



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
EX D.LGS. 8 GIUGNO 2001 N. 231

- PARTE GENERALE -

CLASSIFICAZIONE

PUBBLICO

REVISIONE

01

APPROVAZIONE

DELIBERA CdA DEL 19 OTTOBRE 2026

NATURA DELLA MODIFICA

APPROVAZIONE

ORGANIZZAZIONE

CLOUDFIRE S.R.L.

- PARTE GENERALE I -**IL QUADRO NORMATIVO****1 IL DECRETO LEGISLATIVO 8 GIUGNO 2001 N. 231****1.1. LA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI**

Il D.Lgs. 8 giugno 2001, n. 231, che reca la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (di seguito anche il "**D.Lgs. 231/2001**" o, anche solo il "**Decreto**"), entrato in vigore il 4 luglio 2001 in attuazione dell'art. 11 della Legge-Delega 29 settembre 2000 n. 300, ha introdotto nell'ordinamento giuridico italiano, conformemente a quanto previsto in ambito comunitario, la responsabilità amministrativa degli enti¹.

Tale nuova forma di responsabilità, sebbene definita "amministrativa" dal legislatore, presenta i caratteri propri della responsabilità penale, essendo rimesso al giudice penale competente l'accertamento dei reati dai quali essa è fatta derivare ed essendo estese all'ente le medesime garanzie riconosciute alla persona sottoposta alle indagini o all'imputato nel processo penale.

La responsabilità amministrativa dell'ente deriva dalla consumazione di reati, espressamente indicati nel D.Lgs. 231/2001, commessi:

- nel suo interesse² o a suo vantaggio³ (elemento oggettivo):

¹ L'art.1 del D.Lgs. n. 231 del 2001 ha delimitato l'ambito dei soggetti destinatari della normativa agli "enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica". Alla luce di ciò, la normativa si applica nei confronti degli:

- enti a soggettività privata, ovvero agli enti dotati di personalità giuridica ed associazioni "anche prive" di personalità giuridica;
- enti a soggettività pubblica, ovvero gli enti dotati di soggettività pubblica, ma privi di poteri pubblici (c.d. "enti pubblici economici");
- enti a soggettività mista pubblica/privata (c.d. "società miste").

Sono invece esclusi dal novero dei soggetti destinatari: lo Stato, gli enti pubblici territoriali (Regioni, Province, Comuni e Comunità montane), gli enti pubblici non economici e, in generale, tutti gli enti che svolgano funzioni di rilievo costituzionale (Camera dei deputati, Senato della Repubblica, Corte costituzionale, Segretariato generale della Presidenza della Repubblica, C.S.M., ecc.).

² L'interesse (da valutare *ex ante*) consiste nella prospettiva finalistica, da parte del reo-persona fisica che commette il reato, di conseguire un'utilità per l'ente a prescindere dall'effettivo conseguimento del beneficio per l'ente.

³ Il vantaggio (da valutare *ex post*), corrisponde all'effettivo conseguimento di un beneficio per l'ente senza che sia necessario che il reo-persona fisica abbia volontariamente commesso il reato allo scopo di conseguire un'utilità per l'ente.

- da persone funzionalmente legate all'ente (elemento soggettivo), ed in particolare:
 - a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (c.d. **soggetti apicali**);
 - b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a) (c.d. **soggetti sottoposti**).

La responsabilità dell'ente è esclusa laddove il reato sia stato posto in essere nell'esclusivo interesse dell'autore dell'illecito.

Oltre all'esistenza dei requisiti sopra descritti, il D.Lgs. 231/2001 richiede anche l'accertamento della colpevolezza dell'ente, al fine di poterne affermare la responsabilità. Tale requisito è riconducibile ad una "*colpa di organizzazione*", da intendersi quale mancata adozione, da parte dell'ente, di misure preventive adeguate a prevenire la commissione dei reati previsti dal Decreto da parte dei soggetti individuati.

Là dove l'ente sia in grado di dimostrare di aver adottato, ed efficacemente attuato, un'organizzazione idonea ad evitare la commissione di tali reati, attraverso l'adozione del modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001, questi non risponderà a titolo di responsabilità amministrativa.

1.2. I REATI PREVISTI DAL DECRETO

I reati, dal cui compimento è fatta derivare la responsabilità amministrativa dell'ente, sono quelli espressamente e tassativamente richiamati dal D.Lgs. 231/2001.

Si rimanda all'Allegato 1 del presente documento per il dettaglio delle singole fattispecie di reato attualmente ricomprese nell'ambito di applicazione del D.Lgs. 231/2001 ("**reati presupposto**") precisando, tuttavia, che si tratta di un elenco destinato ad ampliarsi costantemente.

1.3. LE SANZIONI COMMINATE DAL DECRETO

Il sistema sanzionatorio descritto dal D.Lgs. 231/2001, a fronte del compimento dei reati sopra elencati, prevede, a seconda degli illeciti commessi, l'applicazione delle seguenti sanzioni amministrative:

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

Le sanzioni pecuniarie:

Le sanzioni pecuniarie consistono nel pagamento di una somma di denaro nella misura stabilita dal Decreto, comunque non inferiore a euro 10.329 e non superiore a euro 1.549.370, da determinarsi in concreto da parte del Giudice mediante un sistema di valutazione bifasico (c.d. sistema "per quote").

Le sanzioni interdittive:

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 e sussidi, e/o revoca di quelli eventualmente già concessi;
- divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive si applicano, anche congiuntamente tra loro, esclusivamente in relazione ai reati per i quali sono espressamente previste dal Decreto, quando ricorre almeno una delle seguenti condizioni:

- a) l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da un soggetto apicale ovvero da un soggetto subordinato quando,

in quest'ultimo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;

b) in caso di reiterazione degli illeciti.

Quand'anche sussistano una o entrambe le precedenti condizioni, le sanzioni interdittive tuttavia non si applicano se sussiste anche solo una delle seguenti circostanze:

- a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; oppure
- b) il danno patrimoniale cagionato è di particolare tenuità; oppure
- c) prima della dichiarazione di apertura del dibattimento di primo grado, concorrono tutte le seguenti condizioni (qui di seguito, Condizioni ostative all'applicazione di una sanzione interdittiva):
 - 1) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
 - 2) l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di un Modello;
 - 3) l'ente ha messo a disposizione il profitto conseguito ai fini della confisca.

Le sanzioni interdittive possono essere applicate anche in via cautelare su richiesta al Giudice da parte del Pubblico Ministero, quando ricorrono le seguenti condizioni:

- sussistono gravi indizi per ritenere la sussistenza della responsabilità dell'ente a norma del Decreto;
- 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.

