emanazione dell'organo amministrativo e, come tale, allo stesso è rimessa anche l'eventuale modifica e/o integrazione.

3. LA STRUTTURA E ARTICOLAZIONE DEL MODELLO

3.1. Premessa metodologica: concetto di "rischio accettabile"

Di particolare rilievo ai fini della costruzione del Modello è il concetto di "rischio accettabile".

Il rischio è ritenuto tale quando i controlli aggiuntivi introdotti per prevenire la commissione dei reati "costano" più della risorsa da proteggere. Ciò che, infatti, rileva è la necessità di definire quale sia il limite alla quantità/qualità delle presidi da introdurre per evitare la commissione dei reati considerati, oltre la quale l'introduzione di tali strumenti di prevenzione risulti eccessivamente gravoso.

Tale nozione non si identifica con l'assenza di rischio-reato, né con un obiettivo di neutralizzazione assoluta dello stesso, risultando invece espressione di un bilanciamento tra l'esigenza di prevenzione dei reati presupposto e la fisiologica operatività dell'attività d'impresa. In tale prospettiva, il rischio residuo è considerato accettabile

¹ ¹ Ai fini dello svolgimento delle indicate attività di *risk assessment* la metodologia seguita si è concentrata sulla combinazione di due principali parametri di riferimento:

1. Probabilità (grado di possibilità di realizzazione dell'evento);

2. Impatto (potenziali conseguenze in caso di realizzazione dell'evento).

allorché il sistema di prevenzione adottato risulti idoneo a ridurre la possibilità di commissione dei reati entro margini ragionevoli, compatibili con l'assetto organizzativo e con le caratteristiche dimensionali e operative dell'ente.

Ne deriva che la determinazione della soglia di accettabilità costituisce un passaggio necessario della costruzione del Modello, in quanto funzionale a evitare un'impostazione iper-prescrittiva dei controlli, potenzialmente idonea a compromettere l'efficienza e la continuità dell'azione aziendale.

Con riferimento ai reati dolosi, la soglia di rischio accettabile è individuata in un assetto organizzativo tale da rendere la commissione dell'illecito possibile esclusivamente mediante condotte di elusione fraudolenta del Modello, secondo quanto espressamente previsto dall'art. 6, comma 1, lett. c), del D.Lgs. 231/2001. In tale ambito, l'efficacia del Modello si misura, dunque, nella sua idoneità a prevenire comportamenti intenzionalmente diretti alla violazione dei presidi organizzativi, salvo il caso di loro fraudolenta elusione.

Con riguardo ai reati di natura colposa, la nozione di rischio accettabile deve essere declinata in funzione della struttura dell'illecito, con conseguente individuazione della soglia nella predisposizione e nell'efficace attuazione di un sistema di prevenzione idoneo a governare il rischio attraverso il rispetto delle norme cautelari e delle regole prevenzionistiche pertinenti. In tale ambito, la compatibilità logico-sistematica con il paradigma dell'elusione fraudolenta risulta recessiva, attesa la natura non volontaria dell'evento tipica dei reati colposi.

In definitiva, il concetto di rischio accettabile costituisce il parametro tecnico-giuridico di riferimento per la calibratura del Modello, orientandone la struttura verso un equilibrio tra efficacia preventiva, proporzionalità dei presidi e sostenibilità organizzativa, in coerenza con la funzione esimente attribuita dal D.Lgs. 231/2001 al sistema di organizzazione e controllo dell'ente.

3.2. La struttura

Il presente Modello, generalmente ispirato alle «Linee guida per la costruzione di modelli di organizzazione, gestione e controllo deliberato ex d.lgs. 231/01» approvate da Confindustria in data 7 marzo 2002 e successivamente aggiornate, consta di una parte generale, una parte speciale e di documentazione allegata.

La "Parte Generale" descrive la normativa rilevante, le regole generali di funzionamento del Modello, l'Organismo di Vigilanza e il Sistema Sanzionatorio.

La "Parte Speciale" è strutturata in due differenti sezioni: una prima, in relazione alle famiglie di reato potenzialmente verificabili, individua le aree sensibili rilevanti per lo specifico contesto aziendale e detta alcune norme e principi di comportamento al fine di prevenire la commissione di fatti la cui responsabilità risulti ascrivibile all'ente; una seconda sezione, individua i protocolli relativi alle singole aree di attività aziendale.

Il Modello predisposto da Inpower Group si fonda su:

- il Codice etico, destinato a fissare le linee di comportamento generali;
- la struttura organizzativa che definisce l'attribuzione dei compiti, prevedendo, per quanto possibile, la separazione delle funzioni o in alternativa dei controlli compensativi. e i soggetti chiamati a controllare la correttezza dei comportamenti;
- la mappatura delle aree aziendali sensibili vale a dire la descrizione di quei processi nel cui ambito risulta più agevole che possano essere commessi reati;

