Sispi
Persone, Idee, Innovazione

Modello di Organizzazione Gestione e Controllo

Ai sensi del D.Lgs. 231/2001

Organizzazione
Controllo
Responsabilità

Revisione n.00		Approvata dal CdA	01.02.2005
Revisione n.01		Approvata dal CdA	28.01.2008
Revisione n.02		Approvata dal C.d.A	2009
Revisione n.03		Approvata dal C.d.A	26.01.2018
Revisione n.04		Approvata dal C.d.A	18.12 2023
Revisione n.05		Approvata dal C.d.A.	30.04.2026

INDICE

PREMESSA 5
CAPITOLO 1 7
REALTÀ AZIENDALE E MODELLO DI GOVERNANCE 7
1.1 Storia, natura giuridica e attività di SISPI 7
1.2 Struttura societaria e organizzazione 8
1.3 Sistema di deleghe e procure 10
CAPITOLO 2 11
DESCRIZIONE DEL QUADRO NORMATIVO 11
2.1 D.lgs. 175/2016 - Testo unico in materia di società a partecipazione pubblica 11
2.2 Il D.lgs. 231/2001 – la Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica 14
2.3 L'adozione del "Modello di Organizzazione Gestione e Controllo": prevenire il compimento di reati presupposto 23
2.4 Pubblica Amministrazione, pubblico ufficiale e persona incaricata di pubblico servizio 24
2.5 Governance in materia di cybersicurezza, sistema ISO/IEC 27001 e flussi informativi verso l'Organismo di Vigilanza 26
MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO SISPI: LA METODOLOGIA ADOTTATA 28
3.1 Metodologia adottata e fasi 28
3.1.1 Fasi 1 e 2 - Raccolta documentale, individuazione dei processi e coinvolgimento dei responsabili 29
3.1.2 Fase 3 - Gap Analysis 30
3.1.3 Fase 4 - Definizione e adeguamento dei protocolli di controllo 30
3.1.4 Fase 5 - Consolidamento, approvazione e attuazione del MOGC 31
CAPITOLO 4 32
L'ORGANISMO DI VIGILANZA AI SENSI DEL D.lgs. N. 231/2001 32
4.1 Individuazione dell'Organismo di Vigilanza (OdV) 32
4.2 Il Regolamento istitutivo dell'Organismo 34
4.3 Risorse economiche assegnate all'Organismo di Vigilanza 35
4.4 Funzioni e poteri dell'Organismo di Vigilanza 35
4.5 Funzioni dell'OdV: reporting nei confronti degli organi societari 36
CAPITOLO 5 38
FLUSSI INFORMATIVI NEI CONFRONTI DELL'OdV 38
5.1 Obblighi di informazione nei confronti dell'Organismo di Vigilanza 38

5.2 Sistema delle deleghe e delle procure ... 39
5.3 Raccolta e conservazione delle informazioni ... 39
CAPITOLO 6 ... 40
PIANO DI FORMAZIONE E DIVULGAZIONE ... 40
6.1 Premessa ... 40
6.2 Destinatari della divulgazione ... 41
6.3 Componenti degli organi sociali e soggetti con funzioni di rappresentanza ... 42
CAPITOLO 7 ... 43
SISTEMA DISCIPLINARE ... 43
7.1 Principi generali ... 43
7.2 Pubblicità ed efficacia ... 44
7.3 Principi generali di applicazione ... 45
7.4 Criteri di commisurazione ... 46
CAPITOLO 8 ... 48
MODELLO 231, SISTEMA ANTICORRUZIONE E TRASPARENZA, PIANO PERFORMANCE: IL SISTEMA INTEGRATO ... 48
8.1 Integrazione tra Modello 231 e PTPCT ... 48
8.2 Sistema di segnalazione delle violazioni (Whistleblowing) ... 49
CAPITOLO 9 ... 53
ADOZIONE DEL MODELLO e CRITERI DI AGGIORNAMENTO E ADEGUAMENTO ... 53
9.1 Aggiornamento ed adeguamento ... 53
APPENDICE A ... 54
CATALOGO DEI REATI-PRESUPPOSTO EX D.lgs. 231/2001 ... 54
ALLEGATI AL MOGC - DOCUMENTI SEPARATI
Allegato 1 - Codice Etico e di Comportamento
Allegato 2 - Sistema Disciplinare
Allegato 3 - Regolamento istitutivo dell'OdV
Allegato 4 - Regolamento Whistleblowing
Allegato 5 - Schema dei flussi informativi verso l'OdV

PREMESSA

Il presente Modello di Organizzazione, Gestione e Controllo (MOGC) costituisce la Parte Generale del sistema 231 di SISPI. La versione vigente è stata approvata dal Consiglio di Amministrazione il 30 aprile 2026 quale revisione del Modello adottato ai sensi dell'art. 6, comma 1, lett. a), del D.lgs. 231/2001, in ragione dell'evoluzione normativa e degli esiti delle verifiche periodiche sull'adeguatezza e sull'effettiva attuazione del sistema. La presente bozza ne propone l'aggiornamento normativo e redazionale alla data di agosto 2026. L'architettura del Modello è così composta:

- ***Parte Generale,*** *che definisce contesto aziendale, quadro normativo di riferimento e funzionamento dei principali strumenti di prevenzione del Modello stesso;*
- ***Parte Speciale****, di carattere operativo, che definisce attività a carico delle funzioni aziendali per competenza; a tali sezioni sono allegati i seguenti documenti:*
- ***Allegato 1 - Codice Etico e di Comportamento***
- ***Allegato 2 - Sistema Disciplinare***
- ***Allegato 3 - Regolamento istitutivo dell'OdV***
- ***Allegato 4 - Regolamento Whistleblowing***
- ***Allegato 5 - Schema dei flussi informativi verso l'OdV***

Il Modello configura un sistema strutturato e organico di regole, procedure, responsabilità e controlli finalizzato a prevenire, per quanto ragionevolmente possibile, la commissione dei reati rilevanti ai sensi del D.lgs. 231/2001. Esso si rivolge agli amministratori, ai dirigenti, ai dipendenti e, per quanto applicabile, a consulenti, collaboratori, fornitori e partner della Società.

L'individuazione delle attività a rischio-reato e la definizione di presidi di prevenzione consentono di accrescere la consapevolezza dei destinatari, assicurare la tracciabilità dei processi e favorire interventi tempestivi di prevenzione, rilevazione e risposta.

L'efficacia esimente del Modello presuppone non soltanto la sua adozione formale, ma soprattutto la sua effettiva attuazione, il costante monitoraggio e il tempestivo aggiornamento.

L'integrazione del MOGC con il sistema dei controlli interni, con il Codice Etico e di Comportamento e con gli ulteriori presidi di compliance rafforza la correttezza dei processi decisionali, la responsabilizzazione organizzativa e l'affidabilità della Società nei rapporti con il Socio, le amministrazioni, gli utenti e gli altri stakeholder.

CAPITOLO 1

REALTÀ AZIENDALE E MODELLO DI GOVERNANCE

1.1 Storia, natura giuridica e attività di SISPI

La SISPI Sistema Palermo Innovazione S.p.A. è stata **costituita nel 1988** (allora Sistema Palermo Informatica S.p.A.) su iniziativa del Comune di Palermo - allora socio di maggioranza - con la Finsiel S.p.A., per la progettazione, la realizzazione, lo sviluppo e la conduzione tecnica del Sistema Informatico e Telematico Comunale (SITEC).

Dal settembre 1990, SISPI è operativa quale partner tecnologico del Comune di Palermo per la progettazione e la realizzazione di soluzioni tecnologiche per l'innovazione dei processi amministrativi.

Dal maggio 2009 - anche in ragione delle norme nel frattempo intervenute col cd. "Decreto Bersani" (in particolare art. 13 del DL 233/2006, poi abrogato) **il capitale sociale di SISPI è stato interamente acquisito dal Comune di Palermo** (Delibera Consiglio Comunale n.26 del 5 marzo 2009), e, dal 2014, la società è stata inserita nell'"elenco ISTAT" che individua gli enti di natura privata, ricompresi nel conto economico consolidato dello Stato ai fini della quantificazione della spesa pubblica.

SISPI opera in regime di cd. "*in house providing*" fornendo servizi informatici strumentali al funzionamento del Comune di Palermo, socio unico, che esercita sulla Società il suo "controllo analogo", ai sensi del Testo Unico sulle Società Partecipate D.lgs. 175/16 e s.m. e i. (vedi infra), e del correlato Capo VI del Regolamento Unico dei controlli (cfr. Delibera Consiglio Comunale n. 4/2017, dedicato al "controllo sulle società partecipate non quotate". Il Regolamento dispone specifici strumenti di controllo societario, economico-finanziario, di efficienza, efficacia ed economicità della gestione, ispettivo e informativo declinando le modalità di esercizio dello stesso.

Dal febbraio 2020 la Società ha ampliato il suo raggio d'azione, integrando la gestione del SITEC con la realizzazione di soluzioni innovative e complesse rispondenti agli obiettivi di transizione digitale della città, condizione che ha determinato la scelta di ridefinire la denominazione societaria in **Sistema Palermo Innovazione S.p.A..**

Dal marzo 2024 i rapporti col soggetto controllante sono regolati da una Convenzione di durata novennale (2024-2033) per lo sviluppo e la conduzione tecnica del sistema informatico e dei sistemi di telecomunicazione comunali (SITEC) (cfr. Delibera Consiglio Comunale n. 17/2024).

Dal dicembre 2017 SISPI, conseguendo la UNI EN ISO 9001:2015[1], che sostituisce le precedenti certificazioni acquisite a partire dal 1998, ha avviato un complesso percorso di certificazione caratterizzato da estremo dinamismo col quale, alla data (30.04.2026), è stato realizzato un Sistema di Gestione Integrato costantemente manutenuto e gestito che garantisce la sicurezza del patrimonio informativo, la protezione dei dati, la salvaguardia dell'ambiente e per promuovere l'efficienza energetica, secondo gli standard internazionali EN/ISO (standard rappresenta un documento, approvato da un ente riconosciuto, che fornisce le regole, le linee guida o le specifiche tecniche per lo svolgimento di alcune attività). La conformità agli standard assicura che le performance, di solito variabili, possano diventare ripetibili.

L'elenco aggiornato delle certificazioni conseguite dall'Azienda è consultabile sulla pagina "Certificazioni" del sito istituzionale SISPI *www.sispi.it/certificazioni*

1.2 Struttura societaria e organizzazione

Il modello di Governance prevede, nel rispetto delle previsioni statutarie,

- Assemblea dei Soci
- Amministratore unico o Consiglio di Amministrazione
- Collegio Sindacale
- Revisore legale dei Conti nominato ai sensi del D.lgs. 39/2010.

I membri degli organi societari sono designati - previa istruttoria sul possesso dei requisiti richiesti a cura degli uffici competenti - con Determinazioni Sindacali sulla base delle quali l'Assemblea dei soci assume le connesse Deliberazioni ex art. 2449 c.c. Il

[1] relativa a "Progettazione, Sviluppo, Produzione e Manutenzione di Applicazioni Software e di Integrazione Sistemi in ambito ICT. Progettazione, Realizzazione ed Erogazione di: Servizi di Conduzione Operativa di Sistemi di Elaborazione dati e Reti di Telecomunicazione; Servizi di Conduzione Funzionale di Applicazioni Informatiche"

Revisore legale, nel rispetto delle previsioni di cui all'art. 13 D.lgs. 39/2010, viene nominato dall'Assemblea dei Soci su proposta motivata del Collegio sindacale.

Alla società ed ai suoi organi sociali e di controllo si applicano le previsioni del Codice civile e del TUSPP (D.lgs. 175/2016).

L'attività si svolge presso la sede acquisita dalla società nel giugno 2023 a Palermo in via Ammiraglio S. Denti di Piraino.