Il D.Lgs. 231/2001 prevede, inoltre, che qualora vi siano i presupposti per l'applicazione di una sanzione interdittiva che disponga l'interruzione dell'attività dell'ente, il giudice, in luogo dell'applicazione di detta sanzione, possa disporre la prosecuzione dell'attività da parte di un commissario giudiziale (art. 15 Decreto)

nominato per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni:

- l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;
- l'interruzione dell'attività può provocare rilevanti ripercussioni sull'occupazione tenuto conto delle dimensioni dell'ente e delle condizioni economiche del territorio in cui è situato.

La confisca

La confisca consiste nell'acquisizione coattiva da parte dello Stato del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato e fatti in ogni caso salvi i diritti acquisiti dai terzi in buona fede; quando non è possibile eseguire la confisca in natura, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

La pubblicazione della sentenza di condanna

La pubblicazione della sentenza di condanna consiste nella pubblicazione di quest'ultima una sola volta, per estratto o per intero, a cura della cancelleria del Giudice, a spese dell'ente, in uno o più giornali indicati dallo stesso Giudice nella sentenza, nonché mediante affissione nel Comune ove l'ente ha la sede principale.

La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva.

1.4. LA RESPONSABILITA' IN CASO DI VICENDE MODIFICATIVE DELL'ENTE

Il Decreto disciplina il regime della responsabilità dell'ente in caso di trasformazione, fusione, scissione e cessione.

In caso di trasformazione dell'ente resta ferma la responsabilità per i reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto. Il nuovo ente sarà quindi destinatario delle sanzioni applicabili all'ente originario, per fatti commessi anteriormente alla trasformazione.

In caso di fusione, l'ente risultante dalla fusione stessa, anche per incorporazione, risponde dei reati dei quali erano responsabili gli enti che hanno partecipato alla fusione. Se essa è avvenuta prima della conclusione del giudizio di accertamento della responsabilità dell'ente, il Giudice dovrà tenere conto delle condizioni economiche dell'ente originario e non di quelle dell'ente risultante dalla fusione.

Nel caso di scissione, resta ferma la responsabilità dell'ente scisso per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto; gli enti beneficiari della scissione sono solidalmente obbligati al pagamento delle sanzioni pecuniarie inflitte all'ente scisso nei limiti del valore del patrimonio netto trasferito ad ogni singolo ente, salvo che si tratti di ente al quale è stato trasferito anche in parte il ramo di attività nell'ambito del quale è stato commesso il reato. Le sanzioni interdittive si applicano all'ente (o agli enti) in cui sia rimasto o confluito il ramo d'attività nell'ambito del quale è stato commesso il reato. Se la scissione è avvenuta prima della conclusione del giudizio di accertamento della responsabilità dell'ente, il Giudice dovrà tenere conto delle condizioni economiche dell'ente originario e non di quelle dell'ente risultante dalla fusione.

In caso di cessione o di conferimento dell'ente nell'ambito della quale è stato commesso il reato, salvo il beneficio della preventiva escussione dell'ente cedente, il cessionario è solidalmente obbligato con l'ente cedente al pagamento della sanzione pecuniaria, nei limiti del valore dell'ente ceduto e nei limiti delle sanzioni pecuniarie che risultano dai libri contabili obbligatori o dovute per illeciti di cui il cessionario era comunque a conoscenza.

1.5. CONDIZIONE ESIMENTE DELLA RESPONSABILITÀ AMMINISTRATIVA

L'art. 6 del D.Lgs. 231/2001 stabilisce che l'ente non risponde a titolo di responsabilità amministrativa, qualora dimostri che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi (nel seguito anche il **"Modello"** o **"Modello 231"**);

- il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curarne il relativo aggiornamento, è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (nel seguito anche **"Organismo di Vigilanza"** o **"OdV"**);
- le persone hanno commesso il reato eludendo fraudolentemente il Modello (qualora il reato sia stato commesso da un soggetto apicale);
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

L'adozione del Modello 231 consente, dunque, all'ente di potersi sottrarre all'imputazione di responsabilità amministrativa. La mera adozione di tale documento, con delibera dell'organo amministrativo dell'ente, non è, tuttavia, di per sé sufficiente ad escludere detta responsabilità, essendo necessario che il modello sia efficacemente ed effettivamente attuato.

Con riferimento all'efficacia del modello di organizzazione, gestione e controllo per la prevenzione della commissione dei reati previsti dal D.Lgs. 231/2001, si richiede che esso:

- individui le attività aziendali nel cui ambito possono essere commessi i reati;
- preveda specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individui modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- preveda obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
- introduca un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Con riferimento all'effettiva applicazione del Modello, il D.Lgs. 231/2001 richiede:

- una verifica periodica, e, nel caso in cui siano scoperte significative violazioni delle prescrizioni imposte dal Modello o intervengano mutamenti nell'organizzazione o nell'attività dell'ente ovvero modifiche legislative, la modifica del Modello;

- l'irrogazione di sanzioni in caso di violazione delle prescrizioni imposte dal Modello 231.

1.6. IL BENEFICIO DELLA RIDUZIONE DELLA DURATA DELLE SANZIONI INTERDITTIVE

Il comma 5-*bis* dell'art. 25 del D.Lgs. 231/01, introdotto dalla Legge Anticorruzione n. 3/2019 *"Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici"*, prevede una riduzione delle sanzioni interdittive in caso di consumazione dei reati di concussione, induzione indebita a dare o promettere utilità o corruzione (per un termine compreso tra 3 mesi e 2 anni).

Il beneficio è riconosciuto all'ente che, prima dell'emissione della sentenza di primo grado 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, e si sia efficacemente adoperato:

- per evitare che l'attività delittuosa sia portata a conseguenze ulteriori;
- per assicurare le prove dei reati;
- per l'individuazione dei responsabili;
- per il sequestro delle somme o altre utilità trasferite.

1.7. LE "LINEE GUIDA" DI CONFINDUSTRIA

L'art. 6 del D.Lgs. 231/2001 dispone espressamente che i modelli di organizzazione, gestione e controllo possano essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti.

Ai fini della predisposizione del Modello, vengono quindi prese in considerazione le *"Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001"* (di seguito solo **"Linee Guida"**) redatte da Confindustria e da ultimo aggiornate nel giugno 2021.

Nella definizione del Modello di organizzazione, gestione e controllo, le Linee Guida di Confindustria prevedono le seguenti fasi progettuali:

- l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quali aree di attività e secondo quali modalità si possano verificare nel contesto aziendale i reati previsti dal D.Lgs. 231/2001;
- la predisposizione di un sistema di controllo idoneo a prevenire i rischi di reato identificati nella fase precedente, da effettuarsi attraverso la valutazione del sistema di controllo esistente e il relativo grado di adeguamento alle esigenze di prevenzione espresse dal D.Lgs. 231/2001.