- i processi strumentali alle aree aziendali sensibili, ovvero quei processi attraverso i quali vengono gestiti strumenti di tipo finanziario e/o mezzi sostitutivi in grado di supportare la commissione dei reati nelle aree a rischio reato;
- l'utilizzo di procedure aziendali formalizzate, tese a disciplinare le modalità operative corrette per assumere ed attuare decisioni nelle diverse aree aziendali sensibili;
- l'indicazione dei soggetti che intervengono a presidio di tali attività, nei ruoli auspicabilmente distinti sia di esecutori sia di controllori, ai fini di una segregazione dei compiti di gestione e di controllo;
- l'adozione di un sistema di deleghe e di poteri aziendali, coerente con le responsabilità assegnate e che assicuri una chiara e trasparente rappresentazione del processo aziendale di formazione e di attuazione delle decisioni, secondo il requisito della unicità del preposto alla funzione;
- l'individuazione di metodologie e di strumenti che assicurino un adeguato livello di monitoraggio e di controllo, sia diretto sia indiretto, essendo il primo tipo di controllo affidato agli operatori specifici di una data attività e al preposto, nonché il secondo controllo al management e all'Organismo di vigilanza;
- la precisazione dei supporti informativi per la tracciabilità delle attività di monitoraggio e di controllo (es. schede, rapporti ecc.);
- la definizione di un sistema sanzionatorio per coloro che violino le regole di condotta stabilite dalla Società;
- l'attuazione di un piano di informazione e formazione dei soggetti aziendali in posizione apicale e subordinata;
- la costituzione di un Organismo di Vigilanza cui viene assegnato il compito di vigilare sull'efficacia ed il corretto funzionamento del modello, sulla coerenza dello stesso con gli obiettivi e che faccia da impulso al suo aggiornamento periodico.

3.3. Il sistema dei controlli preventivi

Le attività precedentemente descritte si completano con una valutazione del sistema di controlli preventivi eventualmente esistente e con il suo adeguamento, qualora ciò si riveli necessario, o con una sua costruzione quando l'ente ne sia sprovvisto. Il sistema di controlli preventivi dovrà essere tale da garantire che i rischi di commissione dei reati, secondo le modalità individuate e documentate nella fase precedente, siano ridotti ad un "livello accettabile", secondo la definizione esposta in premessa. Si tratta, in sostanza, di progettare quelli che il D. Lgs. 231/01 definisce «specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire».

Di seguito sono elencate le componenti generalmente riconosciute quali protocolli di un sistema di controllo preventivo, che dovranno essere attuate a livello aziendale per garantire l'efficacia del modello:

- il Codice Etico;
- un sistema organizzativo formalizzato e chiaro, soprattutto per quanto attiene all'attribuzione di responsabilità;
- le procedure manuali ed informatiche (sistemi informativi) tali da regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo. In questo ambito una particolare efficacia preventiva riveste lo strumento di controllo rappresentato dalla separazione di compiti fra coloro che svolgono fasi (attività) cruciali di un processo a rischio;
- i poteri autorizzativi e di firma assegnati in coerenza con le responsabilità organizzative e gestionali definite;
- il sistema di controllo di gestione in grado di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità generale e/o particolare;
- la comunicazione e formazione a tutto il personale.

Secondo le Linee Guida di Confindustria, le componenti sopra descritte devono integrarsi organicamente in un'architettura del sistema che rispetti tre principi generali di controllo, fra cui:

- ogni operazione, transazione, azione deve essere verificabile, documentata, coerente e congrua: per ogni operazione vi deve essere un adeguato supporto documentale su cui si possa procedere in ogni momento all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa;
- nessuno può gestire in autonomia un intero processo: il sistema deve garantire l'applicazione del principio di separazione di funzioni, per cui l'autorizzazione all'effettuazione di un'operazione, deve essere sotto la responsabilità di persona diversa da chi contabilizza, esegue operativamente o controlla l'operazione;
- documentazione dei controlli: il sistema di controllo deve documentare (eventualmente attraverso la redazione di verbali) l'effettuazione dei controlli, anche di supervisione.

Più specificamente, con riferimento alle aree di attività cosiddette sensibili, la Società ha poi individuato i seguenti principi cardine del presente Modello, che regolando tali attività rappresentano gli strumenti diretti a programmare la formazione e l'attuazione delle decisioni della Società e a garantire un idoneo controllo sulle stesse, anche in relazione ai reati da prevenire:

- separazione dei compiti attraverso una corretta distribuzione delle responsabilità e la previsione di adeguati livelli autorizzativi, allo scopo di evitare sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto;
- chiara e formalizzata assegnazione di poteri e responsabilità, con espressa indicazione dei limiti di esercizio e in coerenza con le mansioni attribuite e le posizioni ricoperte nell'ambito della struttura organizzativa;
- nessuna operazione significativa può essere intrapresa senza autorizzazione;
- esistenza di regole comportamentali idonee a garantire l'esercizio delle attività aziendali nel rispetto delle leggi e dei regolamenti e dell'integrità del patrimonio aziendale;
- adeguata regolamentazione procedurale delle attività aziendali cosiddette sensibili, cosicché: o i processi operativi siano definiti prevedendo un adeguato supporto documentale per consentire che essi siano sempre verificabili in termini di congruità, coerenza e responsabilità; o le decisioni e le scelte operative siano sempre tracciabili in termini di caratteristiche e motivazioni e siano sempre individuabili coloro che hanno autorizzato, effettuato e verificato le singole attività; o siano garantite modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati; o siano svolte e documentate le attività di controllo e supervisione, compiute sulle transazioni aziendali; o esistano meccanismi di sicurezza che garantiscano un'adeguata protezione all'accesso fisico-logico ai dati e ai beni aziendali; o lo scambio delle informazioni fra fasi o processi contigui avvenga in modo da garantire l'integrità e la completezza dei dati gestiti.

È opportuno evidenziare che la mancata conformità a punti specifici delle Linee Guida di Confindustria non inficia di per sé la validità del Modello. Il singolo Modello, infatti, dovendo essere redatto con riguardo alla realtà concreta della società cui si riferisce, ben può discostarsi in taluni specifici punti dalle Linee Guida (che, per loro natura, hanno carattere generale), quando ciò sia dovuto alla necessità di garantire maggiormente le esigenze tutelate dal Decreto.

