AeGi sRL INDUSTRIAL AUTOMATION	**SGI - Sistema Gestione Integrato**	**FRAMEWORK PRINCIPALE: MOG231** **CODICE: MAN-231-001** **REV.: 00** DATA: 06/11/2026

Modello 231 - Parte generale

0.1 Indice

0.2 Parte Generale

PARTE GENERALE

Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001

0.3 Termini e Definizione

MOGC/Modello: il modello di organizzazione, gestione e controllo secondo i requisiti del D. Lgs. 231/2001.

ODV: Per Organismo di Vigilanza si intende l'organismo interno di controllo, preposto alla vigilanza sul funzionamento e sull'osservanza del modello.

Organi Sociali: sono gli organi societari previsti dallo statuto.

CCNL: contratto collettivo nazionale di lavoro nonché i contratti integrativi aziendali.

ANAC: Autorità Nazionale Anticorruzione.

D.Lgs. n. 231/2001 o Decreto: il D.Lgs. 8 giugno 2001 n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300" e successive modifiche ed integrazioni.

Dipendenti: sono i soggetti che svolgono in favore della società una prestazione lavorativa, alle dipendenze e sotto la direzione della società con contratto a tempo indeterminato o determinato, full time o part time. I lavoratori con contratto di collaborazione autonoma, interinali e tirocinanti sono equiparati ai dipendenti per quanto riguarda l'osservanza delle norme del D. Lgs. 231/2001.

Fornitori: sono i soggetti che forniscono alla Società beni e/o servizi in virtù di accordi e/o contratti.

Linee Guida: sono i documenti emessi da associazioni di categoria o enti pubblici autorevoli in materia di D. Lgs. n. 231/2001.

Risk Assessment: è la metodologia strutturata di valutazione dei rischi e dei relativi controlli.

Stakeholders: soggetti portatori di interessi nei confronti dell'azienda, siano essi interni o esterni alla sfera aziendale.

Sistema di controllo interno: sono l'insieme dei protocolli e di azioni adottate dalla società allo scopo di prevenire i rischi.

Whistleblowing: disciplina la materia di segnalazioni a norma del Decreto Legislativo n. 24/2023.

Rating di Legalità: è un indicatore sintetico del rispetto di elevati standard di legalità da parte delle imprese che ne abbiano fatto richiesta.

1 Premessa

Il presente documento, corredato di tutti i suoi allegati, è il **MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO** ai sensi del Decreto Legislativo n. 231/2001, adottato da AEGI SRL. AEGI SRL intende garantire e promuovere la piena legalità dell'attività aziendale, a tal fine procede alla definizione e attuazione del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001 (Modello di Organizzazione). Sebbene il Decreto Legislativo indichi il Modello come facoltativo e non obbligatorio, la società è fermamente convinta che l'adozione di tale Modello costituisca un valido strumento di sensibilizzazione per tutti coloro che operano in nome e per conto della stessa. Pertanto, tutti coloro che si rapportano, a qualunque titolo, con AEGI SRL sono tenuti nell'espletamento delle proprie attività e/o funzioni, ad assumere comportamenti conformi alle prescrizioni disciplinate dal Modello. **La società ritiene che solo condotte conformi al Modello consentano di prevenire il rischio di commissione dei reati previsti dal D.Lgs. n. 231/2001**. Con l'adozione del MOGC, AEGI SRL predispone all'interno della società un catalogo organico di norme e procedure di controllo volto a neutralizzare i rischi di consumazione dei reati di cui al D. Lgs. n. 231/2001. AEGI SRL si impegna ad assicurare l'implementazione del modello adottato in modo da adeguarlo non solo ai costanti sviluppi normativi, ma