Le componenti più rilevanti del sistema di controllo delineato nelle Linee Guida di Confindustria per garantire l'efficacia del modello di organizzazione, gestione e controllo sono di seguito riassunte:

- la previsione di principi etici e di regole comportamentali in un Codice Etico;
- un sistema organizzativo sufficientemente formalizzato e chiaro, in particolare con riguardo all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e alla descrizione dei compiti;
- procedure manuali e/o informatiche che regolino lo svolgimento delle attività, prevedendo gli opportuni e adeguati controlli;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali attribuite dall'ente, prevedendo, là dove opportuno, limiti di spesa;
- sistemi di controllo di gestione, capaci di segnalare tempestivamente possibili criticità;
- informazione e formazione del personale.

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

- verificabilità, tracciabilità, coerenza e congruità di ogni operazione, transazione e azione;
- applicazione del principio di separazione delle funzioni e segregazione dei compiti (nessuno può gestire in autonomia un intero processo);
- istituzione, esecuzione e documentazione dell'attività di controllo sui processi e sulle attività a rischio di reato;

- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure previste dal Modello;
- individuazione dei requisiti dell'Organismo di Vigilanza, riassumibili come segue:
 - autonomia e indipendenza;
 - professionalità;
 - continuità d'azione;
 - obblighi di informazione dell'Organismo di Vigilanza.

È opportuno evidenziare che la difformità rispetto a punti specifici delle diverse Linee Guida non inficia di per sé la validità del Modello. Il singolo Modello, infatti, dovendo essere redatto con riguardo alla realtà concreta dell'ente cui si riferisce, ben può discostarsi dalle Linee Guida che, per loro natura, hanno carattere generale.

1.8. EVOLUZIONE GIURISPRUDENZIALE

Ai fini della redazione del Modello, CloudFire Srl ha tenuto in considerazione le più importanti e recenti decisioni giurisprudenziali, tenendo conto dei principi dalle stesse affermati e degli orientamenti col tempo affermatisi.

- PARTE GENERALE II -**IL MODELLO ORGANIZZATIVO****2 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO****2.1. FINALITÀ DEL MODELLO**

CloudFire Srl (di seguito anche **"CloudFire"** o la **"Società"**) è una realtà specializzata nell'erogazione di servizi tecnologici avanzati, con particolare riferimento a soluzioni cloud, cybersecurity, infrastrutture digitali e servizi gestiti, rivolti a clienti pubblici e privati sull'intero territorio nazionale. Alla data di aggiornamento del presente Modello, l'attività prevalente della Società consiste nella fornitura di infrastrutture informatiche, servizi di hosting e attività connesse.

CloudFire si impegna a garantire il rispetto di un insieme di regole, principi e valori volti ad assicurare un'operatività efficace, trasparente e conforme alla normativa vigente, prevenendo comportamenti non corretti o la commissione di illeciti da parte di chiunque operi in nome e per conto della Società.

La Società provvede periodicamente all'identificazione e alla valutazione dei rischi rilevanti ai sensi del D.Lgs. 231/2001 e all'adeguamento dei propri presidi organizzativi e procedurali. Le risultanze delle attività di valutazione sono documentate e aggiornate secondo le procedure interne applicabili.

La Società riconosce il valore delle aspettative dei propri stakeholders ed è consapevole dei benefici derivanti dall'implementazione di un sistema di controllo interno efficace, volto a prevenire la commissione di reati da parte di dipendenti, componenti degli organi sociali, fornitori, consulenti, outsourcer e partner commerciali.

Attraverso l'adozione del Modello, la Società intende perseguire le seguenti finalità:

- vietare comportamenti che possano integrare le fattispecie di reato di cui al Decreto;
- determinare la piena consapevolezza in tutti coloro che operano in nome e per conto di CloudFire di poter incorrere in un illecito, la cui commissione è

fortemente censurata dalla Società, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, potrebbe trarne un vantaggio economico immediato;

- diffondere la consapevolezza che dalla violazione del Decreto, delle prescrizioni contenute nel Modello e dei principi del Codice Etico, possa derivare l'applicazione di misure sanzionatorie anche a carico della Società;
- consentire alla Società, grazie a un insieme di procedure e a una costante azione di monitoraggio sulla corretta attuazione di tale sistema, di prevenire e/o contrastare tempestivamente la commissione di reati rilevanti ai sensi del Decreto.

2.2. DESTINATARI

Le disposizioni del presente Modello sono vincolanti per **tutti i soggetti che, a vario titolo, operano nell'ambito dell'organizzazione CloudFire S.r.l.**, ovvero:

- membri del **Consiglio di Amministrazione** e, più in generale, tutti coloro che esercitano funzioni di **rappresentanza, amministrazione, direzione** o attività gestionali e di controllo, anche di fatto (apicali ai sensi del D.Lgs. 231/2001);
- i **dipendenti** (personale subordinato, incluso il personale con funzioni direttive/manageriali);
- i **collaboratori** che svolgono attività continuativa o parasubordinata a favore della Società (es. apprendisti, stagisti, figure junior inserite in percorsi formativi o professionalizzanti);
- soggetti terzi che operano su mandato, incarico o per conto di CloudFire nell'ambito di attività potenzialmente rilevanti ai sensi del D.Lgs. 231/2001.

Tutti i soggetti sopra indicati (di seguito, collettivamente, i **"Destinatari"**) sono tenuti a:

- rispettare pienamente le prescrizioni del Modello, del Codice Etico e delle procedure interne collegate;
- adottare comportamenti improntati a **lealtà, correttezza, trasparenza e diligenza** nello svolgimento delle proprie attività;

- contribuire attivamente alla prevenzione dei reati-presupposto e alla tutela dell'integrità, della reputazione e dell'operatività dell'azienda.

Il Modello è adottato come **strumento di prevenzione e sensibilizzazione** affinché i Destinatari siano consapevoli dei comportamenti potenzialmente idonei a integrare illeciti rilevanti ai sensi del D.Lgs. 231/2001 e assumano condotte conformi alla normativa e alle linee guida interne di CloudFire.