I principi sopra descritti appaiono, comunque, coerenti con le indicazioni fornite dalle Linee Guida emanate da Confindustria e sono ritenuti dalla società ragionevolmente idonei anche a prevenire i reati richiamati dal Decreto.

3.4. Il sistema delle deleghe e dei poteri

Il sistema di deleghe e poteri ha ad oggetto, da un lato, i poteri c.d. “interni”, relativi a processi decisionali interni e alle decisioni da adottare; dall’altro, i poteri c.d. “esterni”, di rappresentanza all’esterno attraverso l’adozione di atti che vincolano l’ente con terze parti (c.d. “procure generali o speciali”).

Il sistema autorizzativo, che si traduce in un sistema articolato e coerente di deleghe di funzioni e procure della Società, deve uniformarsi alle seguenti prescrizioni:

- le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell’organigramma; devono, altresì, essere aggiornate in conseguenza dei mutamenti organizzativi;
- ciascuna delega deve definire e descrivere in modo specifico e non equivoco i poteri gestionali del delegato e il soggetto al quale il delegato riporta gerarchicamente;
- la delega deve essere esplicitamente accettata dal soggetto delegato;
- i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;
- il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli;
- le procure possono essere conferite esclusivamente a soggetti dotati di delega funzionale interna o di specifico incarico e devono prevedere l’estensione dei poteri di rappresentanza e, eventualmente, i limiti di spesa numerici;
- solo i soggetti muniti di specifici e formali poteri possono assumere, in nome e per conto dell’ente, obbligazioni verso terzi;
- tutti coloro che intrattengono rapporti con la P.A. devono essere dotati di delega o procura in tal senso;
- lo Statuto definisce i requisiti e le modalità di nomina del dirigente preposto alla redazione dei documenti contabili e societari.

A tutti i poteri attribuiti mediante delega o espletamento di poteri corrispondono esattamente mansioni e responsabilità come riportate nell’organigramma della Società.

3.5. I processi sensibili e criteri decisionali

Il processo decisionale afferente alle aree di attività sensibili deve uniformarsi ai seguenti criteri generali:

- ogni decisione riguardante le operazioni nell’ambito delle aree di attività sensibili, come di seguito individuate, deve risultare da un documento scritto;
- non deve esservi identità soggettiva tra colui che decide in merito allo svolgimento di un processo all’interno di un’area di attività sensibile e colui che effettivamente lo pone in essere portandola a compimento;
- non deve esservi identità soggettiva tra coloro che decidono e pongono in essere un processo all’interno di un’area sensibile e color che risultano investiti del potere di destinarvi le necessarie risorse economiche e finanziarie.

Le attività condotte nell’ambito delle attività sensibili e dei processi strumentali trovano adeguata formalizzazione con particolare riferimento alla documentazione predisposta all’interno della realizzazione delle stesse.

3.6. I sistemi informativi e applicativi informatici

Al fine di presidiare l'integrità dei dati e l'efficacia dei sistemi informativi e/o gli applicativi informatici utilizzati per lo svolgimento di attività operative o di controllo nell'ambito di attività sensibili o processi strumentali o a supporto delle stesse, è garantita la presenza e l'operatività di:

- sistemi informativi aziendali adeguati e costantemente aggiornati, comprendenti infrastrutture hardware e software idonee a supportare le attività operative e di controllo;
- utilizzo regolamentato della posta elettronica aziendale, con sistemi di gestione degli accessi che disciplinano l'invio, la ricezione e l'archiviazione dei documenti;
- politiche automatizzate di generazione, gestione e aggiornamento delle password, conformi ai requisiti di sicurezza e alle best practice in materia di protezione dei dati;
- tracciabilità soggettiva degli accessi ai sistemi informatici e delle operazioni effettuate dagli utenti, mediante credenziali personali (UserID e password);
- sistemi di monitoraggio e *logging* delle attività svolte all'interno della rete aziendale, con conservazione storica delle operazioni rilevanti;
- meccanismi automatizzati di blocco, limitazione o inibizione degli accessi non autorizzati o anomali;
- procedure di disabilitazione degli *account* in caso di cessazione del rapporto di lavoro o di variazione delle mansioni;
- sistema di registrazione (log) delle transazioni informatiche, strutturato e automatizzato, volto a garantire la ricostruibilità delle attività svolte.

Tali presidi concorrono a garantire che l'accesso ai dati e ai sistemi aziendali avvenga in modo controllato, sicuro e conforme alle procedure interne, riducendo il rischio di comportamenti illeciti o non autorizzati e assicurando la piena tracciabilità delle attività svolte.

3.7. La diffusione e formazione

Diffusione (c.d. "informativa")

Per garantire l'efficacia del Modello, Inpower Group si pone l'obiettivo di assicurarne la corretta conoscenza, da parte di tutti i Destinatari, anche in funzione del loro diverso livello di coinvolgimento nei processi sensibili.

A tal fine, Inpower Group provvede alla diffusione del Modello mediante le seguenti modalità di carattere generale:

1. la pubblicazione nell'*intranet* aziendale del Modello adottato e l'eventuale esposizione nella bacheca aziendale;
2. la richiesta di compilazione di una dichiarazione di impegno a tutti i dipendenti della Società, nella quale si dichiara di osservare le prescrizioni in esso contenute;
3. l'inserimento nei contratti con terzi dell'obbligo di prendere visione del Modello di Inpower Group e del suo Codice Etico e di conformarsi ai principi ivi previsti, nonché della clausola di risoluzione contrattuale in caso di condanna, ancorché non definitiva, subita dalla controparte per uno dei reati previsti dal D.Lgs. 231/2001.