La struttura organizzativa di SISPI è attualmente articolata per Centri di Competenza, che non svolgono una funzione gerarchica ma, secondo criteri di omogeneità (cfr. OdS n. 1/2025), raccordano alla Direzione generale funzioni e servizi aziendali, secondo la seguente strutturazione:

CdC Servizi alla Direzione, che ingloba:

- *Segreteria di Presidenza e Protocollo*
- *Affari Legali e Contrattuali*
- *Affari Societari e assistenza agli Organi deliberativi;*
- *Relazioni esterne e Comunicazione*

CdC Pianificazione, Amministrazione e Controllo, che ingloba:

- *Risorse Umane, Formazione e Sicurezza sul Lavoro*
- *Amministrazione, Controllo di Gestione e Gestione Magazzino*
- *Acquisti*
- *Staff DG – Progetti di Offerta e Reporting*

CdC Tecnologie, che ingloba:

- *Sistemi e Sicurezza ICT (Architettura e Sistemi, Osservatorio ICT, Network e Telecomunicazioni, Gestione Tecnica-operativa DC)*
- *Sviluppo Soluzioni (Devops e System Integration, Piattaforme abilitanti Nazionali, Delivery Servizi, Manutenzione Software)*

CdC Customer Care, che ingloba:

- *Processi Interni, Certificazioni, Sede, CRM e Misura del Valore*
- *CRM, Contact Center, Customer Care*
- *Sistemi Periferici e Logistica (Sicurezza e Analisi 1° livello, Gestione Interventi,*

Stamperia e Logistica)

CdC Smart City, che ingloba:

- *Servizi di Livello Urbano*

CdC e-Government, che ingloba:

- *e-Government e Gestione Entrate*
- *Servizi alle Persone (Assistenza Sociale)*
- *Urbanistica/Sistemi Territoriali/Data Analisi*
- *Dematerializzazione Processi, Polizia Municipale e Cultura*

CdC Macchina Comunale, che ingloba:

- *Personale, CoGe, Bilancio (CoGe Bilancio, Personale)*
- *LL.PP., Uffici Tecnici*

1.3 Sistema di deleghe e procure

Ai sensi dell'art. 25 dello Statuto, l'organo amministrativo è investito dei più ampi poteri per la gestione ordinaria e straordinaria della società, senza eccezione di sorta, salvo quanto per legge è inderogabilmente riservato all'Assemblea dei soci ed agli Enti titolari di controllo analogo.

L'Assemblea dei Soci, come ricordato al superiore § 1.2, provvede alla nomina dell'Amministratore Unico o dei componenti del Consiglio di Amministrazione, e, in quest'ultimo caso, individua all'interno di quest'ultimo il Presidente ed occorrendo il Vice Presidente, carica attribuita solo per i casi di assenza o impedimento del Presidente, senza alcun compenso aggiuntivo.

L'Organo Amministrativo costituito in forma collegiale delibera l'assegnazione dei poteri all'interno del Consiglio e in capo al Direttore Generale.

Il Consiglio di Amministrazione può attribuire deleghe di gestione ad un solo amministratore fatte salve le deleghe attribuite al Presidente preventivamente autorizzate dall'Assemblea.

CAPITOLO 2
DESCRIZIONE DEL QUADRO NORMATIVO

2.1 D.lgs. 175/2016 - Testo unico in materia di società a partecipazione pubblica

L'intervento normativo operato dal ***Decreto legislativo 19 agosto 2016, n. 175***, nel riassumere in un unico quadro organico le numerose disposizioni vigenti in materia, ridisegna la disciplina al fine di razionalizzare il settore delle società a partecipazione pubblica, avendo riguardo ad un'efficiente gestione delle partecipazioni e quindi al contenimento della spesa pubblica. In particolare il testo si sviluppa sui seguenti **quattro** ambiti dispositivi:

1. **Introduttivo,** con l'indicazione di oggetto e ambito di applicazione;
2. **condizioni e limiti delle partecipazioni pubbliche**, con le regole per la costituzione di società o per l'assunzione o il mantenimento di partecipazioni societarie da parte di amministrazioni pubbliche e di alienazione di partecipazioni pubbliche;
3. **organi di amministrazione e di controllo delle società a controllo pubblico**, con riferimento a: requisiti dei componenti degli organi di amministrazione, compensi; regime di responsabilità degli enti pubblici partecipanti; regime di controllo, con riguardo ad attivazione del controllo giudiziario, prevenzione della crisi di impresa, controllo e monitoraggio da parte del MEF;
4. **incentivazione di economicità ed efficienza** con l'introduzione di procedure di razionalizzazione periodica e revisione straordinaria, di gestione del personale, di specifiche norme finanziarie per le partecipate degli enti locali e di promozione della trasparenza.

L'articolo 4 del Testo Unico fissa il **divieto** generale, per le amministrazioni pubbliche, di costituire, anche indirettamente, società aventi per oggetto attività di produzione di beni e servizi **non strettamente necessarie** per il perseguimento delle proprie finalità istituzionali, nonché di acquisire o mantenere partecipazioni, anche di minoranza, in tali società. Nei limiti di tale principio, lo stesso articolo 4 elenca le **finalità perseguibili** dalle amministrazioni mediante le società partecipate:

a. produzione di un servizio di interesse generale;

b. progettazione e realizzazione di un'opera pubblica sulla base di un accordo di programma fra amministrazioni pubbliche;

c. realizzazione e gestione di un'opera pubblica ovvero organizzazione e gestione di un servizio d'interesse generale attraverso un contratto di partenariato con un imprenditore privato selezionato secondo specifiche procedure;

d. **autoproduzione di beni o servizi strumentali all'Ente o agli enti pubblici partecipanti**;

e. servizi di committenza, ivi incluse le attività di committenza ausiliarie, apprestati a supporto di enti senza scopo di lucro e di amministrazioni aggiudicatrici.

SISPI, dunque, rientra nel novero dei soggetti di cui alla superiore lettera d).

L'articolo 16 del Testo Unico – *Società* in house

L'**art. 16** reca disposizioni sulle società *in house* coerenti con la normativa europea, recepita nel nostro ordinamento anche Codice dei Contratti pubblici, D.lgs. 36/2023, che prevede al c.2 dell'art. 7 recante "Principio di auto-organizzazione amministrativa" l'affidamento diretto alle società in house che sancisce un consolidato orientamento di giurisprudenza comunitaria.

In particolare, l'art. 16 del Testo unico prevede la disciplina di seguito enunciata con riferimento ai singoli commi:

- **comma 1**, subordina l'affidamento diretto di contratti pubblici alle società in *house* da parte di amministrazioni che esercitano su di esse il controllo analogo ovvero il controllo analogo congiunto alla condizione che non vi sia partecipazione di capitali privati[2], ad eccezione di forme di partecipazione che siano prescritte da norme di legge e che non comportino controllo o potere di veto, né l'esercizio di un'influenza

[2]La ratio della norma consiste nell'evitare che l'aggiudicazione di un affidamento diretto (in assenza quindi di una procedura competitiva) determini un indebito vantaggio in favore di operatori economici privati, titolari di una partecipazione nel capitale della società partecipata, ai danni degli altri operatori economici concorrenti e, al contempo, nell'evitare di sfavorire quelle realtà in cui la presenza di soggetti privati sia resa obbligatoria da una norma di legge, a condizione che siano rispettati i presupposti del controllo analogo della pubblica amministrazione.

determinante sulla società controllata.

- **comma 2**, conferisce agli statuti delle società *in house* facoltà di derogare ad alcune disposizioni del Codice Civile. In particolare: in deroga delle disposizioni sul sistema di *governance* tradizionale (art. 2380-bis) e dualistico (art. 2409- *novies*) che trovano fondamento nel ruolo penetrante di direzione e gestione svolto dalla P.A. nei confronti dell'organo di gestione, attraverso il cd. "controllo analogo".
- **comma 3**, dispone che gli statuti delle società *in house* debbano prevedere che almeno l'80% del loro fatturato afferisca ai servizi resi dall'Ente/i socio/i.
- **comma 4**. dispone che il mancato rispetto del suddetto limite dell'80% costituisce grave irregolarità, ai sensi dell'articolo 2409 del codice civile e dell'articolo 15 del decreto legislativo in esame.
- **comma 5**, dispone che, nel caso di mancato rispetto del richiamato limite di fatturato, la società possa sanare l'irregolarità se, entro tre mesi dalla data in cui la stessa si è manifestata, rinuncia una parte dei rapporti di fornitura con soggetti terzi, ovvero rinunci agli affidamenti diretti da parte dell'Ente o degli enti pubblici soci. Nell'uno e nell'altro caso la società è tenuta a sciogliere i relativi rapporti contrattuali.
- **comma 6**, prevede che, nel caso di rinuncia agli affidamenti diretti (di cui al comma 5), la società possa continuare la propria attività se e in quanto sussistano i requisiti previsti dall'articolo 4 per la costituzione di società partecipate. A seguito della cessazione degli affidamenti diretti, perdono efficacia le clausole statutarie e i patti parasociali finalizzati a realizzare i requisiti del controllo analogo.
- **comma 7**, prevede che le società *in house* provvedano all'acquisto di lavori, beni e servizi secondo la disciplina recata dal codice dei contratti pubblici.

L'articolo 19 del Testo Unico - Gestione del personale

In materia di gestione del **personale** delle società a controllo pubblico, l'art. 19 del TUSPP stabilisce - salvo specifiche disposizioni contenute nel medesimo provvedimento - che i rapporti di lavoro siano disciplinati dalle disposizioni vigenti per il settore privato, mentre al reclutamento si applichino i principi previsti per l'accesso alle

pubbliche amministrazioni.

Nel caso di SISPI si applicano - per quanto non espressamente disciplinato dal TUSPP - le disposizioni del Codice civile e le norme sui rapporti di lavoro subordinato nell'impresa, ivi incluse quelle in materia di ammortizzatori sociali, ai sensi della vigente normativa e del Contratto di riferimento che è il CCNL METALMECCANICI.

Vige, inoltre, uno specifico meccanismo di gestione dei processi di mobilità esplicitamente declinato in uno specifico Atto di indirizzo del Sindaco di Palermo recepito nel Regolamento sul Reclutamento attualmente vigente, che così recita:

"*nell'effettuazione di percorsi di selezione per il reclutamento di personale, si proceda, prioritariamente, attingendo alle professionalità ed ai profili presenti nel bacino complessivo del personale occupato nelle società partecipate, a parità di profilo e mansione ricercata, che siano disponibili ad effettuare una migrazione tra società con cessione del contratto di lavoro ai sensi dell'art. 1406 c.c. in presenza del consenso della società cedente il contratto di lavoro. In mancanza di copertura dei profili professionali attraverso la migrazione tra società. Procedere al reclutamento nel rispetto delle normative, nazionali e regionali, in materia di assunzione di personale nelle società partecipate. Ai fini dell'economicità e della rapidità di intervento, le Società potranno valutare di attingere ad eventuali graduatorie formate in un periodo precedente per i medesimi profili professionali già oggetto di precedenti migrazioni;*

che le Società effettuino i percorsi di reclutamento del personale, esclusivamente e limitatamente, per profili lavorativi indicati nel Piano di fabbisogno del personale" che annualmente la Società predispone nell'ambito della pianificazione industriali pluriennale.

2.2 Il D.lgs. 231/2001 – la Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica

Il D.lgs. 8 giugno 2001, n. 231, recante la «Disciplina della responsabilità amministrativa

delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300» (di seguito, il **Decreto**), ha introdotto una forma di responsabilità dell'ente qualificata dal legislatore come amministrativa, dipendente da reato e accertata nell'ambito del processo penale, autonoma rispetto alla responsabilità della persona fisica autrice del reato-presupposto.

Secondo tale disciplina, gli Enti possono dunque essere ritenuti responsabili e, conseguentemente, sanzionati, in relazione a taluni reati commessi o tentati, nell'interesse o a vantaggio dell'Ente stesso, dagli amministratori, dai dipendenti o da soggetti che operano per conto della Società.

Affinché sia punibile l'Ente, il reato deve essere commesso da persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente ovvero da persone sottoposte alla direzione o alla vigilanza delle prime.