2.3. ELEMENTI FONDAMENTALI DEL MODELLO

Gli elementi fondamentali sviluppati da CloudFire S.r.l. nella definizione del presente Modello, in coerenza con il D.Lgs. 8 giugno 2001, n. 231 e con le Linee Guida di Confindustria, sono i seguenti:

- la periodica identificazione e valutazione delle attività e dei processi aziendali potenzialmente esposti al rischio di commissione dei reati-presupposto, secondo una metodologia proporzionata alla natura, alle dimensioni e alla struttura organizzativa della Società;
- l'adozione di principi di comportamento, procedure, protocolli e regole aziendali idonei a disciplinare lo svolgimento delle attività e a prevenire la commissione degli illeciti rilevanti ai sensi del Decreto;
- la previsione di modalità di gestione delle risorse finanziarie idonee a garantire la trasparenza, l'autorizzazione, la tracciabilità e la verificabilità delle operazioni;
- la verifica e la documentazione delle operazioni rilevanti, secondo criteri di tracciabilità, completezza, correttezza, coerenza e conservazione delle evidenze, in modo da garantire la trasparenza e la ricostruibilità dei processi decisionali e operativi;
- l'applicazione del principio di separazione delle funzioni e di segregazione dei compiti, assicurando un'adeguata distinzione tra funzioni operative, autorizzative e di controllo;
- l'attribuzione di ruoli, responsabilità e poteri coerenti con l'assetto organizzativo della Società, attraverso gli strumenti societari, organizzativi e procedurali applicabili e nel rispetto dei livelli autorizzativi e dei limiti operativi assegnati;
- la verifica periodica del funzionamento e dell'effettiva attuazione del Modello mediante controlli, monitoraggi e, ove opportuno, attività di audit, nonché

l'adozione delle necessarie misure correttive in caso di violazioni, inefficienze o mutamenti organizzativi, tecnologici o normativi;

- l'istituzione dell'Organismo di Vigilanza, configurato in forma monocratica e dotato di autonomi poteri di iniziativa e controllo, con il compito di vigilare sull'osservanza, sull'efficace attuazione e sull'adeguatezza del Modello e di formulare al Consiglio di Amministrazione proposte di aggiornamento e adeguamento;
- la previsione di obblighi informativi nei confronti dell'Organismo di Vigilanza, comprendenti flussi periodici e comunicazioni relative a eventi o circostanze rilevanti, secondo modalità e periodicità definite dalla Società;
- l'introduzione di canali interni di segnalazione idonei a garantire la riservatezza dell'identità della persona segnalante, della persona coinvolta, del facilitatore e degli eventuali ulteriori soggetti menzionati nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione, in conformità al D.Lgs. 10 marzo 2023, n. 24;
- l'adozione di un sistema sanzionatorio volto a garantire l'effettiva osservanza del Modello, del Codice Etico, delle procedure e dei protocolli aziendali, con misure proporzionate alla natura e alla gravità della violazione;
- la realizzazione di attività di informazione, comunicazione e formazione rivolte ai Destinatari, differenziate in funzione dei rispettivi ruoli, responsabilità e livelli di esposizione al rischio;
- la definizione di principi di comportamento e protocolli di controllo riferiti alle attività e ai processi aziendali potenzialmente esposti a rischio, disciplinati nella documentazione organizzativa e procedurale della Società;
- la previsione di un sistema di aggiornamento e tracciabilità documentale del Modello, mediante l'indicazione della versione, della data di adozione o aggiornamento, della sintesi delle modifiche e dell'organo deliberante, nonché mediante la conservazione delle relative evidenze e la comunicazione della versione vigente ai Destinatari.

2.4. CODICE ETICO

CloudFire S.r.l., sensibile all'esigenza di improntare lo svolgimento delle attività aziendali ai principi di **legalità, correttezza, integrità e trasparenza**, ha adottato un

Codice Etico (di seguito, il “**Codice**” o “**Codice Etico**”), quale documento di riferimento fondamentale per tutti coloro che operano nell’interesse della Società.

Il Codice esprime i **principi, i valori e le regole di condotta** che CloudFire riconosce come propri e che esige siano osservati:

- dagli organi sociali;
- da tutti i dipendenti, inclusi i dirigenti;
- dai collaboratori, consulenti, partner e fornitori che intrattengono rapporti professionali con la Società, anche in relazione alle attività aziendali potenzialmente esposte a rischio ai sensi del D.Lgs. 231/2001.

Il Codice Etico ha portata generale e rappresenta un insieme di regole che CloudFire **riconosce, accetta, condivide e applica**, al fine di:

- diffondere una solida cultura aziendale orientata all’etica, alla trasparenza e al rispetto delle leggi;
- promuovere comportamenti responsabili, corretti e professionali;
- tutelare gli interessi della Società, dei dipendenti, dei clienti, dei partner e di tutti gli stakeholder;
- preservare CloudFire da rischi di natura **legale, reputazionale e organizzativa**, coerentemente con il sistema di controllo interno delineato nel presente Modello 231

In considerazione del fatto che il Codice Etico richiama principi di comportamento – quali legalità, correttezza, trasparenza, tracciabilità (traceability), responsabilità e rispetto dei diritti delle persone – **idonei a prevenire** anche i comportamenti illeciti rilevanti ai sensi del D.Lgs. 231/2001, esso assume rilevanza diretta ai fini del presente Modello e costituisce, pertanto, **elemento complementare e integrante** del sistema di prevenzione adottato da CloudFire.

La violazione delle prescrizioni del Codice può integrare forme di comportamento non conformi ai principi del Modello 231 e costituisce, nei casi previsti, **infrazione disciplinare** perseguibile in base al sistema sanzionatorio descritto nel presente documento.

Il Codice Etico è portato a conoscenza di tutti i Destinatari ed è oggetto di attività

di **formazione e aggiornamento periodico**, coerentemente con i programmi previsti dalla Società in materia di cultura etica e compliance.

2.5. PERCORSO METODOLOGICO DI DEFINIZIONE DEL MODELLO: MAPPATURA DELLE ATTIVITÀ A RISCHIO-REATO - PROCESSI STRUMENTALI E PRESIDI

Il D.Lgs. 231/2001 richiede che il Modello individui le attività aziendali nell'ambito delle quali possono essere commessi i reati-presupposto.

A tal fine, CloudFire S.r.l. provvede periodicamente a identificare e valutare le attività e i processi aziendali potenzialmente esposti al rischio di commissione dei reati rilevanti ai sensi del Decreto, tenendo conto dell'evoluzione normativa, organizzativa, tecnologica e operativa della Società.

Sulla base delle risultanze della valutazione dei rischi, la Società individua e aggiorna i relativi principi di comportamento, protocolli di controllo, procedure e ulteriori presidi organizzativi. L'attività di valutazione è documentata secondo le procedure interne applicabili ed è sottoposta a periodico riesame, anche al fine di verificare l'adeguatezza e l'effettiva attuazione delle misure adottate.

La metodologia di valutazione è proporzionata alla natura, alle dimensioni e alla struttura organizzativa della Società e considera, tra gli altri elementi rilevanti, le attività svolte, i processi decisionali, i ruoli e le responsabilità, i flussi informativi e i controlli esistenti.

2.6. LA STRUTTURA DEL SISTEMA ORGANIZZATIVO E DI CONTROLLO

La Società disciplina l'attribuzione di ruoli, responsabilità e poteri attraverso il proprio assetto organizzativo, gli strumenti societari e le procedure applicabili, assicurando coerenza tra responsabilità assegnate, poteri autorizzativi e controlli.