Pertanto, al momento dell'aggiornamento del Modello è inviata a tutti i dipendenti in organico una comunicazione, da parte degli organi individuati (es. Organo amministrativo, Direzione risorse umane, ecc.), per avvertire che Inpower Group è dotata ed ha aggiornato il Modello di Organizzazione, gestione e controllo ai sensi del Decreto, rimandando al sito *intranet* aziendale per maggiori dettagli e approfondimenti. La comunicazione è corredata da una dichiarazione di ricevuta e accettazione da parte dei dipendenti, da trasmettere all'OdV.

Ai nuovi dipendenti è consegnata un'apposita informativa sul Modello adottato contenente una nota informativa, nel corpo della lettera di assunzione, dedicata al Decreto ed alle caratteristiche del Modello adottato.

Informativa a collaboratori esterni e *partner*

Tutti i soggetti esterni alla Società (consulenti, *partner*, ecc.) sono opportunamente informati in merito all'adozione, da parte di Inpower Group del Modello Organizzativo e del Codice Etico. A tal fine Inpower Group comunica a tutti i suddetti soggetti l'esistenza dell'indirizzo internet nel quale è possibile visionare il Modello e il Codice etico. È inoltre richiesto loro il formale impegno al rispetto delle disposizioni contenute nei suddetti documenti.

Per quanto riguarda i consulenti esterni che stabilmente collaborano con Inpower Group, è cura della stessa Società prendere contatti con questi e accertarsi che detti consulenti conoscano il Modello della Società e siano disposti a rispettarlo.

Formazione

I contenuti dei programmi di formazione devono essere avallati da un consulente esterno alla Società, esperto in materia di responsabilità amministrativa degli enti (D. Lgs. n. 231/2001) o, più in generale, in materie penalistiche, che opererà anche di concerto con l'OdV. Della formazione occorre tenere traccia formale.

La formazione può essere tenuta anche con modalità *e-learning* ovvero, in relazione a quei dipendenti non raggiungibili tramite sistemi informatici, mediante schede in formato cartaceo.

Formazione del personale

La formazione del personale avviene sulla base di un corso di formazione e aggiornamento, con obbligo di partecipazione e di frequenza nonché con un test valutativo finale – che può essere tenuto anche oralmente in grado di attestare la qualità dell'attività formativa ricevuta.

La formazione e l'aggiornamento sono definiti in un programma annuale condiviso con l'OdV di Inpower Group e, per eventuali neo cooptati con funzioni amministrative (es. componenti del C.d.A.) ovvero per eventuali neoassunti, avviene sulla base anche di un'informativa contenuta nella lettera di assunzione.

La formazione deve contenere:

- riferimenti normativi, giurisprudenziali e di *best practice*;
- responsabilità amministrativa dell'ente: scopo, *ratio* del Decreto, natura della responsabilità, presupposti di imputazione; condizioni per l'esclusione della responsabilità o limitazione della stessa;
- descrizione dei reati presupposto;
- tipologie di sanzioni applicabili all'ente.

Nell'ambito della formazione, inoltre, ci si sofferma sulla descrizione della struttura e dei contenuti del Modello adottato, in particolare:

- sulla descrizione delle fattispecie di reato;
- sull'individuazione degli autori dei reati;
- su alcune esemplificazioni delle modalità attraverso le quali i reati vengono posti in essere;
- sulle aree di rischio evidenziate;
- sui protocolli di prevenzione specifici individuati;
- sulla sensibilizzazione dei responsabili delle funzioni aziendali potenzialmente a rischio di reato e dei propri dipendenti gerarchici, in relazione al comportamento da osservare, alle conseguenze derivanti da un mancato rispetto delle stesse e, in generale, del Modello adottato da Inpower Group.

4. IL SISTEMA SANZIONATORIO

La predisposizione di un efficace sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello è condizione essenziale per garantire l'effettività del modello stesso.

Al riguardo, infatti, l'articolo 6 comma 2 lettera e) e l'art. 7 comma 4 lett. b) del Decreto prevedono che il modello debba «introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello».

L'applicazione delle sanzioni disciplinari determinate ai sensi del Decreto prescinde dall'esito di eventuali procedimenti penali, in quanto le regole imposte dal Modello e dal Codice etico sono assunte da Inpower Group in piena autonomia, indipendentemente dalla tipologia di illecito che le violazioni del Modello o del Codice stesso possano determinare.

In particolare, Inpower Group si avvale di un sistema sanzionatorio che:

- è diversamente strutturato a seconda dei soggetti destinatari: soggetti in posizione c.d. "apicale", dipendenti, collaboratori esterni e partner;
- individua esattamente le sanzioni disciplinari da adottarsi nei confronti di soggetti che pongano in essere violazioni, infrazioni, elusioni, imperfette o parziali applicazioni delle prescrizioni contenute nel modello, il tutto nel rispetto delle relative disposizioni dei CCNL e delle prescrizioni legislative applicabili;
- prevede un'apposita procedura di irrogazione delle suddette sanzioni, individuando il soggetto preposto alla loro irrogazione e in generale a vigilare sulla osservanza, applicazione ed aggiornamento del sistema sanzionatorio;
- introduce idonee modalità di pubblicazione e diffusione.

Per i dettagli si rimanda all' "Allegato – Sistema sanzionatorio".