anche laddove si dovesse verificare la consumazione di uno dei reati presupposto previsti dal Decreto Legislativo. AEGI SRL assicura l'osservanza delle procedure mediante una capillare divulgazione, interna ed esterna, del codice etico, del modello ed i successivi aggiornamenti. AEGI SRL auspica di raggiungere i requisiti per l'attribuzione del **rating di legalità,** con il massimo punteggio possibile. Il rating di legalità è lo strumento sviluppato dall'AGCM, in accordo con il Ministero dell'Interno e della Giustizia, che certifica il possesso di elevati standard etici, di legalità, trasparenza e responsabilità sociale delle imprese. La funzione del rating è dare un giudizio alle aziende fornendo dei benefici ed incentivi a quelle più meritevoli, allo stesso tempo, in ragione del punteggio, si procede alla classificazione di aziende etiche e virtuose, le quali rappresentano lo standard da diffondere e promuovere. Al fine di garantire l'osservanza delle disposizioni contenute nel modello, AEGI SRL ha nominato un Organismo di Vigilanza con l'incarico di sorvegliare sul funzionamento, sull'efficacia e sull'osservanza del modello stesso, adottare azioni correttive e, infine, curarne l'aggiornamento continuativo. AEGI SRL ha scelto di redigere il modello in conformità alle Linee Guida di Confindustria, approvate dal Ministero dello Sviluppo Economico, le quali raccomandano: - di individuare per singolo settore o processo aziendale le aree di rischio nella quale si annida la possibile consumazione di uno dei reati presupposti di cui al decreto; - di adottare specifici protocolli atti a prevenire i rischi individuati; - la predisposizione di un idoneo sistema di controllo atto a prevenire i rischi; - di adottare un adeguato sistema disciplinare in caso di violazione delle norme del codice di condotta e dei protocolli previsti dal modello; - di affidare il compito di vigilare sul modello ad un Organismo di Vigilanza, i cui membri siano soggetti dotati di indubbia professionalità e moralità, ai quali deve essere garantita autonomia, indipendenza e continuità di azione; - la previsione di obblighi di informazione nei confronti dell'Organismo di Vigilanza. **Il Consiglio di Amministrazione ha proceduto, con propria determina, a nominare i membri dell'Organismo di Vigilanza, nel rispetto delle regole previste dal presente Modello.**

2 Il Decreto Legislativo N. 231/2001

2.1 La responsabilità amministrativa degli enti

Il Decreto Legislativo 8 giugno 2001, n. 231 (di seguito anche solo il *"Decreto"*), emanato in esecuzione della Legge Delega 29 settembre 2000, n. 300, ha introdotto nell'ordinamento giuridico nazionale " *la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica* ", in ottemperanza agli obblighi previsti da strumenti internazionali (Convenzione di Bruxelles del 26 luglio 1995 - sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione di Bruxelles del 26 maggio 1997 - sulla lotta alla corruzione nella quale sono coinvolti funzionari della Comunità Europea o degli Stati membri e la Convenzione OCSE del 17 dicembre 1997 - sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali) i quali stabiliscono i paradigmi di responsabilità delle persone giuridiche e il sistema sanzionatorio in caso di consumazione dei reati nell'interesse o vantaggio dell'ente. Con il D.Lgs. n. 231/2001 e successive modifiche ed integrazioni, il legislatore ha introdotto la " *responsabilità amministrativa degli enti* " benché definita *"amministrativa", si tratta di responsabilità di natura penale connessa alla consumazione di reati tassativamente previsti dal catalogo del Decreto (***c.d. reati presupposto – requisito oggettivo***).* La stessa Relazione al D. Lgs. n. 231/2001 parla di *"nascita di un tertium genus che coniuga i tratti essenziali del sistema penale e di quello amministrativo".* Quanto ai destinatari l'art. 1, comma 2, del Decreto n. 231 indica *"gli enti forniti di personalità giuridica, le società fornite di personalità giuridica e le società e le associazioni anche prive di personalità giuridica"*; Invece, sono esclusi ai sensi dell'art. 1, comma 3, *"allo Stato, agli enti pubblici-territoriali, agli altri enti pubblici non economici nonché agli enti che svolgono funzioni di rilievo costituzionale"*. Alla luce dell'interpretazione giurisprudenziale, nella platea dei destinatari del Decreto figurano anche società di diritto privato che esercitino un pubblico servizio - per esempio in base a un rapporto concessorio - e società controllate da pubbliche amministrazioni. In particolare, le Sezioni Unite della Cassazione