Obiettivi del sistema organizzativo e di controllo

Il sistema organizzativo e di controllo attualmente in essere – inteso come insieme coordinato di strumenti, ruoli, responsabilità e presidi – garantisce il perseguimento dei seguenti obiettivi fondamentali:

- **efficacia ed efficienza** nell'utilizzo delle risorse aziendali, nella prevenzione delle perdite e nella tutela del patrimonio della Società;
- **conformità** a leggi, regolamenti e norme applicabili in tutte le operazioni svolte da CloudFire (compliance);
- **affidabilità e accuratezza delle informazioni** (reliable information), intese come comunicazioni tempestive, corrette e tracciabili, idonee ad assicurare la qualità dei processi decisionali.

Principi posti alla base del sistema dei controlli interni

I presidi di controllo, disciplinati da procedure e protocolli, si fondano sui seguenti principi:

- ogni operazione, transazione e azione deve essere **verificabile, documentata, coerente e congrua** (verifiable and properly documented);
- il sistema assicura – anche mediante una chiara attribuzione di poteri, deleghe e livelli autorizzativi – la **segregazione dei compiti** (segregation of duties), garantendo che nessun soggetto possa gestire un intero processo in autonomia;
- il sistema dei controlli interni prevede la **documentazione dell'esecuzione dei controlli**, inclusi i controlli di supervisione.

Struttura dei controlli aziendali

Il sistema dei controlli di CloudFire si articola in:

- **controlli di linea** (first-level controls), svolti dalle singole Direzioni/Funzioni sui processi di propria responsabilità, finalizzati ad assicurare il corretto svolgimento delle operazioni;
- **controlli verticali e funzionali** (functional oversight).

2.7. IL SISTEMA DI DELEGHE E PROCURE DELLA SOCIETÀ

La Società disciplina l'attribuzione di ruoli, responsabilità e poteri attraverso il proprio assetto organizzativo, gli strumenti societari e le procedure applicabili.

L'organizzazione aziendale è strutturata in modo da assicurare coerenza tra le responsabilità assegnate, i poteri autorizzativi e i relativi controlli, nel rispetto dei principi di separazione delle funzioni, segregazione dei compiti, tracciabilità e verificabilità delle attività.

Le attribuzioni di responsabilità e i livelli autorizzativi sono oggetto di aggiornamento in relazione all'evoluzione dell'organizzazione, delle attività e dei processi aziendali.

3 L' ORGANISMO DI VIGILANZA

L'art. 6, comma 1, del D.Lgs. 231/2001 richiede, quale condizione per beneficiare dell'esimente dalla responsabilità amministrativa dell'ente, che il compito di **vigilare sull'osservanza, sull'efficace attuazione e sull'aggiornamento del Modello 231** sia affidato a un **Organismo di Vigilanza (OdV)** dotato di **autonomi poteri di iniziativa e di controllo** (independent supervisory body), operante con continuità di azione.

L'Organismo di Vigilanza deve esercitare le proprie funzioni **al di fuori dei processi operativi della Società**, senza essere sottoposto a vincoli gerarchici nei confronti dei vertici aziendali o dei Responsabili di Direzione/Funzione, riferendo **periodicamente** al Consiglio di Amministrazione (Board of Directors).

In ossequio alle prescrizioni del Decreto, il **Consiglio di Amministrazione di CloudFire S.r.l.** ha nominato, con apposita deliberazione, l'**Organismo di Vigilanza monocratico**, al quale è attribuita piena autonomia funzionale e indipendenza nello svolgimento dei compiti di vigilanza.

La configurazione dell'OdV monocratico adottata dalla Società garantisce i requisiti previsti dalla normativa e dalle Linee Guida di Confindustria.

3.1. DURATA IN CARICA, DECADENZA E REVOCA

L'Organismo di Vigilanza resta in carica per il periodo determinato dal Consiglio di Amministrazione (Board of Directors) nella delibera di nomina. Alla scadenza del mandato, l'OdV **continua a operare in regime di prorogatio** sino alla nuova nomina da parte del CdA.

Composizione dell'Organismo di Vigilanza

Per CloudFire S.r.l., l'Organismo di Vigilanza è configurato in forma **monocratica** (single-member Supervisory Body), cui sono attribuiti autonomi poteri di iniziativa e di controllo.

Tale assetto risponde alle caratteristiche dimensionali e organizzative della Società, nonché ai requisiti previsti dal D.Lgs. 231/2001.

Requisiti dell'OdV monocratico

1) Autonomia e indipendenza (autonomy & independence)

Il requisito è garantito da:

- assenza di vincoli gerarchici verso il CdA o le Funzioni aziendali;
- accesso libero a documenti, dati, personale e informazioni rilevanti;
- dipendenza funzionale esclusiva dal CdA.

2) Professionalità (professional competence)

Il requisito deriva dalle competenze giuridiche, di controllo e di compliance maturate dal componente monocratico, nonché dalla conoscenza dei modelli organizzativi 231 e delle tecniche di vigilanza e monitoraggio.

3) Continuità d'azione (continuity of action)

L'OdV monocratico garantisce un presidio costante, attraverso:

- attività di vigilanza periodica e continuativa;
- poteri di indagine e accesso diretto alle informazioni;
- gestione dei flussi informativi (information flows);
- curatela dell'aggiornamento del Modello.

4) Cause di ineleggibilità e decadenza

Non può essere nominato OdV (e, se nominato, decade automaticamente):

- chi si trovi in situazioni di conflitto di interessi con la Società;
- chi ricopre incarichi esecutivi o operativi all'interno della Società;
- chi è legato da rapporti che pregiudichino autonomia e indipendenza;
- chi è destinatario di condanne – anche non definitive – per reati rilevanti ai sensi del D.Lgs. 231/2001;
- chi sia interdetto, inabilitato, fallito o privo dei requisiti di onorabilità.

Il componente monocratico deve comunicare tempestivamente al CdA l'insorgere di qualsiasi causa ostativa o incompatibilità.

5) Revoca

Il Consiglio di Amministrazione può revocare l'OdV **solo per giusta causa**, tra cui:

- grave violazione dei doveri di riservatezza;
- mancata comunicazione di situazioni di conflitto di interessi;
- inadempienze gravi nello svolgimento delle funzioni di vigilanza;
- condotte che pregiudichino l'autonomia o l'efficacia del ruolo.

La revoca senza giusta causa comporta il diritto dell'OdV a chiedere la **reintegrazione immediata**.

6) Recesso

L'OdV monocratico può recedere dall'incarico con preavviso scritto (notice) di almeno 30 giorni, da trasmettere al Legale Rappresentante tramite PEC o raccomandata A/R, affinché il CdA possa provvedere alle opportune determinazioni.