5. L'ORGANISMO DI VIGILANZA

In ottemperanza a quanto previsto all'art. 6 comma 1, lett. b) del Decreto, che prevede che il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne il relativo aggiornamento sia affidato ad un organismo di Inpower Group, dotato di autonomi poteri di iniziativa e controllo, denominato Organismo di Vigilanza (OdV), la Società ha provveduto all'identificazione e alla nomina di tale Organismo, mediante delibera dell'organo amministrativo. La durata dell'incarico e l'indicazione del Presidente, scelto tra i membri dell'OdV, sono altresì stabiliti nell'atto di nomina.

Sulla base delle indicazioni contenute nel D.Lgs. 231/01 e delle Linee guida, nonché in considerazione della dimensione e dell'organizzazione di Inpower Group, la Società ha deciso di dotarsi un OdV Collegiale.

I membri dell'OdV sono scelti tra soggetti che soddisfino i requisiti di autonomia, indipendenza, professionalità e onorabilità e, nello svolgimento delle proprie funzioni, l'OdV si avvale di risorse interne e consulenti esterni, utilizzando le disponibilità previste ed approvate nel *budget*.

In casi di particolare gravità, l'organo amministrativo, sentito il Consiglio di Amministrazione ed ascoltato preventivamente il/i membro/i dell'ODV interessato/i, potrà disporre la sospensione del/i componente/i dell'ODV e la nomina di/ dei sostituto/i ad *interim* e potrà altresì disporre l'eventuale revoca per giusta causa dei membri dell'ODV sempre previa audizione del/dei componente/i interessato/i.

5.1. Funzionamento dell'OdV

L'OdV, nell'esercizio della propria autonomia, si è dotato di un proprio Regolamento conservato a cura del Presidente dell'OdV e in copia presso i Componenti dell'organo.

5.2. Funzioni e poteri

All'OdV sono riconosciuti autonomi poteri di iniziativa e controllo. Le attività e la metodologia di programmazione e lavoro che l'OdV dovrà seguire vengono qui di seguito sintetizzate.

Tenuto conto della peculiarità delle funzioni attribuite all'OdV e dei contenuti professionali specifici ad esso richiesti, l'OdV può avvalersi, per lo svolgimento dei propri compiti, delle altre strutture interne della Società, così come di consulenti esterni.

1) Attività di verifica e controllo

A tal fine l'ODV:

- a. verifica l'osservanza, l'attuazione e l'adeguatezza del Modello adottato rispetto alla prevenzione e all'impedimento della commissione dei reati previsti dal D. Lgs. 231/2001;
- b. vigila sull'effettiva e concreta applicazione del Modello, verificando la congruenza dei comportamenti all'interno della Società rispetto allo stesso;
- c. verifica il rispetto del Sistema di Controllo Esistente e dei Protocolli previsti dal Modello e rileva gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i Responsabili dei vari processi individuati dall'OdV;
- d. effettua verifiche periodiche mirate su determinate operazioni compiute dalla Società, appartenenti ad un'area cosiddetta "sensibile" (d'ora in poi "Operazioni" / "Operazione");
- e. svolge, direttamente o attraverso risorse interne o esterne, attività di *audit* rivolgendosi direttamente alla funzione aziendale che ha curato l'Operazione, acquisisce copia di tutta documentazione disponibile, svolge colloqui diretti con i responsabili dell'Operazione, discute con essi delle eccezioni eventualmente riscontrate, propone eventuali azioni correttive;
- f. ha accesso a tutti i documenti riguardanti il Modello ed il Sistema Controllo Esistente nel suo complesso.
- g. comunica eventuali violazioni del Modello agli organi competenti in base al Sistema Disciplinare, per l'adozione di eventuali provvedimenti sanzionatori;
- h. curare il costante aggiornamento del Modello, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservarne l'adeguatezza e/o l'effettività.

Scopo di queste attività è quello di verificare l'effettività del Modello, la sua idoneità a prevenire i rischi e la correttezza con cui sono state compiute le Operazioni sensibili.

Con specifico riferimento ai flussi informativi, è di seguito riportato un elenco dei principali flussi e tempistiche di riferimento:

Oggetto del flusso informativo	Cadenza	Funzione competente
Infortuni, incidenti, mancati incidenti	IMMEDIATO	RSPP / Datore di Lavoro delegato QSA (per cantieri) Direzione del Personale
Non idoneità alla mansione / malattie professionali	TEMPESTIVO	RSPP Direzione del Personale
Aggiornamenti DVR e documentazione sicurezza	SEMESTRALE	RSPP / Datore di Lavoro delegato QSA
Incidenti ambientali / rifiuti / cantieri	IMMEDIATO	RSPP QSA Responsabili Centri Operativi
Cambiamenti nell'assetto interno: organigramma / deleghe / procure	TEMPESTIVO	AD Coordinamento Compliance Back Office
Variazioni degli organi societari (CdA, Collegio Sindacale, OdV)	IMMEDIATO	AD Coordinamento Compliance
Operazioni straordinarie (fusioni, acquisizioni, aumenti capitale, investimenti rilevanti)	IMMEDIATO	AD Back Office
Nuovi fornitori, distaccanti, subappaltatori: qualificazione e anomalie	TEMPESTIVO	Acquisti Direzione del Personale (distaccati) QSA
Verbali e accertamenti da Autorità di controllo (INPS, GdF, AdF, ASL, Ispettorato Lavoro, ARPA)	IMMEDIATO	Consulente fiscale RSPP (ASL, Ispettorato Lavoro) Back Office Compliance
Delibere, domande e ottenimento di contributi / finanziamenti pubblici	TEMPESTIVO	Ufficio Gare e Supporto Legale AD Tesoreria
Operazioni sospette o irregolari — pagamenti anomali / variazioni IBAN	IMMEDIATO	Tesoreria Amministrazione e Contabilità Back Office