con la sentenza 28699 del 2010 hanno ritenuto le s.p.a. a partecipazione mista pubblico-privata soggette al decreto 231. Infatti, considerata la forma societaria, esse sono qualificate come Enti a carattere economico che non svolgono funzioni di rilievo costituzionale, ma al più intercettano nella loro attività valori di rango costituzionale. Al contrario, è stato superato il tentativo di includere le imprese individuali tra i destinatari della disciplina della responsabilità da reato degli Enti. La giurisprudenza di legittimità ha infatti confermato che il decreto 231 può applicarsi solo ai soggetti collettivi (Cass., VI sez. pen., 30085/2012). Ciò chiarito, affinché si configuri la responsabilità i reati presupposti devono essere commessi nell'interesse o a vantaggio dell'ente (**requisito oggettivo**).
L'interesse è la specifica finalità della condotta di colui che ha agito e caratterizza in senso soggettivo la condotta delittuosa della persona fisica mediante una verifica *ex ante*. Per contro, **il vantaggio** è un effetto della condotta di colui che ha agito e può essere anche indiretto e non patrimoniale, richiede sempre una verifica *ex post*. Tuttavia, quando il catalogo dei reati-presupposto è stato esteso per includervi anche quelli afferenti la tutela della salute e sicurezza sul lavoro (art. 25 septies del decreto 231) e poi, ancora, le fattispecie ambientali (art.25 undecies), si è posto un problema di compatibilità del criterio dell'interesse o vantaggio con i reati colposi. La giurisprudenza ha ritenuto che nei reati colposi l'interesse o vantaggio dell'ente andrebbe valutato con riguardo all'intera fattispecie di reato, non già rispetto all'evento dello stesso. Infatti, mentre nei reati-presupposto dolosi l'evento del reato ben può corrispondere all'interesse dell'ente, non può dirsi altrettanto nei reati-presupposto a base colposa, attesa la contro-volontà, che caratterizza questi ultimi ai sensi dell'articolo 43 del codice penale. Si pensi, infatti, ai reati in materia di salute e sicurezza: difficilmente l'evento lesioni o morte del lavoratore può esprimere l'interesse dell'ente o tradursi in un vantaggio per lo stesso. Ancora alla violazione colposa dell'obbligo della ditta appaltatrice di adottare adeguate misure preventive, cui consegua l'evento delittuoso, che abbiano consentito, secondo i criteri economici, l'aggiudicazione dell'appalto adottati dalla committente o, ancor di più, la violazione dell'obbligo di valutare la congruità dei costi della sicurezza (art. 26, comma 6, D. Lgs. n. 81/2008). In questi casi, dunque, l'interesse o vantaggio dovrebbero piuttosto riferirsi alla condotta inosservante delle norme cautelari. Così, l'interesse o vantaggio dell'ente potrebbero ravvisarsi nel risparmio dei costi per la sicurezza ovvero nel potenziamento della velocità di esecuzione delle prestazioni o nell'incremento della produttività, sacrificando l'adozione di presidi antinfortunistici (Cfr. Cass., IV Sez. pen., sent. n. 16713/2018, Cass., IV Sez. pen., sent. n. 48779/2019, Cass. pen. Sez. III, sent. n. 3157/2019, Cass., IV Sez. pen., sent. n.3731/2020). A partire da queste premesse, alcune pronunce giurisprudenziali hanno ravvisato l'interesse nella «tensione finalistica della condotta illecita dell'autore volta a beneficiare l'ente stesso, in forza di un giudizio ex ante, ossia da riportare al momento della violazione della norma cautelare». Si ritengono imputabili all'Ente solo le condotte consapevoli e volontarie finalizzate a favorire l'Ente. Per contro, sarebbero irrilevanti le condotte derivanti dalla semplice imperizia, dalla mera sottovalutazione del rischio o anche dall'imperfetta esecuzione delle misure antinfortunistiche da adottare. In questo modo, si riflette fedelmente il sistema del decreto 231 che mostra di considerare disgiuntamente i due concetti interesse e vantaggio anche nei reati colposi. Tali condotte devono essere poste in essere da parte di soggetti determinati dal Decreto: - **SOGGETTI APICALI**: persone che rivestono funzioni di rappresentanza, amministrazione o direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, di fatto, la gestione e il controllo della stessa; - **SOGGETTI SUBORDINATI**: persone sottoposte alla direzione o vigilanza di uno dei soggetti sopra indicati. Restano escluse dalla responsabilità amministrativa (penale) della persona giuridica le ipotesi in cui il soggetto agente abbia commesso il fatto nell'interesse esclusivo proprio o di terzi estranei all'ente. È importante sottolineare che la responsabilità dell'Ente può sussistere anche laddove il dipendente, autore dell'illecito, abbia concorso nella sua realizzazione con soggetti estranei all'organizzazione dell'Ente medesimo. Tale ipotesi è chiaramente rappresentata nel codice penale e, in particolare, negli art. 110 c.p. " *Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita* " e art. 113 c.p. " *Nel delitto colposo, quando l'evento è stato cagionato dalla cooperazione di più persone, ciascuna di queste soggiace alle pene stabilite per il delitto stesso* ". Diversi possono essere i settori di *business* nei quali può annidarsi più facilmente il rischio del coinvolgimento in concorso del dipendente e quindi, ricorrendone i presupposti di interesse e/o vantaggio, dell'Ente. In particolare, rilevano i rapporti connessi agli appalti e, in generale, i contratti di *partnership*. Con riferimento al tipo di attività svolta dalla società i reati-presupposto in materia ambientale, come la gestione non autorizzata di rifiuti (art. 256, D.Lgs. n. 152/2006), nei casi