7) Regolamento di funzionamento

L'Organismo di Vigilanza disciplina autonomamente le modalità operative del proprio funzionamento in un **Regolamento interno** (OdV Internal Regulation), che viene trasmesso al Consiglio di Amministrazione per presa d'atto.

3.2. POTERI E FUNZIONI DELL'ORGANISMO DI VIGILANZA

L'**Organismo di Vigilanza di Cloudfire**, in composizione **monocratica**, è incaricato di:

- vigilare sulla diffusione all'interno della Società della conoscenza, della comprensione e dell'osservanza del Modello;
- vigilare sull'osservanza del Modello da parte dei Destinatari nell'ambito delle aree di attività potenzialmente a rischio di reato;
- vigilare sulla validità e adeguatezza del Modello, con particolare riferimento all'effettiva capacità del Modello di prevenire la commissione dei reati previsti dal D.Lgs. 231/2001;
- segnalare alla Società l'opportunità di aggiornare il Modello qualora si riscontrino esigenze di adeguamento in relazione a mutate condizioni aziendali e/o normative.

Nello svolgimento di dette attività, l'Organismo di Vigilanza provvede ai seguenti adempimenti:

- coordinarsi e collaborare con le **Funzioni aziendali** (anche attraverso riunioni) per il monitoraggio delle attività identificate nel Modello a rischio reato;
- effettuare verifiche mirate su operazioni o atti specifici posti in essere nell'ambito delle aree individuate a potenziale rischio di reato, anche con il supporto delle Funzioni aziendali;
- verificare l'effettivo svolgimento delle iniziative di informazione e formazione sul Modello intraprese dalla Società, supportando le Funzioni competenti nella verifica della relativa adeguatezza;
- verificare l'istituzione e il funzionamento di uno specifico canale informativo dedicato (es. indirizzo e-mail), diretto a facilitare il flusso di informazioni verso l'Organismo da parte delle Funzioni coinvolte nei processi potenzialmente a rischio di reato;
- segnalare tempestivamente al **Consiglio di Amministrazione** eventuali violazioni del Modello ritenute fondate, in particolare ove riferite ad Amministratori o soggetti apicali.

Ai fini dello svolgimento degli adempimenti sopra elencati, l'Organismo di Vigilanza è dotato dei poteri di seguito indicati:

- disciplinare le proprie attività e predisporre e aggiornare l'elenco delle informazioni e dei flussi informativi che devono pervenire all'Organismo di Vigilanza dalle funzioni aziendali;
- accedere, senza autorizzazioni preventive, a ogni documento aziendale rilevante per lo svolgimento delle funzioni attribuite dal D.Lgs. 231/2001;
- richiedere ai responsabili delle Funzioni aziendali e, in ogni caso, a tutti i Destinatari, informazioni, dati e notizie utili per individuare aspetti connessi alle attività rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso;
- ricorrere a consulenti esterni di comprovata professionalità qualora necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello.

Per un miglior svolgimento delle proprie attività, l'Organismo di Vigilanza può **avvalersi del supporto** delle Funzioni aziendali competenti e/o di consulenti esterni per specifiche attività istruttorie o di approfondimento, restando ferma la responsabilità dell'Organismo in ordine alle valutazioni e alle determinazioni assunte.

L'Organismo di Vigilanza dispone delle risorse necessarie allo svolgimento autonomo e indipendente delle proprie funzioni.

Oltre quanto sopra, in relazione all'entrata in vigore del **D.Lgs. 24/2023 (Whistleblowing)**, l'Organismo di Vigilanza è chiamato a:

- vigilare sull'implementazione da parte della Società di un **canale di segnalazione interna** e sulla sua rispondenza al D.Lgs. 24/2023, nonché sul conseguente aggiornamento del Modello in riferimento al canale stesso;
- vigilare sull'adozione da parte della Società di una **procedura Whistleblowing** ("Procedura Whistleblowing"), che disciplini la gestione delle segnalazioni interne (raccolta, gestione, istruttoria e archiviazione) effettuate tramite il canale interno;
- vigilare sulla formazione, informazione e diffusione di quanto previsto nel Modello e nella Procedura Whistleblowing;
 - vigilare sull'effettività e sull'accessibilità del canale di segnalazione interna;
- vigilare sul funzionamento del canale e sull'osservanza di quanto previsto nel Modello e nella Procedura Whistleblowing (es. verifiche a campione su

tempistiche di avviso di ricevimento e riscontro, presidi di riservatezza e divieto di ritorsione, eventuale applicazione del sistema disciplinare)

3.3. FLUSSI INFORMATIVI E REPORTING DELL'ORGANISMO DI VIGILANZA

Al fine di garantire piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'Organismo di Vigilanza di Cloudfire, in composizione monocratica, riferisce direttamente al Consiglio di Amministrazione.

In particolare, l'OdV riferisce sullo stato di attuazione del Modello 231 e sugli esiti dell'attività di vigilanza secondo le seguenti modalità:

- **periodicamente** al Presidente del Consiglio di Amministrazione / Legale Rappresentante, al fine di assicurare un costante allineamento con il vertice aziendale in merito alle attività svolte;
- **con cadenza annuale** al Consiglio di Amministrazione, mediante una **relazione scritta** che illustri le attività di monitoraggio svolte, le eventuali criticità emerse e gli interventi correttivi o migliorativi ritenuti opportuni ai fini dell'efficace attuazione e dell'aggiornamento del Modello.

L'OdV può essere convocato in qualsiasi momento dal Consiglio di Amministrazione e, a sua volta, può richiedere di essere sentito qualora ravvisi l'opportunità di riferire su aspetti inerenti al funzionamento e all'efficace attuazione del Modello o in relazione a situazioni specifiche.

Ai fini dello svolgimento delle verifiche e dell'esercizio delle proprie funzioni, l'OdV può richiedere chiarimenti e informazioni ai responsabili delle Funzioni interessate, nonché acquisire la documentazione ritenuta necessaria.

3.4. FLUSSI INFORMATIVI E SEGNALAZIONI NEI CONFRONTI DELL'ORGANISMO DI VIGILANZA

3.4.1. I flussi informativi verso l'Organismo di Vigilanza

Il D.Lgs. 231/2001, all'art. 6, comma 2, lett. d), richiede che il Modello preveda obblighi di informazione nei confronti dell'Organismo di Vigilanza (OdV) per consentirgli di assolvere efficacemente ai propri compiti.

A tal fine, tutti i Destinatari del Modello sono tenuti a fornire all'OdV, con tempestività e completezza, le informazioni rilevanti per l'attuazione del Modello stesso. I flussi informativi sono articolati in due categorie principali: **Flussi Informativi Periodici** e **Flussi Informativi su Evento**.

A) Flussi Informativi Periodici

I Destinatari sono tenuti a trasmettere all'Organismo di Vigilanza, secondo modalità e periodicità definite dalla Società, le informazioni rilevanti per la verifica dell'attuazione e dell'osservanza del Modello.