Oggetto del flusso informativo	Cadenza	Funzione competente
Bilancio, relazioni organi di controllo e nota integrativa	ANNUALE	Amministrazione e Contabilità
		Back Office
		Controllo di Gestione
		Consulenti fiscali
Segnalazioni della società di revisione / Collegio Sindacale	TEMPESTIVO	Amministrazione e Contabilità Back Office
Eventi con impatto sul MOG 231 — mutamenti aree a rischio / operativi	TEMPESTIVO	Tutte le funzioni — ciascuna per la propria AS di competenza Coordinamento Compliance (coordinamento)
Modifica procedure con impatto sui rischi 231 (PQSA, PQ, protocolli operativi)	TEMPESTIVO	Coordinamento Compliance QSA Acquisti (per PQSA_08_10)
Richieste di nuove autorizzazioni / licenze / certificazioni alla P.A.	TEMPESTIVO	Ufficio Gare e Supporto Legale Compliance
Presa visione MOG da parte dei dipendenti	SEMESTRALE	Direzione del Personale Coordinamento Compliance
Esiti procedimenti disciplinari	TEMPESTIVO	Direzione del Personale AD Compliance
Segnalazioni di violazioni del Modello o del Codice Etico o Whistleblowing (D.Lgs. 24/2023)	TEMPESTIVO	Coordinamento Compliance Direzione del Personale (segnalazioni HR)
Segnalazioni di criticità da parte dei lavoratori e dei Centri Operativi	TEMPESTIVO	responsabili dei Centri Operativi BU Delivery & Assurance
Atti, provvedimenti, indagini da Autorità / Procura / PG — notizie di indagini rilevanti ai fini 231	IMMEDIATO	AD Compliance Ufficio Gare e Supporto Legale

Oggetto del flusso informativo	Cadenza	Funzione competente
Provvedimenti interdittivi antimafia	TEMPESTIVO	AD Compliance Ufficio Acquisti
Gestione contenziosi giudiziali e notizie di indagini rilevanti ai fini 231	AD EVENTO	Ufficio Gare e Supporto Legale AD
Esiti delle Attività dell' <i>Internal Auditor</i>	AD EVENTO/ TEMPESTIVO (in particolare comunicazione degli esiti a sorpresa e delle ricerche antimafia)	Internal Auditor

Legenda cadenza dei flussi

IMMEDIATO	Entro 1-24 ore : flussi critici per la misura di prevenzione (atti giudiziari, infortuni gravi, operazioni sospette)
TEMPESTIVO	Entro 48 ore dall'evento : flussi rilevanti ai fini 231 e della misura di prevenzione
SEMESTRALE	Con cadenza semestrale: in regime AG la cadenza è raddoppiata rispetto al normale (da annuale a semestrale)
ANNUALE	Con cadenza annuale (bilancio, DVR)
AD EVENTO	Al verificarsi dell'evento: senza cadenza predefinita

2) Attività di coordinamento

A tal fine l'ODV:

- a. si coordina con le altre Funzioni Aziendali per:
 - i) il miglior monitoraggio delle attività più sensibili,
 - ii) la programmazione dell'informazione e della formazione del personale,
 - iii) l'adozione di eventuali sanzioni da parte della Direzione del personale,
 - iv) la diffusione più consona del Modello e del Codice Etico;
- b. formula all'Organo Dirigente le proposte di aggiornamento e adeguamento del Modello adottato a seguito di significative violazioni delle prescrizioni del Modello, di significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle proprie attività o a seguito di modifiche normative.

3) Attività di reporting

L'attività di *reporting* costituisce la sintesi delle attività poste in essere dall'OdV. I *report* indicheranno almeno:

- a. carenze, eccezioni, violazioni rilevate nel corso delle attività di verifica;
- b. suggerimenti, raccomandazioni per porre rimedio a quelle carenze ed eccezioni che non costituiscono violazioni;
- c. eventuali violazioni al Modello;
- d. proposte di modifiche, aggiornamento, implementazioni del Modello.

5.3. Reporting nei confronti dell'ODV

Dovrà essere portata a conoscenza dell'OdV (oltre alla documentazione prevista nella successiva Parte Speciale di cui al presente Modello) ogni altra informazione riguardante:

- le notizie e i documenti relativi ai procedimenti disciplinari azionati in relazione a notizia di violazione del Modello, alle sanzioni irrogate, ovvero ai provvedimenti di archiviazioni completi di motivazione;
- i provvedimenti e le notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, da cui si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D. Lgs. 231/2001;
- i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo da cui potrebbero emergere dei profili di criticità rispetto all'osservanza del Modello (ci si riferisce, per esempio, agli *audit* di qualità e sicurezza, alle verifiche contabili).

Deve essere portata a conoscenza dell'Organismo ogni informazione, di qualsiasi tipo, proveniente anche da terzi ed attinente all'attuazione del Modello nelle aree di attività a rischio. Al fine di facilitare il flusso di segnalazioni ed informazioni verso l'Organismo è stato istituito, quale canale dedicato di comunicazione con l'Organismo di Vigilanza.

6. WHISTLEBLOWING

Per *whistleblowing* si intende la segnalazione di presunti illeciti di cui si è venuti a conoscenza nell'ambito di un rapporto di lavoro. Si tratta di uno strumento volto alla garanzia della libertà di espressione e al contrasto dei fenomeni illeciti nelle organizzazioni pubbliche e private.