L'Ente è quindi responsabile per i reati commessi (nel suo interesse o vantaggio) dai seguenti soggetti:

- **soggetti in posizione apicale**, con funzioni di rappresentanza, direzione, amministrazione, gestione e controllo, anche di fatto, dell'Ente (amministratori, direttori generali, liquidatori, socio unico, socio tiranno, amministratore di fatto), o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale (institori, direttori di stabilimento o ramo aziendale, responsabili di filiale): tali soggetti devono essere in concreto investiti di funzioni gestorie e di controllo, il che esclude la rilevanza dei reati posti ad esempio in essere dai revisori, dagli addetti all'internal auditing e sindaci;
- **soggetti sottoposti a direzione o vigilanza dei soggetti apicali** (c.d. soggetti sottoposti: dipendenti, collaboratori, agenti, franchisees, concessionari di vendita, ecc.): si tratta di soggetti che non rappresentano l'Ente, o comunque le cui scelte non determinano la politica aziendale, essendo esse stesse espressione ed attuazione di decisioni prese da un gruppo di comando al quale essi non partecipano.

L'esimente da responsabilità si atteggia diversamente a seconda che il reato sia stato commesso da un soggetto apicale o da un soggetto sottoposto.

a. **Qualora il reato sia stato commesso da soggetti apicali, anche se all'Ente non viene automaticamente attribuita la responsabilità del reato commesso dal proprio vertice, la colpevolezza organizzativa dell'Ente è presunta**, in quanto si ritiene che il loro operato, **dato il rapporto di immedesimazione organica con l'Ente**, sia espressione della politica dell'impresa; in questo caso opera una inversione dell'onere della prova e, dunque, ai fini della responsabilità dell'Ente l'accusa dovrà solo provare che:
   - è stato commesso uno dei reati-presupposto;
   - l'autore è una persona in posizione apicale;
   - il reato è stato commesso nell'interesse o a vantaggio dell'Ente.

   L'Ente dovrà invece dimostrare di avere adottato un efficace MOGC (mancanza di colpa da organizzazione), oppure che il comportamento del soggetto apicale è stato frutto di un comportamento fraudolento, cioè che tale soggetto abbia agito con la consapevolezza e la volontà di eludere, di "forzare" la rete di precauzioni che la Società si è imposta per impedire la commissione di quel reato, interrompendo così il legame tra la condotta del reo e l'Ente.
b. **Qualora, invece, il reato sia stato commesso da un soggetto sottoposto, spetta all'accusa l'onere della prova** e, pertanto, non soltanto la prova degli stessi fatti costitutivi previsti in caso di reato commesso dai vertici ma, anche, che il reato sia stato commesso a seguito dell'inosservanza degli obblighi di direzione e vigilanza sull'operato del subordinato da parte dei vertici. **L'Ente sarà invece esente da responsabilità qualora dimostri di avere adottato ed efficacemente attuato un MOGC idoneo alla prevenzione del reato**.

   In questo caso, dunque, la c.d. colpa organizzativa dell'Ente (l'inosservanza degli obblighi di direzione e vigilanza sul sottoposto che ha commesso il reato) deve essere provata dal PM, poiché non vige alcuna presunzione di riferibilità del reato all'Ente. Qualora l'Ente dimostri di avere adottato un MOGC idoneo ed efficace, non

è possibile richiamare l'inosservanza degli obblighi di direzione e vigilanza.

Il catalogo sintetico delle fattispecie di reato-presupposto rilevanti ai sensi del D.lgs. 231/2001 e delle ulteriori disposizioni richiamate è riportato nell'Appendice A, che costituisce parte integrante del presente Modello.

Evoluzione normativa recente rilevante ai fini del Modello

Il catalogo dei reati-presupposto e i relativi apparati sanzionatori sono oggetto di continua evoluzione. Ai fini del presente aggiornamento, assumono particolare rilievo le modifiche intervenute dal 2024 al 2026, da recepire nella mappatura dei rischi e, ove pertinenti, nelle Parti Speciali e nei protocolli di controllo.

La Legge 28 giugno 2024, n. 90 ha inciso sull'art. 24-bis del D.lgs. 231/2001, rafforzando il trattamento sanzionatorio dei delitti informatici e introducendo ulteriori fattispecie rilevanti. Tali modifiche assumono particolare rilievo per SISPI in considerazione della natura ICT delle attività svolte.

Il D.L. 4 luglio 2024, n. 92, convertito con modificazioni, ha modificato l'art. 25 del D.lgs. 231/2001, anche in conseguenza dell'abrogazione dell'abuso d'ufficio e dell'introduzione di nuove fattispecie contro la Pubblica Amministrazione.

Il D.lgs. 26 settembre 2024, n. 141 ha modificato l'art. 25-sexiesdecies in materia di contrabbando, nell'ambito della revisione della disciplina doganale e delle accise.

Il D.lgs. 4 settembre 2024, n. 138, di recepimento della Direttiva (UE) 2022/2555 (NIS2), pur non configurando di per sé un autonomo catalogo di reati-presupposto 231, rafforza gli obblighi di governance, gestione del rischio e sicurezza dei sistemi informativi. Per SISPI, destinataria della specifica comunicazione ACN richiamata al § 2.5, tali obblighi costituiscono un elemento rilevante del sistema di controllo interno e della prevenzione dei reati informatici.

Nel 2025 il catalogo 231 è stato ulteriormente ampliato, tra l'altro con l'introduzione dell'art. 25-undevicies relativo ai delitti contro gli animali. L'aggiornamento della Parte Speciale deve essere effettuato secondo il criterio di effettiva pertinenza rispetto alle attività della Società.

Nel 2026 sono intervenute ulteriori modifiche. Il D.lgs. 21 aprile 2026, n. 81, di attuazione della Direttiva (UE) 2024/1203 sulla tutela penale dell'ambiente, ha modificato l'art. 25-undecies del D.lgs. 231/2001, ampliando e rimodulando le fattispecie e le sanzioni in materia ambientale. La Legge 21 aprile 2026, n. 75, recante «Disposizioni sanzionatorie a tutela dei prodotti alimentari italiani», ha modificato l'art. 25-bis.1, comma 1, lettera a), del D.lgs. 231/2001, inserendo il richiamo all'art. 517-octies, quarto comma, c.p. Tali novità devono essere considerate nel risk assessment anche quando il rischio inerente risulti basso o solo indiretto.

L'aggiornamento del MOGC deve pertanto essere inteso come processo continuo: ogni modifica normativa rilevante è sottoposta a valutazione di impatto rispetto ai processi aziendali, ai protocolli esistenti, ai flussi verso l'OdV, al sistema disciplinare e alla formazione.

Le sanzioni

Il Decreto 231 prevede un articolato quadro di sanzioni per l'Ente che non abbia adottato un valido ed efficace MOGC, in caso di reati-presupposto commessi da apicali o sottoposti a suo vantaggio o nel suo interesse.

Il sistema per quote costituisce il criterio generale di determinazione della sanzione pecuniaria. Il numero delle quote e la cornice sanzionatoria applicabile dipendono tuttavia dalla singola fattispecie di reato-presupposto, nel rispetto dei limiti generali previsti dal D.lgs. 231/2001. La determinazione si articola in due fasi:

1. il giudice determina il numero delle quote entro la cornice prevista per la specifica fattispecie, tenendo conto della gravità del fatto, del grado di responsabilità dell'Ente e dell'attività svolta per eliminare o attenuare le conseguenze del fatto e prevenire ulteriori illeciti;
2. il giudice determina il valore monetario della singola quota, da euro 258,23 a euro 1.549,37, in considerazione delle condizioni economiche e patrimoniali dell'Ente. L'importo finale deriva dal prodotto tra il numero di quote stabilito per il caso concreto e il valore attribuito a ciascuna quota; non esiste quindi un'unica cornice

pecuniaria valida per tutti i reati-presupposto.

La sanzione può essere ridotta, fino a 2/3, in una serie di casi, ovvero qualora:

- sia accertato il prevalente interesse dell'autore del reato e nessuno o scarso vantaggio per l'Ente;
- il danno patrimoniale sia di lieve entità;
- il danno patrimoniale sia stato risarcito;
- sia stato adottato, dopo la commissione del reato, un efficace MOGC.

Accanto alle sanzioni pecuniarie, il dettato del D.lgs. 231/2001 prevede, per i reati e nei casi espressamente stabiliti e alle condizioni stabilite dall'art. 13[3], sanzioni interdittive idonee a incidere direttamente sull'operatività dell'Ente, quali:

- interdizione dell'esercizio dell'attività d'impresa;
- sospensione o revoca di autorizzazioni e licenze;
- divieto di contrattare con la P.A.;
- esclusione e revoca, di finanziamenti, sussidi, contributi, agevolazioni;
- divieto di pubblicizzare beni e servizi.

Il giudice ne determina il tipo e la durata in base ai criteri individuati per le sanzioni pecuniarie (gravità del fatto, grado di responsabilità dell'Ente, attività svolta per limitare i danni e prevenire futuri illeciti), tenendo conto dell'idoneità a prevenire illeciti del tipo di quello commesso.

La durata delle sanzioni interdittive è determinata secondo la disciplina generale e le eventuali disposizioni speciali applicabili alla specifica fattispecie; in casi tassativamente previsti[4], include anche ipotesi di interdizione definitiva.

[3] Nei casi in cui:
- l'Ente ha tratto dal reato un profitto di rilevante entità;
- il reato è stato commesso da soggetti apicali o da sottoposti a causa di gravi carenze organizzative;
- vi è un pericolo di reiterazione degli illeciti.

[4] Nei casi in cui
- All'Ente siano state già applicate temporaneamente 3 volte in 7 anni;
- l'Ente ha come scopo principale il compimento di reati.

Qualora l'Ente svolga un pubblico servizio o un servizio di pubblica necessità, la cui interruzione è pregiudizievole per la collettività o quando si prospettano rilevanti ripercussioni sull'occupazione, tenuto conto delle dimensioni dell'Ente e del territorio in cui è situato, il giudice, invece di erogare la sanzione cautelare interdittiva, può nominare un commissario giudiziale, dotato di specifici compiti e poteri, tra i quali la prosecuzione dell'attività, l'adozione e l'efficace attuazione di un MOGC idoneo a prevenire ulteriore commissione di reati.

Le sanzioni interdittive possono anche essere applicate anche in via cautelare, qualora ricorrano i seguenti presupposti:

- il *fumus commissi delicti*, e cioè una probabilità qualificata e ragionevole della sussistenza nel caso di specie del reato;
- il *periculum in mora*, e cioè la sussistenza di fondati e specifici elementi circa la probabilità effettiva ed attuale della ripetibilità di reati della stessa specie di quello per cui si procede.

La misura cautelare può essere sospesa se l'Ente chiede di poter adottare le condotte "riparatorie" e quindi di procedere agli adempimenti cui la legge condiziona l'esclusione della sanzione (risarcimento integrale del danno, eliminazione delle conseguenze dannose o pericolose ovvero efficace adoperarsi a tal fine, superamento delle carenze organizzative che hanno determinato il reato con l'adozione e l'attuazione di idoneo MOGC, messa a disposizione del profitto conseguito ai fini della confisca).
In caso di condanna dell'Ente è disposta la confisca del prezzo o del profitto del reato, salvo che per la parte restituibile al danneggiato; quando non è possibile eseguirla direttamente, può operare la confisca per equivalente nei limiti previsti dal Decreto.

Può essere disposta la confisca:

- del prezzo (denaro o altra utilità data o promessa per indurre a commettere il reato) o del profitto (utilità economica immediata ricavata dal reato) dei reati commessi nell'interesse o a vantaggio dell'Ente
- di denaro, beni o altre utilità di valore equivalente, salvo che per la parte che può essere restituita all'eventuale soggetto danneggiato.

In fase cautelare, può essere concesso il sequestro preventivo dei beni (prezzo, profitto, denaro o altre utilità) per i quali è consentita la confisca, senza necessità di provare una pericolosità connessa alla libera disponibilità dei beni stessi.

Le misure interdittive non si applicano se prima del processo l'Ente abbia posto in essere tutte le seguenti condotte riparatorie:

- **abbia risarcito il danno ed eliminato le conseguenze;**
- **abbia adottato un MOGC *post factum* idoneo a prevenire i reati della stessa specie;**
- **abbia messo a disposizione il profitto conseguito ai fini della confisca.**

Le Linee Guida e i contributi elaborati dal CNDCEC, dalle associazioni di categoria e da Confindustria

Nella predisposizione e nell'aggiornamento dei Modelli di organizzazione, gestione e controllo assumono rilievo, quali autorevoli riferimenti metodologici e interpretativi, i documenti elaborati dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (CNDCEC), anche con il supporto della Fondazione Nazionale dei Commercialisti, nonché le Linee Guida e i documenti di indirizzo emanati dalle principali associazioni di categoria, tra le quali particolare rilievo rassumono quelli predisposti da Confindustria.