B) Flussi Informativi su Evento (Segnalazioni Occasionali)

Indipendentemente dai flussi periodici, i responsabili di funzione e tutti i Destinatari del Modello hanno l'obbligo di segnalare **immediatamente** all'OdV qualsiasi evento o situazione che possa avere rilevanza ai fini del D.Lgs. 231/2001.

C) Modalità di Trasmissione e Riservatezza

Tutti i flussi informativi e le segnalazioni destinate all'OdV devono essere trasmessi utilizzando il canale dedicato, al fine di garantirne la tracciabilità e la riservatezza. Le informazioni e la documentazione raccolte dall'OdV sono conservate in un archivio dedicato, con accesso riservato, per il tempo necessario all'espletamento delle sue funzioni e nel rispetto degli obblighi di legge.

D) Conseguenze della Violazione degli Obblighi Informativi

L'omessa o ritardata trasmissione delle informazioni dovute, così come la comunicazione di informazioni false o reticenti, costituisce una grave violazione del Modello di Organizzazione e Gestione e sarà sanzionata in conformità con quanto previsto dal Sistema Disciplinare.

Le informazioni e la documentazione acquisite dall'Organismo di Vigilanza sono trattate e conservate in modo riservato e tracciabile, nel rispetto della normativa applicabile.

3.4.2. Le segnalazioni (Whistleblowing)

CloudFire S.r.l. mette a disposizione delle persone legittimate a effettuare una segnalazione i canali e le modalità di tutela previsti dal D.Lgs. 10 marzo 2023, n. 24, dalla normativa applicabile e dalla Procedura Whistleblowing adottata dalla Società.

Sono previste le seguenti modalità:

- a) segnalazione attraverso il canale interno, in forma scritta o orale;
- b) segnalazione attraverso il canale esterno istituito e gestito dall'Autorità Nazionale Anticorruzione – ANAC, nei casi e alle condizioni previste dalla legge;
- c) divulgazione pubblica, nei casi e alle condizioni previste dalla legge;
- d) denuncia all'autorità giudiziaria o contabile competente, secondo quanto previsto dalla normativa applicabile.

La persona segnalante è invitata a utilizzare prioritariamente il canale interno. Il ricorso al canale esterno, alla divulgazione pubblica o alla denuncia resta consentito nei casi e alle condizioni stabiliti dalla legge e dalla Procedura Whistleblowing. La scelta del canale deve pertanto essere effettuata nel rispetto dei presupposti normativi applicabili.

a) Canale interno

Il canale interno è disponibile in forma scritta e orale ed è organizzato in modo da garantire, secondo le modalità previste dalla normativa applicabile, la riservatezza dell'identità della persona segnalante, della persona coinvolta, del facilitatore e degli eventuali ulteriori soggetti menzionati nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

La segnalazione scritta può essere effettuata mediante la piattaforma informatica dedicata, accessibile dalla sezione whistleblowing del sito istituzionale della Società. Le modalità di accesso alla piattaforma, di trasmissione della segnalazione e di verifica dello stato della relativa gestione sono indicate nella Procedura Whistleblowing e nella sezione dedicata del sito.

La segnalazione orale può essere effettuata mediante il canale telefonico o di messaggistica vocale dedicato indicato nella sezione whistleblowing del sito istituzionale e nella Procedura Whistleblowing. È inoltre possibile richiedere un incontro diretto con il gestore della segnalazione, che viene fissato entro un termine ragionevole secondo le modalità previste dalla Procedura Whistleblowing.

La registrazione della conversazione o la redazione del verbale dell'incontro sono effettuate nei casi, con le modalità e previo consenso previsti dalla normativa applicabile e dalla Procedura Whistleblowing.

La gestione delle segnalazioni interne è affidata all'Organismo di Vigilanza monocratico, quale soggetto individuato dalla Società ai sensi della Procedura Whistleblowing, nel rispetto dei requisiti di autonomia, imparzialità, indipendenza, riservatezza e adeguata formazione.

Qualora la segnalazione riguardi direttamente l'Organismo di Vigilanza, il suo componente, oppure sussista un conflitto di interessi anche potenziale, l'Organismo di Vigilanza si astiene dalla gestione della segnalazione. In tali casi la segnalazione è gestita dal Consiglio di Amministrazione o dal soggetto terzo appositamente individuato secondo quanto previsto dalla Procedura Whistleblowing. La gestione da parte di un soggetto in conflitto deve essere evitata, poiché non consentirebbe di assicurare un efficace seguito alla segnalazione.

L'Organismo di Vigilanza assicura il monitoraggio del funzionamento del canale interno e predispone, nel rispetto della riservatezza, una reportistica periodica in forma aggregata nei confronti del Consiglio di Amministrazione.

Il gestore della segnalazione fornisce alla persona segnalante l'avviso di ricevimento e il riscontro sul seguito dato alla segnalazione nei termini e con le modalità previsti dalla normativa applicabile e dalla Procedura Whistleblowing.

Il trattamento dei dati personali connesso alla gestione delle segnalazioni è effettuato nel rispetto del Regolamento (UE) 2016/679, del D.Lgs. 30 giugno 2003, n. 196, come modificato, del D.Lgs. 10 marzo 2023, n. 24 e della documentazione privacy adottata dalla Società.

b) Canale esterno gestito da ANAC

La persona segnalante può ricorrere al canale esterno istituito e gestito da ANAC nei casi e alle condizioni previste dall'art. 6 del D.Lgs. 10 marzo 2023, n. 24, tra cui l'assenza, l'inattivazione o la non conformità del canale interno, l'assenza di seguito a una segnalazione interna, il rischio di ritorsione o il fondato motivo di ritenere che la violazione costituisca un pericolo imminente o palese per il pubblico interesse.

Il canale esterno non costituisce un canale liberamente alternativo a quello interno, ma può essere utilizzato quando ricorrano i presupposti stabiliti dalla legge.

c) Divulgazione pubblica

La divulgazione pubblica consiste nel rendere di pubblico dominio informazioni sulle violazioni attraverso la stampa, mezzi elettronici o altri mezzi di diffusione idonei a raggiungere un numero elevato di persone.

La persona segnalante beneficia delle tutele previste dalla normativa applicabile quando la divulgazione pubblica è effettuata nel rispetto dei presupposti e delle condizioni stabiliti dal D.Lgs. 10 marzo 2023, n. 24.

d) Denuncia all'autorità competente

Resta ferma la facoltà della persona segnalante di presentare denuncia all'autorità giudiziaria o contabile competente, secondo quanto previsto dalla legge.

L'utilizzo del canale interno, del canale esterno o degli altri strumenti previsti dalla normativa whistleblowing non esclude eventuali obblighi di denuncia direttamente previsti dalla legge a carico di specifici soggetti.