In Italia l'argomento era già stato affrontato in forma molto embrionale dalla l. 190/2012 e quindi dalla Legge 30.11.2017 n. 179, ma trova ora una più compiuta regolamentazione con il Decreto Legislativo 10 marzo 2023, n. 24, che ha recepito la direttiva UE 2019/1937 relativa alla protezione delle persone che segnalano violazioni del diritto dell'Unione.

La norma racchiude importanti cambiamenti di prospettiva sul whistleblowing introducendo nell'ordinamento giuridico italiano un apparato di obblighi a carico degli enti al fine di stabilire standard minimi comuni per assicurare la protezione delle persone che effettuano una segnalazione, attraverso canali di comunicazione sicuri, sia all'interno che all'esterno di un'organizzazione.

I destinatari della disciplina

Per quanto riguarda il settore privato la normativa si applica a:

- tutte le aziende con più di 250 dipendenti, a prescindere dall'adozione o meno di un Modello Organizzativo ex D.lgs. 231/2001;

- tutti i soggetti del settore privato che abbiano impiegato nell'ultimo anno una media di lavoratori subordinati tra i 50 e i 249, a prescindere dall'adozione o meno di un Modello Organizzativo ex D.lgs. 231/2001 nonché le aziende che pur non avendo un numero di dipendenti pari o superiore a 50 abbiano comunque un Modello Organizzativo ex D.lgs. 231/2001. Tutte le Società con meno di 50 dipendenti senza il Modello 231/2001 sono fuori dall'applicazione del Decreto.

Chi può segnalare?

L'ambito di applicazione soggettivo delle disposizioni del D.Lgs. 24/2023 è definito in senso ampio e comprende tutti i soggetti che, a qualsiasi titolo, abbiano acquisito le informazioni sulle violazioni in un contesto lavorativo. In particolare, sono legittimati a segnalare:

- lavoratori subordinati, dipendenti e collaboratori con rapporto di lavoro in corso;
- lavoratori autonomi, liberi professionisti e consulenti che operino nell'ambito di un rapporto contrattuale con la Società;
- tirocinanti, anche non retribuiti, e volontari;
- azionisti e persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza;
- soggetti candidati in fase di selezione precontrattuale, qualora le informazioni sulle violazioni siano state acquisite nel corso del processo di selezione o durante fasi precontrattuali, ancorché il rapporto non sia ancora formalmente instaurato (art. 3, co. 1, lett. a), D.Lgs. 24/2023);
- ex dipendenti, collaboratori e lavoratori il cui rapporto giuridico si sia successivamente sciolto, purché le informazioni sulle violazioni siano state acquisite prima della cessazione del rapporto (art. 3, co. 1, lett. b), D.Lgs. 24/2023).

Le medesime tutele previste per il segnalante si estendono ai c.d. *facilitatori*, ossia le persone fisiche che assistono il segnalante nel processo di segnalazione, operando nel medesimo contesto lavorativo, nonché ai colleghi di lavoro del segnalante che abbiano con lo stesso relazioni abituali nel contesto lavorativo, e ai parenti e conviventi del segnalante entro il quarto grado (art. 3, co. 5, D.Lgs. 24/2023). La Società garantisce che tali soggetti non siano destinatari di misure ritorsive in ragione dell'assistenza prestata al segnalante.

Quando si può segnalare?

Tutti i soggetti succitati rientrano nella categoria dei cosiddetti whistleblower e possono effettuare una segnalazione quando:

- il rapporto giuridico è in corso;
- quando il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
- durante il periodo di prova;
- successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite prima dello scioglimento (pensionati).

Cosa può essere segnalato?

Si possono segnalare le violazioni delle disposizioni normative nazionali e dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui i soggetti segnalanti siano venuti a conoscenza in un contesto lavorativo pubblico o privato.

Violazioni di disposizioni normative nazionali:

- condotte illecite rilevanti ai sensi del D. lgs. 231/2001 (i c.d. reati presupposto quali a titolo esemplificativo la corruzione, la frode informatica o il trasferimento fraudolenti di valori);
- violazioni dei Modelli di organizzazione gestione e controllo laddove previsti;

- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea relativi ai seguenti settori: appalti pubblici, servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; sicurezza degli alimenti, salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali; sicurezza delle reti e dei sistemi informativi;
- violazioni della normativa Antitrust.

Le segnalazioni possono avere oggetto anche:

- le informazioni relative alle condotte volte ad occultare le violazioni sopra indicate;
- le attività illecite non ancora compiute ma che il whistleblower ritenga ragionevolmente che possano verificarsi in presenza di elementi concreti precisi e concordanti;
- i fondati sospetti, la cui nozione dovrà essere oggetto di interpretazione.

Cosa non può denunciare il whistleblower o segnalante?

Le segnalazioni non possono riguardare le contestazioni legate a interessi di carattere personale del segnalante che attengono ai rapporti individuali di lavoro.

I canali di segnalazione

Secondo quanto previsto dalla direttiva, le segnalazioni possono essere effettuate attraverso i canali di segnalazione di seguito riportati:

- canale interno;
- canale esterno (gestito da ANAC);
- divulgazioni pubbliche;
- denuncia all'autorità giudiziaria o contabile.

Va notato che a scelta del canale di segnalazione non è rimessa alla discrezione del whistleblower in quanto in via prioritaria è favorito l'utilizzo del canale interno e, solo al ricorrere di una delle condizioni di cui all'art. 6, è possibile effettuare una segnalazione esterna.