Tra i contributi del **CNDCEC** maggiormente significativi ai fini dell'evoluzione dei sistemi di compliance ex D.lgs. 231/2001 si richiamano, oltre ai "Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'Organismo di Vigilanza" pubblicati nel 2019, i seguenti documenti:

2023

- "*Nuova disciplina del Whistleblowing e impatto sul D.lgs. 231/2001*", che chiarisce il legame tra le due discipline con particolare riferimento all'integrazione dei canali di segnalazione, delle misure di tutela e del sistema disciplinare nel MOGC;
- "*MOGC ex D.lgs. 231/2001 nelle società sottoposte a misure di prevenzione CAM*",

dedicato al Modello 231 quale strumento di prevenzione, rafforzamento organizzativo e recupero della legalità;

2025

- "*Rischio di infiltrazioni criminali e «self cleaning» preventivo: il ruolo del modello 231*" sui sistemi di prevenzione e gestione del rischio di condizionamento criminale;
- "*Riforma del D.lgs. 231/2001: osservazioni e proposte*", utile ai fini dell'interpretazione evolutiva della disciplina della responsabilità degli enti;
- le "*Linee Guida per lo svolgimento delle funzioni dell'Organismo di Vigilanza ex D.lgs. 231/2001*", che sistematizzano principi e criteri operativi relativi a composizione, autonomia, indipendenza, professionalità, continuità di azione, pianificazione della vigilanza, flussi informativi e reporting dell'OdV.

Per quanto concerne Confindustria, restano un fondamentale parametro metodologico le «Linee Guida Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001», aggiornate a giugno 2021 e approvate dal Ministero della Giustizia. Le Linee Guida valorizzano un approccio basato sulla preventiva identificazione dei rischi, sulla progettazione di specifici protocolli di controllo e sull'integrazione del Modello 231 con gli ulteriori sistemi di compliance aziendale. Esse hanno inoltre recepito l'evoluzione della disciplina in materia di whistleblowing, anticorruzione e nuove fattispecie di reato-presupposto.
A tali riferimenti si affiancano i successivi documenti applicativi predisposti da Confindustria, tra i quali, per i profili rilevanti ai fini del presente Modello, la procedura in materia di whistleblowing aggiornata al D.lgs. 24/2023 già oggetto dell'intervento del CNDCEC sopra richiamato.

Alla luce di tali contributi, il processo di predisposizione e aggiornamento del MOGC può essere ricondotto, in sintesi, alle seguenti attività fondamentali:

- **analisi della struttura organizzativa, dei processi e delle peculiarità dell'ente;**
- **individuazione delle attività sensibili e valutazione dei rischi di commissione dei reati-presupposto;**

- **analisi del sistema dei controlli esistenti e individuazione degli eventuali gap;**
- **definizione o adeguamento dei protocolli di prevenzione;**
- **attribuzione coerente di ruoli, responsabilità, deleghe e poteri;**
- **previsione di adeguati flussi informativi, strumenti di monitoraggio e meccanismi di aggiornamento del Modello.**

Le componenti essenziali del sistema di controllo preventivo comprendono, tra l'altro, il Codice Etico, il sistema organizzativo, le procedure operative e informatiche, il sistema di deleghe e procure, i controlli sulla gestione delle risorse finanziarie, il sistema disciplinare, la formazione e la comunicazione, nonché un Organismo di Vigilanza dotato dei requisiti di autonomia, indipendenza, professionalità e continuità di azione.

Tali componenti devono essere improntate ai principi di tracciabilità e documentabilità delle operazioni, segregazione delle funzioni, coerenza tra poteri e responsabilità, documentazione dei controlli e adeguatezza dei flussi informativi verso l'Organismo di Vigilanza.

2.3 L'adozione del "Modello di Organizzazione Gestione e Controllo": prevenire il compimento di reati presupposto

L'articolo 6 del Decreto introduce una particolare forma di esonero dalla responsabilità in oggetto qualora l'Ente dimostri:

a) di aver adottato ed efficacemente attuato attraverso il suo organo dirigente, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
b) di aver affidato ad un organismo interno, dotato di autonomi poteri d'iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza dei modelli, nonché di curare il loro aggiornamento;
c) che le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti modelli di organizzazione e di gestione;

d) che non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

Il Decreto prevede, inoltre, che – in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati – i modelli debbano:

- **individuare le attività nel cui ambito possono essere commessi reati;**
- **prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;**
- **individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;**
- **prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;**
- **introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.**

Ai sensi dell'art. 6, comma 2-bis, del D.lgs. 231/2001, come modificato dal D.lgs. 24/2023, il Modello deve inoltre prevedere, in conformità alla disciplina whistleblowing, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare. La disciplina di dettaglio è richiamata al paragrafo 8.2 oltreché nel Regolamento Whistleblowing aziendale.

Secondo quanto previsto dal Decreto i modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (o anche Linee Guida) redatti dalle associazioni rappresentative di categoria, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro trenta giorni, osservazioni sull'idoneità dei modelli a prevenire i reati.

2.4 Pubblica Amministrazione, pubblico ufficiale e persona incaricata di pubblico servizio

Considerato che nell'ambito delle categorie di reati presupposto del Decreto rientrano reati contro la PA, alcuni dei quali cd. Reati "propri" (*quelli che possono essere commessi solamente da soggetti che rivestono particolari qualifiche soggettive, status,*

condizione, posizione, qualità personale, che li pongono in un particolare rapporto con l'interesse protetto dalla norma), **si ritiene utile ausilio alla lettura e comprensione del presente Modello richiamare le seguenti definizioni**

Pubblica Amministrazione

Per Pubblica Amministrazione si intendono tutti quei soggetti, privati e di diritto pubblico, italiani o europei, che svolgano una "funzione pubblica" o un "pubblico servizio".

Funzione pubblica e pubblico ufficiale

Per funzione pubblica si intende, nel diritto, lo svolgimento di un'attività nell'interesse della collettività (interesse pubblico) da parte di enti pubblici o locali, e consiste in un'attività retta da norme di diritto pubblico o da atti autoritativi.

Ai sensi dell'art. 357 del codice penale sono pubblici ufficiali "coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa".

Il pubblico ufficiale esercita la propria funzione tramite poteri autoritativi, deliberativi o certificativi. Si ricorda che:

- il potere autoritativo è quel potere che permette alla Pubblica Amministrazione di realizzare i propri fini mediante veri e propri comandi, rispetto ai quali il privato si trova in una posizione di soggezione. Si tratta dell'attività in cui si esprime il c.d. potere d'imperio, che comprende sia i poteri di coercizione (arresto, perquisizione ecc.), di contestazione di violazioni di legge (accertamento di contravvenzioni ecc.), sia i poteri di supremazia di carattere pubblico nei confronti di un soggetto (autorizzazioni, concessioni);
- il potere deliberativo è quel potere che permette la formazione e manifestazione della volontà della Pubblica Amministrazione;
- il potere certificativo è quel potere di rappresentare come certa una determinata situazione sottoposta alla cognizione del pubblico agente.

Pubblico servizio e persona incaricata di pubblico servizio

L'art. 358 c.p. definisce "persona incaricata di un pubblico servizio" colui che "a qualunque titolo presta un pubblico servizio".

Per pubblico servizio "deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

Per pubblico servizio si intendono quindi a titolo esemplificativo:

– le attività di produzione di beni e servizi di interesse generale e assoggettate alla vigilanza di un'Autorità Pubblica; e

– le attività volte a garantire i diritti della persona alla vita, alla salute, alla libertà, alla previdenza e assistenza sociale, all'istruzione, alla libertà di comunicazione ecc., in regime di concessione e/o di convenzione (ad esempio, Enti Ospedalieri, ASL, I.N.P.S., I.N.A.I.L., membri dei Consigli Comunali, Banche, Uffici Postali, Uffici Doganali, Ferrovie, Autostrade, Aziende Energetiche Municipali, Compagnie Aeree ecc.).

2.5 Governance in materia di cybersicurezza, sistema ISO/IEC 27001 e flussi informativi verso l'Organismo di Vigilanza

Ai fini dell'inquadramento di SISPI nell'ambito della disciplina NIS2 e del D.lgs. 4 settembre 2024, n. 138 (ai sensi dell'art.7 c.3 lett. a), la Società ha ricevuto la comunicazione dell'Agenzia per la cybersicurezza nazionale (ACN) per l'inserimento nell'elenco dei soggetti NIS quale **essenziale** (prot. ACN n.140822 del 12.04.2025; prot. Sispi n. 001- 002711-AREG/2025)

La gestione dei rischi connessi alla sicurezza delle reti e dei sistemi informativi assume pertanto rilievo strategico e trasversale nell'assetto organizzativo della Società.

La Società ha adottato un sistema di gestione per la sicurezza delle informazioni conforme alla norma ISO/IEC 27001:2022, sottoposto a periodica verifica ai fini del mantenimento della certificazione. Nell'ambito di tale sistema, viene effettuata una strutturata valutazione del rischio cibernetico, finalizzata all'identificazione, analisi e trattamento dei rischi relativi alla riservatezza, integrità e disponibilità delle informazioni e dei sistemi informativi aziendali.

Il processo di *risk assessment cyber*, periodicamente aggiornato, costituisce parte integrante del sistema dei controlli interni e rileva altresì ai fini della prevenzione dei

reati previsti dal D.lgs. 231/2001, in particolare con riferimento ai delitti informatici di cui all'art. 24-bis, ai reati societari e contro la PA realizzabili mediante alterazione, manipolazione o indisponibilità di dati e sistemi, nonché ai reati che possano essere agevolati da carenze nei presidi di sicurezza digitale o nella gestione degli accessi e delle autorizzazioni.

La governance in materia di cybersicurezza è formalizzata attraverso anzitutto la chiara attribuzione di ruoli e responsabilità in materia di sicurezza ICT e gestione del rischio.

Altresì, rilevano la definizione di deleghe e poteri coerenti con le funzioni attribuite, nonché l'adozione di policy in materia di gestione degli accessi, protezione dei dati, monitoraggio dei sistemi, gestione delle vulnerabilità, continuità operativa, incident response e sicurezza della supply chain ICT. L'organo di gestione supervisiona il sistema di sicurezza informatica in conformità agli obblighi derivanti dalla normativa NIS2.

Per coordinare il sistema di gestione della sicurezza delle informazioni e il MOGC, i flussi informativi cyber verso l'OdV sono distinti in flussi periodici e flussi ad evento.

Flussi periodici

(a) esiti degli audit interni ed esterni relativi alla sicurezza delle informazioni e dei sistemi;

(b) risultanze del risk assessment cyber, incluse le vulnerabilità rilevanti emerse nelle verifiche programmate e le revisioni del piano di trattamento dei rischi;

(c) stato delle azioni correttive, dei piani di rimedio e delle iniziative di miglioramento.

Flussi ad evento

(d) incidenti informatici significativi e relative notifiche o comunicazioni alle autorità competenti;

(e) vulnerabilità rilevanti che richiedano interventi urgenti o incidano sui presidi del MOGC;

(f) violazioni delle policy di sicurezza informatica;

(g) modifiche rilevanti a ruoli, deleghe e responsabilità in materia di sicurezza ICT;

(h) eventi significativi riguardanti la supply chain ICT, compresi incidenti o inadempimenti di fornitori critici.

I flussi devono contenere elementi verificabili, indicare la funzione responsabile, il periodo o l'evento di riferimento, le valutazioni compiute, le misure adottate e lo stato delle eventuali azioni correttive. Essi consentono all'OdV di valutare l'adeguatezza e l'effettiva attuazione dei presidi rilevanti ai fini del D.lgs. 231/2001, senza sovrapporsi alle responsabilità operative e agli obblighi di notifica previsti dalla disciplina NIS2.