4 COORDINAMENTO CON ALTRI SISTEMI DI GESTIONE

La Società coordina il presente Modello con gli altri sistemi di gestione e compliance adottati, nonché con le procedure e i protocolli aziendali applicabili.

Tale coordinamento riguarda, in particolare, i presidi relativi alla protezione dei dati personali, alla salute e sicurezza sul lavoro, alla tutela dell'ambiente e alla sicurezza delle informazioni.

I diversi sistemi e presidi aziendali concorrono, secondo le rispettive finalità e competenze, alla prevenzione dei rischi, alla corretta gestione dei processi e alla tracciabilità delle attività rilevanti ai sensi del D.Lgs. 231/2001.

5 IL SISTEMA SANZIONATORIO

Costituiscono violazioni rilevanti ai fini del presente sistema sanzionatorio le condotte poste in essere in violazione delle disposizioni applicabili in materia di salute e sicurezza sul lavoro, ove idonee a configurare reati-presupposto rilevanti ai sensi del D.Lgs. 231/2001. Le sanzioni sono applicate nel rispetto della normativa applicabile, dei contratti collettivi e delle regole aziendali vigenti, tenendo conto della gravità della condotta e del ruolo ricoperto dal soggetto responsabile.

Il mancato rispetto delle procedure, dei protocolli e delle regole aziendali adottati in attuazione del presente Modello costituisce violazione rilevante ai fini del sistema disciplinare. Le sanzioni sono applicate secondo criteri di proporzionalità e nel rispetto della normativa applicabile, dei contratti collettivi e dei rapporti contrattuali in essere.

Il mancato rispetto delle regole contenute nel Modello e nel Codice Etico può essere considerato nell'ambito della valutazione professionale del soggetto responsabile,

nei limiti e secondo le modalità previste dalla normativa applicabile, dalla contrattazione collettiva e dalla disciplina contrattuale vigente

6 DIFFUSIONE DEL MODELLO E FORMAZIONE

Con riguardo alla diffusione del Modello, del Codice Etico e della Procedura Whistleblowing, la Società, per il tramite delle funzioni competenti e/o del Presidente del Consiglio di Amministrazione, anche con il supporto dell'Organismo di Vigilanza, provvede a:

- comunicare ai Destinatari l'avvenuta adozione del Modello e del Codice Etico;
- rendere disponibili il Modello, il Codice Etico e la Procedura Whistleblowing mediante strumenti idonei;
- informare i Destinatari dell'esistenza e delle modalità di accesso ai canali interni di segnalazione;
- organizzare attività formative sui principi del D.Lgs. 231/2001, del D.Lgs. 24/2023, del Modello, del Codice Etico e della Procedura Whistleblowing;
- aggiornare le attività informative e formative in occasione di modifiche significative del Modello, della Procedura Whistleblowing o del quadro normativo applicabile.

7 ADOZIONE E AGGIORNAMENTO DEL MODELLO

L'adozione del Modello costituisce responsabilità del **Consiglio di Amministrazione di CloudFire S.r.l.**

Le successive modifiche e/o integrazioni di carattere **sostanziale** del presente Modello sono rimesse alla competenza del Consiglio di Amministrazione, mediante delibera assunta secondo le modalità previste per l'adozione del Modello stesso.

Tra le modifiche sostanziali si intendono ricomprese, a titolo esemplificativo, quelle conseguenti

a:

- significative violazioni delle previsioni del Modello;
- identificazione di nuove aree a rischio / attività sensibili e processi strumentali/funzionali alla commissione dei reati, connessi allo svolgimento di nuove attività da parte della Società o a variazioni di quelle precedentemente individuate;

- mutamenti dell'assetto organizzativo e/o del sistema di procure e deleghe che comportino impatti sul Modello;
- mutamenti del sistema di segnalazione interna e/o delle disposizioni di legge in materia di whistleblowing;
- identificazione di aree di miglioramento del Modello riscontrate dall'Organismo di Vigilanza a seguito delle periodiche attività di verifica.

Costituiscono in ogni caso modifiche sostanziali quelle che incidono sulla **composizione, durata in carica e operatività dell'Organismo di Vigilanza**, nonché sulle regole del **sistema sanzionatorio**.

L'**Organismo di Vigilanza** (in composizione monocratica) nell'ambito dei poteri previsti dall'art. 6, comma 1, lett. b) e dall'art. 7, comma 4, lett. a) del D.Lgs. 231/2001, è responsabile di sottoporre al Consiglio di Amministrazione proposte di aggiornamento e adeguamento del Modello.

Le modifiche, gli aggiornamenti e le integrazioni del Modello sono sempre portati a conoscenza dell'Organismo di Vigilanza.

Le procedure operative adottate in attuazione del presente Modello sono modificate dalle funzioni aziendali competenti qualora risultino inefficaci ai fini della corretta attuazione delle disposizioni del Modello. Le funzioni competenti provvedono a modificare o integrare le procedure al fine di rendere effettive le revisioni del Modello; l'Organismo di Vigilanza è tenuto informato dell'aggiornamento delle procedure esistenti e dell'adozione/attuazione di quelle nuove.

Qualora si rendano necessarie modifiche al Modello di natura esclusivamente **formale** (quali chiarimenti o precisazioni del testo), il **Legale Rappresentante**, su proposta o comunque sentito l'Organismo di Vigilanza, può provvedervi autonomamente. Di tali modifiche è data successiva comunicazione al Consiglio di Amministrazione nella prima seduta utile.

Le relazioni e le comunicazioni dell'Organismo di Vigilanza al Consiglio di Amministrazione sono trasmesse con modalità idonee a garantirne la certezza della ricezione e sono oggetto di verbalizzazione o di altra registrazione societaria

idonea. Le eventuali decisioni e azioni conseguenti sono monitorate dall'Organismo di Vigilanza nell'ambito dei successivi flussi di reporting.

In presenza di violazioni gravi, fatti urgenti o circostanze suscettibili di incidere sull'efficacia del Modello o sulla responsabilità della Società, l'Organismo di Vigilanza informa senza ritardo il Consiglio di Amministrazione, anche al di fuori della relazione periodica.

Il presente Modello è identificato da numero di versione e data di adozione/aggiornamento. Ogni revisione è tracciata in apposito Registro delle Revisioni (versione, data, sintesi delle modifiche, organo deliberante). La versione vigente è resa disponibile ai Destinatari con modalità idonee e tracciabili.

I Destinatari sono tenuti a trasmettere all'Organismo di Vigilanza, secondo modalità e periodicità definite dalla Società, le informazioni rilevanti per la verifica dell'attuazione e dell'osservanza del Modello.

Firmato digitalmente da: Roberto Bondavalli
Luogo: Reggio Emilia
Data: 19/10/2026 22:04:03