Il sistema di protezione al segnalante

Il sistema di protezione ai segnalanti è volto soprattutto a garantire che il whistleblower non subisca ritorsioni, tra cui, ad esempio: il licenziamento; la sospensione; la retrocessione di grado; il mutamento di mansioni in peius; il cambiamento del luogo di lavoro; la riduzione dello stipendio; la modifica dell'orario di lavoro; la sospensione della formazione; le note di merito negative; l'adozione di misure disciplinari o di altra sanzione anche pecuniaria, ecc.

Inoltre, a beneficio del segnalante in buona fede, sono riconosciute anche la tutela della riservatezza, l'inversione dell'onere della prova e la Limitazioni della responsabilità.

Tali misure di protezione si applicano non solo ai segnalanti ma anche ai cosiddetti "facilitatori", colleghi, parenti o affetti stabili di chi ha segnalato.

Il canale interno di segnalazione *Whistleblowing* di Inpower Group è conforme alle disposizioni del D.Lgs. 24/2023 in materia di tutela delle persone che segnalano violazioni di normative nazionali o dell'Unione Europea.

Per la trasmissione e la gestione delle segnalazioni, la Società ha adottato una piattaforma informatica dedicata, accessibile al seguente link: [WhistleBlowing - Piattaforma per le segnalazioni](#)

Raccordo operativo con il canale di segnalazione 231

Il canale di segnalazione disciplinato dal presente paragrafo 6 ai sensi del D.Lgs. 24/2023 e il canale di segnalazione 231 di cui al successivo paragrafo 7 operano in modo distinto ma coordinato. Qualora una segnalazione ricevuta tramite la piattaforma *whistleblowing* abbia ad oggetto, in tutto o in parte, condotte illecite rilevanti ai sensi del D.Lgs. 231/2001, l'OdV è immediatamente coinvolto nella gestione della stessa, senza che ciò comporti la duplicazione del procedimento di indagine. In tali ipotesi trova applicazione il Protocollo di gestione di cui al paragrafo 7 per gli aspetti attinenti alla responsabilità amministrativa degli enti, ferme restando le garanzie di riservatezza e tutela del segnalante previste dal D.Lgs. 24/2023.

L'OdV e la funzione competente alla gestione del canale *whistleblowing* si coordinano tempestivamente per definire il perimetro dell'istruttoria e le rispettive competenze, assicurando in ogni caso la tracciabilità delle attività svolte e la separazione delle informazioni riservate dall'identità del segnalante.

7. SEGNALAZIONI 231 – PROTOCOLLO DI GESTIONE

Il presente Protocollo regola il processo di ricezione, analisi e gestione delle segnalazioni aventi ad oggetto condotte illecite rilevanti ai sensi del D.Lgs. 231/2001, effettuate da dipendenti o da qualsiasi altro soggetto che sia venuto a conoscenza di tali condotte in ragione delle funzioni svolte a favore della Società. Il canale di segnalazione 231 opera in modo distinto rispetto al canale *whistleblowing* di cui al precedente paragrafo 6, ferme restando le regole di raccordo operativo ivi previste per le segnalazioni a contenuto misto. Le segnalazioni devono essere circostanziate e fondate su elementi di fatto precisi e concordanti.

Contenuto delle Segnalazioni e Principi Generali

Le segnalazioni 231 dovranno avere per oggetto: condotte illecite rilevanti ai sensi del D. Lgs. 231 e del presente Modello circostanziate e fondate su elementi di fatto precisi e concordanti.

Il segnalante, in buona fede, viene protetto da ogni forma di ritorsione. Al contrario il segnalante che in mala fede invia una segnalazione consapevolmente falsa può essere soggetto ad un'azione disciplinare in accordo con la normativa del lavoro applicabile.

Invio delle Segnalazioni ex d.lgs. 231/2001

Le segnalazioni 231 devono essere inviate tramite la piattaforma pubblicata sul sito internet della Società: <https://www.inpowergroup.it/>.

Il segnalante, in buona fede, viene protetto da ogni forma di ritorsione. Al contrario il segnalante che in mala fede invia una segnalazione consapevolmente falsa può essere soggetto ad un'azione disciplinare in accordo con la normativa del lavoro applicabile.

Analisi Preliminare e Indagine

Una volta ricevuta la Segnalazione l'OdV coinvolge sin da subito le funzioni interne competenti, informando nel contempo il Consiglio di Amministrazione.

Qualora la Segnalazione venisse ritenuta verificabile, le funzioni competenti, unitamente all'OdV, definiscono un piano di lavoro allo scopo di verificare la fondatezza o meno dei contenuti con il coinvolgimento, se necessario, anche di consulenti esterni e/o esperti a supporto dell'indagine.

Reporting

Alla fine dell'indagine la funzione interna competente redige un report riepilogativo contenente:

- la descrizione di tutte le attività svolte

- i risultati
- il piano di azione conseguente

Una volta completato il *report* viene inviato all'OdV e all'organo amministrativo.

Archiviazione

Tutte le Segnalazioni, unitamente all'attività di reporting vengono archiviate dall'OdV garantendone tracciabilità e massimo livello di sicurezza, segretezza e confidenzialità.

Azioni Disciplinari

La Società potrà applicare le adeguate misure disciplinari, in accordo con quanto previsto nell'apposito documento allegato, al dipendente che dalle indagini risulti responsabile degli illeciti segnalati o che abbia minacciato o intimidito il segnalante in buona fede.

Nello stesso modo sarà soggetto ad azione disciplinare il segnalante che in mala fede abbia consapevolmente inviato una falsa Segnalazione.