CAPITOLO 3

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO SISPI: LA METODOLOGIA ADOTTATA

3.1 Metodologia adottata e fasi

L'adozione e l'efficace attuazione del Modello costituiscono un elemento centrale del sistema di controllo interno di SISPI. Il processo di aggiornamento è impostato secondo un approccio risk based e mira a mantenere allineati il MOGC, l'organizzazione, i processi, le procedure e l'evoluzione del catalogo dei reati-presupposto.
L'aggiornamento è svolto con il coinvolgimento delle funzioni responsabili dei processi, dell'Organismo di Vigilanza e, per gli ambiti di rispettiva competenza, delle ulteriori funzioni di controllo e compliance. Le evidenze raccolte sono documentate e tracciate.
Il processo si articola in cinque fasi tra loro coordinate, sintetizzate nella tabella seguente e descritte nei paragrafi successivi.

ATTIVITÀ

Fase 1	**Avvio delle attività e individuazione dei processi e attività nel cui ambito possono essere commessi i reati richiamati dal D.lgs. n. 231/2001** *Raccolta e analisi della documentazione, e preliminare individuazione dei processi/attività nel cui ambito possono astrattamente essere commessi i reati richiamati dal D.lgs. n. 231/2001 (processi/attività c.d. "sensibili").*
Fase 2	**Identificazione dei Responsabili di Funzione** *Identificazione dei Responsabili di Funzione, ovvero delle persone della Società che, in base a funzioni e responsabilità, hanno una conoscenza approfondita delle aree/attività sensibili, nonché dei meccanismi di controllo attualmente in essere, al fine di determinare gli ambiti di intervento ed esecuzione di un piano di interviste dettagliato.*
Fase 3	**Analisi delle interviste, dei processi e delle attività sensibili. Gap Analysis** *Analisi delle interviste, individuazione e analisi dei processi e delle attività sensibili e dei meccanismi di controllo in essere, con particolare attenzione ai controlli preventivi ed altri elementi/attività di compliance*
Fase 4	**Individuazione dei protocolli di controllo** *Individuazione dei requisiti organizzativi caratterizzanti un idoneo modello di organizzazione, gestione e controllo ex D.lgs. n. 231/2001 e dei protocolli di controllo con funzione penale-preventiva, tenuto conto delle procedure già esistenti in SISPI.*
Fase 5	**Definizione del modello di organizzazione, gestione e controllo**. *Definizione del modello di organizzazione, gestione e controllo ex D.lgs. n. 231/2001 articolato in tutte le sue componenti e regole di funzionamento.*

3.1.1 Fasi 1 e 2 - Raccolta documentale, individuazione dei processi e coinvolgimento dei responsabili

La prima fase consiste nella raccolta e nell'analisi della documentazione organizzativa e procedurale rilevante: organigramma, ordini di servizio, deleghe e procure, regolamenti, procedure, sistemi di gestione, flussi informativi, esiti di audit e precedenti risk assessment. Su tale base sono individuati i processi e le attività potenzialmente esposti alla commissione dei reati-presupposto.

La seconda fase individua i responsabili e i referenti dei processi da coinvolgere nell'analisi. Attraverso questionari sul Sistema di Controllo Interno (SCI), interviste e confronti mirati sono rilevati, per ciascun processo, responsabilità, modalità operative, controlli esistenti, strumenti informatici, flussi autorizzativi e documentali, nonché eventuali criticità o aree di miglioramento.

L'analisi considera in particolare: integrità e valori etici; assetto organizzativo; chiarezza di ruoli, deleghe e responsabilità; segregazione delle funzioni; tracciabilità delle operazioni; sistemi di gestione del personale; controlli manuali e automatizzati; gestione delle eccezioni; formazione e consapevolezza.

Gli esiti alimentano la mappa dei processi sensibili e costituiscono la base informativa per la successiva Gap Analysis.

3.1.2 Fase 3 - Gap Analysis

La Gap Analysis confronta i presidi effettivamente in essere con i requisiti di controllo ritenuti adeguati rispetto ai rischi 231 individuati. L'analisi non si limita a registrare conformità o scostamenti, ma valuta l'idoneità sostanziale dei controlli e individua le azioni necessarie a colmare eventuali carenze.

Per ciascuna area sensibile sono considerati almeno: livello di rischio inerente; controlli preventivi e successivi; segregazione delle responsabilità; tracciabilità; poteri autorizzativi e di firma; gestione delle risorse finanziarie; presidi informatici; flussi informativi verso l'OdV; disciplina delle anomalie e delle deroghe; formazione; coordinamento con gli altri sistemi di compliance.

Gli scostamenti sono classificati secondo priorità e rilevanza e confluiscono in un piano di adeguamento con indicazione delle azioni, dei responsabili e delle tempistiche di attuazione.

3.1.3 Fase 4 - Definizione e adeguamento dei protocolli di controllo

Sulla base degli esiti della Gap Analysis sono definiti o aggiornati i protocolli di

prevenzione applicabili ai processi sensibili. I protocolli traducono i rischi individuati in regole operative e controlli verificabili, valorizzando, ove adeguati, i presidi già presenti nei sistemi aziendali e nelle certificazioni adottate da SISPI.

I protocolli sono costruiti secondo principi di proporzionalità e verificabilità e, in funzione del processo, disciplinano: attribuzione di ruoli e responsabilità; separazione tra funzioni incompatibili; livelli autorizzativi; tracciabilità delle decisioni e delle operazioni; controlli di primo e secondo livello; gestione delle risorse finanziarie; qualificazione e controllo delle controparti; gestione dei sistemi informativi e degli accessi; obblighi di escalation e flussi verso l'OdV.

Le azioni di adeguamento sono integrate, per quanto possibile, nelle procedure e nei sistemi gestionali esistenti, evitando duplicazioni e garantendo coerenza con il Sistema di Gestione Integrato, con la disciplina anticorruzione e trasparenza, con la cybersecurity e con la protezione dei dati personali.

3.1.4 Fase 5 - Consolidamento, approvazione e attuazione del MOGC

La fase conclusiva consiste nel consolidamento delle risultanze del risk assessment e della Gap Analysis nella Parte Generale, nelle Parti Speciali e nei documenti collegati al MOGC. Sono verificate la coerenza tra rischi, protocolli, responsabilità, flussi informativi e sistema disciplinare, nonché la corretta integrazione con il Codice Etico e di Comportamento e con il Regolamento dell'OdV.

La proposta di aggiornamento è sottoposta all'Organo di gestione per le determinazioni di competenza. Dopo l'approvazione, le modifiche sono comunicate ai destinatari e accompagnate, ove necessario, da interventi formativi, aggiornamento delle procedure e implementazione delle azioni correttive individuate.

L'effettiva attuazione delle misure e il permanere della loro idoneità sono oggetto di monitoraggio nel tempo. Gli esiti dei controlli, le modifiche normative e organizzative, le segnalazioni, gli incidenti rilevanti e le risultanze degli audit costituiscono input per il successivo ciclo di aggiornamento del Modello.

CAPITOLO 4

L'ORGANISMO DI VIGILANZA AI SENSI DEL D.lgs. N. 231/2001

4.1 Individuazione dell'Organismo di Vigilanza (OdV)

Come anticipato nel capitolo 2 relativo al "Quadro normativo", in base alle previsioni del D.lgs. n. 231/2001 – art. 6, comma 1, lett. a) e b) – la Società può essere esonerata dalla responsabilità amministrativa conseguente alla commissione di reati da parte dei soggetti qualificati ex art. 5 del D.lgs. 231/2001, se l'Organo di gestione societaria ha:

- adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo (MOGC) idoneo a prevenire i reati presupposto;
- affidato il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento ad un Organismo di vigilanza (OdV) della Società dotato di autonomi poteri di iniziativa e controllo.

In tal senso il Socio unico di SISPI, novellando gli statuti delle partecipate anche alla luce del Testo Unico entrato in vigore dal 27 giugno 2017, ha introdotto apposita previsione con l'attuale art. 34 rubricato "Organismo di Vigilanza ai sensi del D.lgs. 231/2001".

Le «Linee Guida Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001», aggiornate a giugno 2021, suggeriscono, quali requisiti indispensabili dell'OdV:

- ***autonomia e indipendenza***; valutate in relazione all'organismo e non ai singoli componenti, in termini di:
  - assenza di conflitti di interessi, anche potenziali, con SISPI;
  - possesso di autonomi poteri di iniziativa e controllo;
  - non attribuzione di compiti operativi all'interno di SISPI;
  - collocazione in posizione di diretto riferimento all'organo di gestione;
- ***professionalità*** intesa come:
  - possesso di adeguate competenze specialistiche;

- dotazione di strumenti e tecniche specialistiche per poter svolgere l'attività, anche avvalendosi della consulenza di soggetti esterni.

- ***continuità d'azione*** intesa come:

- durata del mandato indipendente da quella degli altri organi sociali;
- periodicità dei controlli.

In attuazione ai principi sopra menzionati, SISPI ha ritenuto opportuno costituire un Organismo di vigilanza di composizione collegiale, costituito *ad hoc* da tre membri scelti nel rispetto dei requisiti sopra richiamati- intesi in relazione alla funzionalità dell'Organismo ed ai compiti che la legge assegna allo stesso -, tra soggetti particolarmente qualificati nelle materie rilevanti ai fini della norma di riferimento, in tal modo garantendo idonee conoscenze giuridiche ed amministrative, di principi e delle tecniche di controllo, nonché dell'organizzazione e dei principali processi aziendali.

L'Organismo di Vigilanza SISPI è alla data (30.04.2026) formato da:

- **due componenti scelti tra professionalità esterne di cui una con funzioni di Presidente, individuati con apposita procedura ad evidenza pubblica di cui viene data diffusione mediante la pubblicazione di apposito avviso sul sito istituzionale, dotati di comprovata esperienza e professionalità in materia di D.lgs. 231/2001, nel settore amministrativo e del controllo dei conti maturata nei confronti di enti pubblici e/o privati e in particolare di OdV. in Società a partecipazione pubblica.**
- **un componente interno**, possibilmente responsabile di una funzione aziendale che, compatibilmente con organico e organizzazione aziendale, non sia coinvolta nei processi produttivi e, in generale nei processi a rischio reato, individuato con apposita determinazione dell'Organo di gestione tra i soggetti dotati delle necessarie competenze individuate dal Regolamento Istitutivo approvato dal Socio ai sensi dell'art. 34 dello Statuto;

Rispetto poi ai requisiti della professionalità, tenendo altresì conto delle esperienze maturate in questi anni oltreché delle pronunce giurisprudenziali già formulate al riguardo, i componenti dell'Organismo di Vigilanza, dovranno collegialmente garantire

la necessaria competenza, nonché, singolarmente, astenersi in occasione delle decisioni da assumere nell'ambito delle funzioni attribuite su argomenti di diretta competenza aziendale.

Per i componenti esterni, sarà necessario verificare che gli stessi siano dotati di una provata esperienza nel settore amministrativo e del controllo dei conti maturata nei confronti di enti pubblici e/o privati. Si privilegeranno candidati che abbiano già maturato esperienze quali componenti di OdV o abbiano svolto altra attività di gestione e/o controllo in altre società e/o Enti pubblici o privati e siano in possesso di titoli di studio adeguati all'attività da svolgere.

4.2 Il Regolamento istitutivo dell'Organismo

L'Organismo di Vigilanza di SISPI è istituito con delibera dell'Organo di gestione nel rispetto delle previsioni per ciò contenute nel Regolamento istitutivo dell'Organismo di Vigilanza approvato dal Socio con apposita delibera ex art. 34 dello Statuto societario, resta in carica per tre anni; decade alla data stabilita nell'atto di nomina, pur continuando a svolgere *ad interim* le proprie funzioni fino alla nuova nomina.

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza dei requisiti soggettivi dell'onorabilità, integrità e rispettabilità, nonché all'assenza di cause di ineleggibilità e/o decadenza, di incompatibilità, o potenziali conflitti di interesse.

In particolare, all'atto del conferimento dell'incarico, ogni soggetto designato a ricoprire la carica di componente dell'Organismo di Vigilanza deve rilasciare una dichiarazione nella quale attesta l'assenza di motivi di ineleggibilità e/o decadenza, di incompatibilità previsti nel Regolamento istitutivo.

Nello svolgimento dei compiti affidatigli, l'OdV potrà giovarsi, sotto la sua diretta sorveglianza e responsabilità, della collaborazione di tutte le Funzioni e servizi di SISPI, ovvero di consulenti esterni avvalendosi delle rispettive competenze e professionalità (ciò è reso possibile dall'attribuzione di adeguate risorse finanziarie all'OdV).

La decadenza dell'OdV potrà avvenire, oltre che per la naturale scadenza del mandato, per giusta causa nei casi previsti dal Regolamento istitutivo, mediante un'apposita

delibera dell'Organo di gestione.

4.3 Risorse economiche assegnate all'Organismo di Vigilanza

L'Organo di gestione in fase di pianificazione del Budget aziendale, assegna, ogni anno, un budget di spesa all'OdV.
L'assegnazione del budget permette all'OdV di operare in autonomia per un efficace espletamento del compito assegnatogli dal presente Modello, secondo quanto previsto dal Decreto.

4.4 Funzioni e poteri dell'Organismo di Vigilanza

Le funzioni ed i poteri dell'OdV sono disciplinate da un regolamento che ne definisce:

- la pianificazione delle attività;
- la determinazione delle modalità e dei tempi previsti per lo svolgimento delle attività di controllo/verifica/audit;
- l'individuazione di criteri e procedure di analisi e audit;
- l'eventuale aggiornamento dei Flussi informativi di cui alla Sezione Quarta del MOGC.

Tale Regolamento, e le eventuali modifiche che l'Organismo riterrà necessarie o opportune sono oggetto di trasmissione all'Organo di gestione per la dovuta presa d'atto e la relativa approvazione.
All'OdV è affidato il compito di vigilare:

1. sull'osservanza delle prescrizioni del Modello, in relazione alle diverse tipologie di reati contemplate dal Decreto e dalle successive leggi che ne hanno esteso il campo di applicazione;
2. sulla efficacia del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei reati;
3. sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione alle mutate condizioni aziendali e/o normative.

L'Organismo dispone di autonomi poteri di iniziativa, intervento e controllo, che si estendono a tutte le Funzioni e ai servizi della SISPI.

In particolare, all'Organismo di Vigilanza sono affidati, per l'espletamento e l'esercizio delle proprie funzioni, i seguenti compiti e poteri:

- vigilare sul funzionamento del Modello sia rispetto alla prevenzione della commissione dei reati richiamati dal D.lgs. 231/2001 sia con riferimento alla capacità di far emergere il concretizzarsi di eventuali comportamenti illeciti;
- svolgere periodica attività ispettiva e di controllo, di carattere continuativo - con frequenza temporale e modalità predeterminata dal Regolamento interno delle attività di vigilanza - e controlli a sorpresa, in considerazione dei vari settori di intervento o delle tipologie di attività e dei loro punti critici al fine di verificare l'efficienza ed efficacia del Modello;
- accedere liberamente presso gli Uffici di SISPI – senza necessità di alcun consenso preventivo – per richiedere ed acquisire informazioni, documentazione e dati, ritenuti necessari per lo svolgimento dei compiti previsti dal D.lgs. 231/2001, da tutto il personale dipendente e dirigente.

4.5 Funzioni dell'OdV: reporting nei confronti degli organi societari

L'Organismo di Vigilanza riferisce in merito alle attività e compiti affidati, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi, attraverso distinte linee di reporting:

- su base continuativa o periodica nei confronti dell'Organo di gestione e del Collegio Sindacale.
- ove risultino accertati fatti di particolare gravità, tempestivamente all'Organo di gestione societaria ed al Collegio Sindacale;
- alla notizia di una violazione del Modello commessa da parte di uno o più membri dell'Organo di gestione, l'OdV informa il Collegio Sindacale.

Gli incontri con gli Organi sociali di SISPI, cui l'Organismo di Vigilanza riferisce devono

essere documentati mediante appositi verbali. L'Organismo di Vigilanza cura l'archiviazione della relativa documentazione.

L'Organismo di Vigilanza predispone:

- **periodicamente**, una relazione informativa semestrale, relativa all'attività svolta, da presentare all'organo di gestione e al Collegio Sindacale;
- **tempestivamente**, una nota o relazione al verificarsi di situazioni straordinarie (ad esempio: significative violazioni dei principi contenuti nel Modello, novelle normative in materia di responsabilità amministrativa delle Società, significative modificazioni dell'assetto organizzativo della SISPI, ecc.) da presentare al Direttore Generale, all'Organo di gestione, o al Collegio Sindacale

Tra i possibili contenuti delle relazioni periodiche si evidenzia:

– eventuali problematiche sorte riguardo alle modalità di attuazione delle procedure previste dal Modello o adottate in attuazione o alla luce del Modello o del Codice Etico;
– il resoconto delle segnalazioni ricevute da soggetti interni ed esterni in ordine al Modello o al Codice Etico;
– le procedure disciplinari e le sanzioni eventualmente applicate dalla SISPI, con riferimento esclusivo alle attività a rischio;
– una valutazione complessiva sul funzionamento del Modello o del Codice Etico, con eventuali indicazioni per integrazioni, correzioni o modifiche.

L'Organo di gestione ed il Collegio Sindacale hanno la facoltà di convocare in qualsiasi momento l'OdV

Per quanto non espressamente indicato nel presente capitolo, si rimanda al Regolamento istitutivo dell'OdV (Allegato 3 del presente MOGC).

CAPITOLO 5

FLUSSI INFORMATIVI NEI CONFRONTI DELL'OdV

5.1 Obblighi di informazione nei confronti dell'Organismo di Vigilanza

Le strutture operative aziendali devono trasmettere all'OdV, all'indirizzo di posta elettronica odv@sispi.it, i flussi informativi periodici e i flussi ad evento funzionali all'attività di vigilanza, secondo uno schema che individua soggetto responsabile, contenuti, documenti di supporto e tempistica ed è sottoposto ad aggiornamento periodico a cura dell'OdV.

Per la cybersicurezza, i flussi periodici comprendono, a titolo esemplificativo, gli esiti degli audit interni ed esterni, le risultanze del risk assessment cyber, le vulnerabilità rilevanti emerse nelle verifiche programmate e lo stato delle azioni correttive.

I flussi cyber ad evento comprendono, a titolo esemplificativo, gli incidenti informatici significativi, le vulnerabilità rilevanti che richiedono interventi urgenti, le violazioni delle policy di sicurezza, le modifiche rilevanti a ruoli, deleghe e responsabilità, gli eventi significativi della supply chain ICT e le notifiche o comunicazioni alle autorità competenti.

Restano altresì ricompresi, a titolo esemplificativo, i seguenti flussi informativi:

- informazioni sui contratti aziendali e sulle relative attività produttive, nonché sull'acquisizione ed impiego dei fattori produttivi;
- informazioni sugli adempimenti relativi alle normative specifiche di settore (sicurezza, privacy, qualità, ambiente etc.)
- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D.lgs. 231/2001 e che possano coinvolgere SISPI;
- richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario nei loro confronti ed in relazione ai reati di cui al D.lgs. 231/2001, salvo espresso divieto dell'autorità giudiziaria;
- rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con

profili critici rispetto all'osservanza delle norme e previsioni del Modello;

– ogni altra informazione che, sebbene non ricompresa nell'elenco che precede, risulti rilevante ai fini di una corretta e completa attività di vigilanza ed aggiornamento del Modello.

Le Funzioni e i servizi della Società, gli organi di governance, i dipendenti, i consulenti e i collaboratori di SISPI sono tenuti a prendere visione dello Schema dei flussi informativi verso l'OdV, allegato alla presente Parte Generale del MOGC quale Allegato 5, individuando le informazioni di propria competenza da trasmettere all'OdV.

5.2 Sistema delle deleghe e delle procure

All'OdV deve essere comunicato il sistema delle deleghe e delle procure adottato da SISPI e, tempestivamente, ogni successiva modifica dello stesso.
In particolare, l'OdV, potrà richiedere alla Funzione Affari Legali la copia delle procure speciali in essere.

5.3 Raccolta e conservazione delle informazioni

Ogni informazione, segnalazione, report, relazione previsti nel Modello sono conservati dall'Organismo di Vigilanza in un apposito archivio (informatico o cartaceo) per un periodo di almeno 10 anni.

CAPITOLO 6

PIANO DI FORMAZIONE E DIVULGAZIONE

6.1 Premessa

SISPI, al fine di dare efficace attuazione al presente Modello e al Codice Etico e di comportamento che ne costituisce parte integrante, intende assicurare una corretta divulgazione di contenuti e principi degli stessi sia all'interno che all'esterno della propria organizzazione. In particolare, obiettivo di SISPI è quello di darne comunicazione non soltanto ai propri dipendenti ma anche ai soggetti che, pur non essendo dipendenti, operano – in maniera continuativa – per il conseguimento degli obiettivi di SISPI.

SISPI, infatti, intende:

- determinare, in tutti coloro che operano in suo nome e per suo conto nelle attività a rischio reato, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni;
- informare tutti coloro che operano a qualsiasi titolo in suo nome, per suo conto o comunque nel suo interesse, che la violazione delle prescrizioni contenute nel presente Modello comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale che ad essa li lega;
- ribadire la non tolleranza di comportamenti illeciti che, anche nel caso fosse possibile potesse configurare una condizione di apparente vantaggio per sé stessa, sono contrari ai principi etici cui la stessa informa la sua attività.

L'attività di formazione e divulgazione deve essere diversificata a seconda dei destinatari cui essa si rivolge e deve, in ogni caso, essere improntata a principi di completezza, chiarezza, accessibilità e continuità al fine di consentire ai diversi destinatari la piena consapevolezza delle disposizioni aziendali che sono tenuti a rispettare e dei principi etici che devono ispirare i loro comportamenti, anche con riferimento ai doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati da SISPI.

L'attività di formazione e divulgazione è concordata con l'Organismo di Vigilanza, cui

sono assegnati, tra gli altri, i compiti di promuovere e definire le iniziative per la diffusione della conoscenza e della comprensione del MOGC, la sensibilizzazione all'osservanza dello stesso.

6.2 Destinatari della divulgazione

Tutto il personale dipendente (dirigente e non), ed i collaboratori esterni con rapporto stabile con la società, è tenuto a:

i) acquisire consapevolezza dei principi e contenuti del Modello (e, con esso, si ribadisce, del Codice Etico);
ii) conoscere le modalità operative con le quali deve essere realizzata la propria attività;
iii) contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del MOGC, segnalando eventuali carenze riscontrate negli stessi.

Ai dipendenti, ai nuovi assunti, ai collaboratori esterni è consegnata copia del Codice Etico e di comportamento, ed è garantita la consultazione diretta del Modello con l'accesso all'area all'uopo dedicata nella Intr@com, la rete intranet aziendale, su apposito spazio dedicato "MOGC D.lgs. 231/01". È inoltre fatta loro richiesta di sottoscrivere dichiarazione di conoscenza ed osservanza dei principi del Modello e del Codice Etico e di comportamento.

In ogni caso, per i dipendenti o collaboratori esterni stabili che non dovessero avere accesso alla rete aziendale, la documentazione dovrà essere messa a loro disposizione con mezzi alternativi (ad es.: affissione nelle bacheche aziendali, sito istituzionale, trasmissione via mail).

La formazione e la divulgazione di principi e contenuti del Modello sono garantite dai responsabili delle funzioni aziendali preposte che, secondo quanto all'uopo concordato tra la Funzione risorse umane dell'azienda, l'Organismo di Vigilanza e, occorrendo, in relazione ai temi da trattare il RPC aziendale, identificano la migliore modalità di fruizione di tali servizi (ad esempio: *staff meeting*, sessioni formative in aula, ecc.).

Come per tutta la formazione aziendale, a conclusione degli eventi formativi, come consueto, i partecipanti compileranno apposito questionario, attestando, così, la

frequentazione del momento formativo.

Naturalmente tali eventi potranno essere organizzati anche attraverso moduli di formazione a distanza con l'utilizzo di sistemi informatici (es.: video conferenza, e-learning).

In caso di aggiornamento le nuove versioni del documento saranno rese note al personale tramite mail con richiesta di presa visione.

6.3 Componenti degli organi sociali e soggetti con funzioni di rappresentanza

Ai componenti degli Organi sociali ed ai soggetti con funzioni di rappresentanza è resa disponibile copia del MOGC al momento dell'accettazione della carica loro conferita e sarà fatta loro sottoscrivere dichiarazione di osservanza dei principi del Modello e Codice Etico.

Idonei strumenti di formazione e divulgazione saranno adottati per aggiornare tali destinatari circa le eventuali modifiche apportate al Modello, nonché ogni rilevante cambiamento procedurale, normativo o organizzativo.

Le iniziative di formazione e aggiornamento potranno svolgersi anche a distanza mediante l'utilizzo di sistemi informatici (es.: video conferenza, e-learning).

CAPITOLO 7

SISTEMA DISCIPLINARE

7.1 Principi generali

La definizione di un adeguato sistema disciplinare e sanzionatorio costituisce un presupposto essenziale per l'efficacia del modello di organizzazione, gestione e controllo ai sensi del D.lgs. 231/2001.

Nel rispetto delle previsioni della L. 300/1970 cd. "Statuto dei Lavoratori", SISPI ha definito il proprio Codice disciplinare che individua infrazioni, sanzioni e procedure di contestazione con precipuo riferimento alle previsioni di Codice Civile e Contratto Collettivo Nazionale applicato in azienda integrate con le previsioni di cui al Codice Etico e di Comportamento aziendale.

Infatti, con l'entrata in vigore del D.lgs. 231/2001 (di seguito "Decreto") il legislatore ha individuato, quale condizione per l'efficace attuazione del Modello di Organizzazione, Gestione e Controllo (di seguito "MOGC") eventualmente adottato dalle aziende, l'introduzione di un sistema idoneo a sanzionare il mancato rispetto di Codice Etico, regole e procedure previste nell'ambito del modello stesso (cfr. artt. 6, c. 2, lett. e) e 7, c. 4, lett. b del D.lgs. 231/2001).

SISPI S.p.A., essendosi dotata, sin dall'entrata in vigore della norma, di un modello di organizzazione gestione e controllo, ha dunque integrato e adeguato il proprio sistema sanzionatorio con riferimento allo stesso ed al Codice Etico ivi previsto.

Successivamente, tenuto conto del combinato disposto delle previsioni di cui alla L. 190/12 e delle Determinazioni ANAC 50/2014, 8 e 12 del 2015 e n. 1134 del 2017, SISPI S.p.A. ha altresì provveduto ad introdurre nel proprio MOGC misure idonee a prevenire anche i fenomeni di corruzione e di illegalità al suo interno in coerenza con le finalità della disciplina sulla prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione, redigendo un apposito Codice di Comportamento – ispirato ai principi del DPR 62/2013 (alla data integrato dalle disposizioni del DPR81/2023)– nel quale, integrando il Codice Etico aziendale già introdotto ai sensi del D.lgs. 231, stabilisce le regole di comportamento rilevanti ai fini della prevenzione della corruzione.

Il Codice disciplinare aziendale[5] definisce le misure e le sanzioni previste per i casi di violazione del sistema di norme e procedure contenuto nel MOGC aziendale, con particolare riferimento al Codice Etico e di Comportamento e ne disciplina l'applicazione nei confronti dei soggetti destinatari.

Lo stesso Codice individua, altresì, i criteri di commisurazione ed applicazione delle sanzioni previste.

L'applicazione delle sanzioni previste dal Codice disciplinare non sostituisce le norme di legge vigenti e le clausole della pattuizione collettiva in tema di sanzioni disciplinari ed è condotta indipendentemente e oltre gli eventuali procedimenti civili, amministrativi e/o penali instauratisi anche a prescindere dall'esito degli stessi.

Per tutto quanto non previsto nel Codice disciplinare, troveranno quindi applicazione le norme di legge e di regolamento vigenti, nonché le previsioni della contrattazione, inclusa quella collettiva, e dei regolamenti aziendali, laddove applicabili.

In ogni caso, l'applicazione delle sanzioni di cui al Codice disciplinare non pregiudica né preclude:

a) per la Società il diritto di agire nei confronti del soggetto responsabile al fine di ottenere il risarcimento di tutti i danni patiti a causa o in conseguenza della condotta accertata;

b) per i lavoratori l'esercizio dei propri diritti compresi quelli di contestazione o di opposizione avverso il provvedimento disciplinare, loro riconosciuti da norme di legge o di regolamento, nonché dalla contrattazione, inclusa quella collettiva, e/o dai regolamenti aziendali.

7.2 Pubblicità ed efficacia

Ai sensi di quanto previsto dall'art. 7 della L.300/70, le norme contenute nel Codice disciplinare devono essere portate a conoscenza dei lavoratori mediante affissione in

[5] predisposto nel rispetto degli artt. 2118 e 2119 del Codice Civile, rispettivamente "recesso dal contratto a tempo indeterminato"' e "recesso per giusta causa", nonché nel rispetto della L. 300/70, cd. "Statuto dei lavoratori", e dei vigenti "Contratto Collettivo Nazionale di Lavoro dell'Industria metalmeccanica e della installazione di impianti" e "Contratto nazionale dei Dirigenti di aziende produttrici di beni e di servizi" attualmente applicati in azienda

luogo accessibile a tutti, nonché attraverso il sistema di comunicazione informatico interno, provvedendo ad attestare l'avvenuta ricezione del documento da parte degli interessati.

Per la pubblicità nei confronti di consulenti e terzi in genere, la Società provvede ad inserire apposite clausole nelle lettere di incarico e/o nei contratti che ne disciplinano il rapporto secondo quanto previsto nei successivi articoli.

Le disposizioni contenute nel Codice Disciplinare sono, altresì, portate a conoscenza di tutti gli interessati con la pubblicazione sul sito istituzionale https://sispi.sispipat.it/archivio19_regolamenti_0_18.html.

Sono soggetti al sistema sanzionatorio e disciplinare, di cui al presente Modello, tutti i lavoratori dipendenti, gli amministratori, i collaboratori di SISPI, nonché tutti coloro che abbiano rapporti contrattuali con la stessa, nell'ambito dei rapporti in essere.

7.3 Principi generali di applicazione

Le sanzioni previste saranno applicate ad ogni violazione delle disposizioni contenute nel Modello e nel Codice Etico e di comportamento a prescindere dallo svolgimento e, nel caso in cui il comportamento da censurare integri gli estremi di una fattispecie di reato rilevante ai sensi del D.lgs. 231/2001, dall'esito del procedimento penale eventualmente avviato presso l'Autorità giudiziaria.

L'applicazione delle sanzioni disciplinari deve attuarsi nel rispetto dei seguenti principi:

- **complementarità**: il sistema disciplinare previsto dal Modello è complementare, e non alternativo, rispetto al sistema disciplinare stabilito dal CCNL applicato dalla SISPI *("CCNL METALMECCANICI")*;
- **pubblicità**: SISPI dà massima e adeguata conoscenza e conoscibilità al Modello ed al Codice Etico e di comportamento.
- **contraddittorio**: SISPI garantisce il rispetto del contraddittorio mediante la previa pubblicità del Modello, del Codice Etico e del sistema sanzionatorio, nonché con la previa contestazione scritta in modo specifico, immediato e immutabile degli addebiti;
- **gradualità**: le decisioni relative alla tipologia di sanzione da irrogare tengono

necessariamente conto della gravità dell'infrazione, di tutte le circostanze, oggettive e soggettive;

- **tempestività**: il procedimento disciplinare e l'eventuale irrogazione della sanzione devono avvenire entro un termine ragionevole e certo dall'apertura del procedimento stesso.

Le regole di condotta imposte dal Modello, infatti, sono assunte dall'Azienda in piena autonomia, al fine del miglior rispetto delle regole aziendali adottate.

7.4 Criteri di commisurazione

Le sanzioni disciplinari qui trattate sono applicate secondo il criterio di proporzionalità previsto dall'art. 2106 c.c.

In via generale, concorrono alle valutazioni dei comportamenti, i seguenti elementi:

a) gravità oggettiva della condotta, con attenzione anche all'intenzionalità o meno del comportamento;
b) modalità della condotta stessa;
c) gravità effettiva dell'evento determinato;
d) tipologia della violazione compiuta;
e) circostanze nel cui ambito si è sviluppata la condotta.

Ai fini dell'eventuale aggravamento della sanzione, devono, inoltre, essere considerati i seguenti elementi:

a) eventuale commissione di più violazioni nell'ambito della medesima condotta, nel qual caso l'aggravamento sarà operato rispetto alla sanzione prevista per la violazione più grave;
b) eventuale concorso di più soggetti nella commissione della violazione;
c) gravità degli effetti dell'illecito disciplinare, ossia del livello di rischio cui la Società ragionevolmente può essere esposta in seguito alla violazione contestata;
d) eventuale recidività del suo autore;
e) altre particolari circostanze che accompagnano l'illecito.

Nel caso di applicazione delle sanzioni nei confronti dei lavoratori, si terrà anche conto:

a) dell'intenzionalità del comportamento o del grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
b) del comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
c) delle mansioni del lavoratore;
d) della posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
e) delle altre particolari circostanze che accompagnano l'illecito disciplinare.

CAPITOLO 8

MODELLO 231, SISTEMA ANTICORRUZIONE E TRASPARENZA, PIANO PERFORMANCE: IL SISTEMA INTEGRATO

8.1 Integrazione tra Modello 231 e PTPCT

La disciplina del D.lgs. 231/2001 e quella in materia di prevenzione della corruzione e trasparenza restano distinte per finalità, presupposti, presidi e responsabilità. Il coordinamento organizzativo non comporta sovrapposizione dei rispettivi ambiti applicativi né delle competenze attribuite ai diversi soggetti di controllo.

Il sistema 231 è finalizzato a prevenire i reati-presupposto commessi, nell'interesse o a vantaggio dell'ente, dai soggetti indicati dall'art. 5 del D.lgs. 231/2001. I relativi presidi sono il MOGC, i protocolli di controllo, il sistema disciplinare, la formazione e i flussi informativi verso l'OdV. L'eventuale responsabilità amministrativa da reato ricade su SISPI; l'OdV vigila sul funzionamento e sull'osservanza del MOGC e ne cura l'aggiornamento nei limiti dei poteri attribuiti, senza assumere funzioni gestorie.

La disciplina anticorruzione e trasparenza persegue la prevenzione della corruzione in senso ampio e della cattiva amministrazione, anche quando le condotte possano arrecare danno alla Società, e assicura l'adempimento degli obblighi di pubblicità, trasparenza e accesso civico. I riferimenti principali sono la L. 190/2012, il D.lgs. 33/2013, le Linee Guida ANAC approvate con delibera n. 1134 dell'8 novembre 2017 e il Piano Nazionale Anticorruzione 2026-2028, approvato con delibera ANAC n. 19 del 28 gennaio 2026.

I relativi presidi sono le misure di prevenzione della corruzione e trasparenza, la programmazione periodica, la mappatura dei processi, la gestione dei conflitti di interessi, gli obblighi di pubblicazione, il monitoraggio e i flussi informativi verso i responsabili competenti. Le responsabilità restano attribuite all'Organo di gestione, al Responsabile della prevenzione della corruzione (RPC) e al Responsabile della trasparenza (RT), secondo l'assetto organizzativo di SISPI e le rispettive competenze; tali funzioni non sono assorbite dall'OdV.

SISPI adotta un documento unitario nel quale le misure anticorruzione e trasparenza

sono coordinate con il MOGC, mantenendo sezioni, finalità, presidi, flussi e responsabilità chiaramente distinguibili. Il coordinamento riguarda gli ambiti di interferenza, tra cui la mappatura dei processi e dei rischi, i controlli, la formazione, i flussi informativi e il monitoraggio delle azioni correttive.

Negli ambiti comuni, l'OdV, il RPC e l'RT si scambiano le informazioni pertinenti nel rispetto delle rispettive attribuzioni, evitando duplicazioni e preservando l'autonomia delle valutazioni previste dalle singole discipline.

8.2 Sistema di segnalazione delle violazioni (Whistleblowing)

SISPI adotta un sistema di segnalazione interna conforme al D.lgs. 10 marzo 2023, n. 24, all'art. 6, comma 2-bis, del D.lgs. 231/2001, alle Linee Guida ANAC n. 1/2025 sui canali interni (delibera n. 478 del 26 novembre 2025) e, per quanto rilevante, alla disciplina ANAC sulle segnalazioni esterne aggiornata con delibera n. 479 del 26 novembre 2025. Il presente paragrafo definisce i principi di raccordo con il MOGC; le modalità operative sono disciplinate dal Regolamento Whistleblowing aziendale, al quale si rinvia.

Ambito e soggetti tutelati

Possono essere segnalate le violazioni rientranti nell'ambito oggettivo del D.lgs. 24/2023, comprese, nei limiti previsti dalla legge, le condotte illecite rilevanti ai sensi del D.lgs. 231/2001 e le violazioni del MOGC. Non rientrano nel canale whistleblowing le contestazioni o rivendicazioni di carattere esclusivamente personale attinenti al rapporto individuale di lavoro, salvo che assumano rilievo ai sensi della disciplina applicabile.

Le tutele si applicano alle persone che acquisiscono informazioni sulle violazioni nel contesto lavorativo, secondo le categorie previste dal D.lgs. 24/2023, e si estendono, ricorrendone i presupposti, ai facilitatori e agli altri soggetti collegati alla persona segnalante indicati dalla legge. La protezione opera quando, al momento della segnalazione, sussistono fondati motivi per ritenere vere le informazioni e ricompreso il fatto nell'ambito della disciplina.

Canale interno e soggetto gestore

SISPI mette a disposizione un canale interno idoneo a ricevere segnalazioni in forma scritta e orale, progettato e gestito in modo da garantire, anche mediante strumenti di cifratura ove appropriati, la riservatezza dell'identità della persona segnalante, della persona coinvolta e di ogni persona menzionata, nonché del contenuto della segnalazione e della relativa documentazione.

In quanto società a controllo pubblico/ *in house*, la gestione del canale interno è affidata al RPC ai sensi dell'art. 4, comma 5, del D.lgs. 24/2023. Il Regolamento individua un gestore sostitutivo per le ipotesi di conflitto di interessi, assenza o altra situazione che impedisca al RPC di trattare la segnalazione con imparzialità e riservatezza.

La piattaforma informatica aziendale costituisce il canale prioritario per le segnalazioni scritte. Devono essere assicurate anche le modalità orali previste dalla legge, mediante sistema di messaggistica vocale e/o, su richiesta della persona segnalante, incontro diretto entro un termine ragionevole. Le modalità concretamente disponibili e i relativi recapiti sono pubblicati sul sito istituzionale e indicati nel Regolamento Whistleblowing.

Gestione della segnalazione

Il gestore rilascia alla persona segnalante avviso di ricevimento entro sette giorni dalla presentazione, mantiene le interlocuzioni, dà diligente seguito alla segnalazione e fornisce riscontro entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza, dalla scadenza del termine di sette giorni. La segnalazione interna ricevuta da un soggetto diverso dal gestore è trasmessa al soggetto competente entro sette giorni, dando contestuale notizia della trasmissione alla persona segnalante.

L'istruttoria è svolta secondo criteri di imparzialità, proporzionalità, necessità e minimizzazione dei dati. Possono essere coinvolte altre funzioni o professionalità, interne o esterne, solo quando necessario e previa adozione delle misure organizzative idonee a preservare la riservatezza e a limitare l'accesso alle sole informazioni indispensabili.

Raccordo tra RPC e Organismo di Vigilanza

Quando la segnalazione riguarda fatti potenzialmente rilevanti ai sensi del D.lgs. 231/2001 o violazioni del MOGC, l'RPC (in SISPI alla data funzione separata dall'RT) assicura il necessario raccordo con l'OdV, trasmettendo esclusivamente le informazioni pertinenti e nel rispetto degli obblighi di riservatezza e della disciplina in materia di protezione dei dati personali. L'OdV valuta i profili di propria competenza senza sostituirsi al gestore del canale e senza duplicare l'istruttoria.

Tutela della riservatezza, dati personali e conservazione

L'identità della persona segnalante e qualsiasi informazione dalla quale essa possa essere desunta, direttamente o indirettamente, non sono rivelate a soggetti diversi da quelli competenti e autorizzati, salvo i casi e con le garanzie espressamente previste dalla legge. Il trattamento dei dati personali è effettuato nel rispetto del Regolamento (UE) 2016/679, del D.lgs. 196/2003 e dei principi di liceità, correttezza, trasparenza, minimizzazione e limitazione della conservazione.

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario alla gestione e comunque non oltre cinque anni dalla comunicazione dell'esito finale della procedura, fatti salvi eventuali ulteriori obblighi di legge applicabili a documenti distinti dalla segnalazione e trattati per autonome finalità.

Divieto di ritorsione e sistema disciplinare

È vietata qualsiasi ritorsione, anche solo tentata o minacciata, collegata alla segnalazione, alla denuncia all'Autorità giudiziaria o contabile o alla divulgazione pubblica effettuata alle condizioni di legge. Il sistema disciplinare sanziona, secondo proporzionalità e nel rispetto delle garanzie applicabili, le violazioni delle misure di tutela del segnalante, gli ostacoli alla segnalazione, le violazioni della riservatezza e le altre condotte sanzionabili previste dal D.lgs. 24/2023.

Le tutele non operano nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per diffamazione o calunnia, ovvero

la responsabilità civile per lo stesso titolo nei casi di dolo o colpa grave, secondo quanto previsto dall'art. 16 del D.lgs. 24/2023.

Segnalazione esterna, divulgazione pubblica e denuncia

La persona segnalante può ricorrere al canale esterno gestito da ANAC quando ricorre una delle condizioni previste dall'art. 6 del D.lgs. 24/2023, tra cui: mancata attivazione o non conformità del canale interno obbligatorio; segnalazione interna rimasta senza seguito; fondato motivo di ritenere inefficace il seguito o concreto il rischio di ritorsione; pericolo imminente o palese per il pubblico interesse. Restano ferme, alle condizioni di legge, la possibilità di divulgazione pubblica e la denuncia all'Autorità giudiziaria o contabile.

Informazione e formazione

SISPI assicura informazioni chiare e facilmente accessibili sul canale interno, sulle condizioni per ricorrere al canale esterno ANAC e sulle tutele previste. Il gestore, il personale autorizzato e i soggetti che possono essere coinvolti nel processo ricevono formazione adeguata e periodica, in coerenza con le Linee Guida ANAC n. 1/2025 e con la Guida operativa Confindustria aggiornata nel 2026.

Per eventuali comunicazioni all'Organismo di Vigilanza che non costituiscano segnalazioni whistleblowing resta disponibile l'indirizzo odv@sispi.it. Le segnalazioni protette devono invece essere inoltrate attraverso i canali individuati dal Regolamento Whistleblowing, al fine di assicurare l'applicazione delle specifiche garanzie di legge.

CAPITOLO 9

ADOZIONE DEL MODELLO e CRITERI DI AGGIORNAMENTO E ADEGUAMENTO

9.1 Aggiornamento ed adeguamento

L'Organo di gestione adotta il MOGC con atto deliberativo. Gli aggiornamenti meramente descrittivi, che si limitano a recepire variazioni formali o anagrafiche e non incidono sulla struttura del Modello, sulla mappatura dei rischi, sui protocolli, sulle responsabilità, sui flussi informativi o sul sistema disciplinare, possono essere incorporati senza una nuova delibera, previa informativa all'OdV e ferma la successiva presa d'atto dell'Organo di gestione.

Sono invece modifiche sostanziali, riservate alla deliberazione dell'Organo di gestione anche quando proposte dall'OdV, quelle rese necessarie o opportune dai seguenti fattori:

- ✓ modifiche normative, organizzative o di processo;
- ✓ introduzione o modifica rilevante di attività o tecnologie;
- ✓ esiti del risk assessment, dei controlli e degli audit;
- ✓ violazioni significative, segnalazioni rilevanti o incidenti;
- ✓ altre circostanze idonee a incidere sul profilo di rischio o sull'efficacia dei presidi.

Il termine triennale costituisce il limite massimo entro il quale effettuare un riesame organico del MOGC. Resta fermo l'obbligo di procedere tempestivamente alla valutazione e, ove necessario, all'aggiornamento del Modello in presenza di modifiche normative, organizzative, tecnologiche o di processo, nonché di variazioni del profilo di rischio o di altri eventi rilevanti per l'idoneità e l'efficace attuazione dei presidi.

APPENDICE A
CATALOGO DEI REATI-PRESUPPOSTO EX D.lgs. 231/2001

Nota di aggiornamento. *Il presente catalogo è aggiornato alla data di approvazione/revisione del Modello e costituisce parte integrante dello stesso. Esso deve essere oggetto di verifica periodica e, ove necessario, di tempestivo aggiornamento in occasione di modifiche normative che incidano sul catalogo dei reati-presupposto o sul relativo apparato sanzionatorio.*

In base al D.lgs. 231/2001, l'Ente può essere ritenuto responsabile soltanto per la commissione dei reati espressamente richiamati dal D.lgs. 231/2001 o da altri provvedimenti normativi (ad es. art. 10 L. 146/2006 in tema di "Reati transnazionali"), se commessi nel suo interesse o a suo vantaggio dai soggetti qualificati ex art. 5, comma 1, del Decreto stesso.

Le fattispecie di reato richiamate dal D.lgs. 231/2001 sono (alla data) comprese, nelle seguenti macro-categorie:

- *Reati contro la Pubblica Amministrazione ed il Patrimonio (art. 24 e 25 D.lgs. 231/2001);*
- *Delitti informatici e trattamento illecito di dati (Art. 24-bis, D.lgs. 231/2001);*
- *Delitti di criminalità organizzata (Art. 24-ter, D.lgs. 231/2001);*
- *Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis, D.lgs. 231/2001);*
- *Delitti contro l'industria e il commercio (Art. 25-bis.1, D.lgs. 231/2001);*
- *Reati societari (Art. 25-ter, D.lgs. 231/2001);*
- *Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (Art. 25-quater, D.lgs. 231/2001);*
- *Pratiche di mutilazione degli organi genitali femminili (Art. 25-quater.1, D.lgs. 231/2001);*
- *Delitti contro la personalità individuale (Art. 25-quinquies, D.lgs. 231/2001);*
- *Reati di abuso di mercato (Art. 25-sexies, D.lgs. 231/2001);*
- *Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Art. 25-septies, D.lgs.*

231/2001);

- *Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-octies, D.lgs. 231/2001);*
- *Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1 D.lgs. 231/2001);*
- *Reati in materia di violazione di misure restrittive dell'Unione europea (Art. 25-octies.2., D.lgs. 231/2001);*
- *Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.lgs. 231/2001);*
- *Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria (Art. 25-decies, D.lgs. 231/2001);*
- *Reati ambientali (Art. 25-undecies, D.lgs. 231/2001);*
- *Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies, D.lgs. 231/2001);*
- *Razzismo e xenofobia (art.25-terdecies, D.lgs. 231/2001);*
- *Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art.25-quaterdieces, D.lgs. 231/2001);*
- *Reati tributari (art. 25-quinquiesdecies, D.lgs. 231/2001);*
- *Reati di contrabbando (art. 25-sexiesdecies, D.lgs. 231/2001);*
- *Reati contro il patrimonio culturale (art. 25- septiesdecies, D.lgs. 231/2001);*
- *Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25- duodevicies, D.lgs. 231/2001);*
- *Delitti contro gli animali (art. 25-undevicies, D.lgs. 231/2001)*
- *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].*

La legge 16 marzo 2006, n. 146 recante "Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001", entrata in vigore

sul piano internazionale il 1° settembre 2006, ha introdotto nell'ordinamento italiano la punibilità per i cosiddetti "Reati Transnazionali". Si tratta di delitti di un certo rilievo, commessi da gruppi organizzati che, in considerazione del superamento dei confini nazionali nelle fasi di ideazione, preparazione, esecuzione, controllo o effetti, coinvolgano più Stati. Tali reati, seppur richiamati in altra disposizione di legge (la Legge 146/2006), costituiscono anch'essi reati-presupposto della Responsabilità amministrativa degli enti definita dal D.lgs. 231/2001, e, pertanto, anche ad essi si applica la disciplina del Decreto.