di mancata valutazione preliminare del committente circa la sussistenza dei requisiti di legge in capo alle ditte potenziali appaltatrici, ovvero di accettazione pedissequa di condizioni economiche di particolare vantaggio, se non addirittura fuori mercato. Altro ambito è quello riguardante il rischio di partecipazione concorsuale da parte del committente che manchi di considerare - o escluda in modo non motivato - taluni indici di valutazione previsti per legge ai fini della selezione dei propri *partners* commerciali. In proposito rilevano, ad esempio, le c.d. *white lists* previste dalla Legge n. 190/2012 e disciplinate dal DPCM del 18 aprile 2013, entrato in vigore il 14 agosto 2013. In attuazione di questa disciplina, presso le Prefetture è stato istituto l'elenco dei fornitori, prestatori di servizi ed esecutori di lavori non soggetti a tentativo di infiltrazione mafiosa, operanti nei settori esposti maggiormente a rischio. L'iscrizione nell'elenco, che è di natura volontaria, soddisfa i requisiti per l'informazione antimafia per l'esercizio dell'attività per cui è stata disposta l'iscrizione ed è valida per dodici mesi, salvi gli esiti delle verifiche periodiche. Al riguardo, si rileva che la mancata valutazione di tali indici di rischio può determinare l'accertamento di un'ipotesi concorsuale in ordine a gravi reati-presupposto. In questi casi, peraltro, non si può escludere il rischio che l'impresa committente venga coinvolta a titolo di colpa nei reati intenzionalmente compiuti dalle imprese criminali, per aver trascurato di valutare in via preliminare il suo potenziale partner alla luce delle specifiche indicazioni di pericolosità previste dalla legge. Il concorso nel reato può rilevare ai fini della responsabilità dell'Ente anche nella particolare ipotesi del c.d. concorso dell' *extraneus* nel reato *"proprio"*. In particolare, la responsabilità in concorso dell' *extraneus* può ricorrere laddove costui, consapevole della particolare qualifica soggettiva del suo *partner* criminale (es.pubblico ufficiale, testimone, sindaco, ecc.), concorra nella condotta di reato proprio a quest'ultimo ascrivibile (es. abuso in atti d'ufficio). In tal caso, l' *extraneus* risponderà in concorso del medesimo reato previsto a carico del soggetto qualificato. Al riguardo, la giurisprudenza di legittimità ha chiarito che *"ai fini dell'applicabilità dell'art. 117 c.p., che disciplina il mutamento del titolo del reato per taluno dei concorrenti, è necessaria, per l'estensione del titolo di reato proprio al concorrente* extraneus*, la conoscibilità della qualifica soggettiva del concorrente* intraneus " (Cass. Pen. Sez. VI, Sent. n. 25390/2019). La fattispecie sopra considerata potrebbe realizzarsi, in concreto, nel caso del dipendente di un'impresa che, approfittando di rapporti personali con il funzionario pubblico preposto al rilascio di determinati permessi e/o autorizzazioni, prenda contatto con quest'ultimo per ottenere un provvedimento favorevole nell'interesse dell'impresa, pur consapevole di non averne diritto. In un caso del genere, il dipendente potrebbe supportare il funzionario pubblico fornendogli pareri legali e documenti utili ai fini del perfezionamento del reato. La condotta del funzionario che rilascia il provvedimento non dovuto si inquadrerebbe nella fattispecie dell'abuso d'ufficio (art. 323 c.p.), che si configura come reato *"proprio"*. Tuttavia, il dipendente (e con lui l'impresa nel cui interesse lo stesso abbia agito) risponderebbe a titolo di concorso dell' *extraneus* nel reato *"proprio"*, in quanto nella sua condotta si rinverrebbero: a) la consapevolezza della funzione di pubblico ufficiale del soggetto contattato; b) consapevolezza dell'antigiuridicità della condotta richiesta; c) partecipazione attiva alla concretizzazione della condotta stessa. Ciò soprattutto per favorire un'attenta selezione e successiva gestione dei propri *partners* e interlocutori, sia pubblici che privati. Quanto all'ambito di applicazione territoriale della responsabilità, dipendente dal reato dell'Ente. L'articolo 4 del Decreto 231 disciplina i reati commessi all'estero e prevede, che gli Enti aventi la sede principale nel territorio dello Stato, rispondono anche in relazione ai reati commessi all'estero nei casi e alle condizioni previsti dagli articoli da 7 a 10 del codice penale, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto. Pertanto, l'Ente è perseguibile quando: - in Italia ha la sede principale, cioè la sede effettiva ove si svolgono le attività amministrative e di direzione, eventualmente anche diversa da quella in cui si trova l'azienda o la sede legale (Enti dotati di personalità giuridica), ovvero il luogo in cui viene svolta l'attività in modo continuativo (Enti privi di personalità giuridica); - nei suoi confronti non sta procedendo lo Stato del luogo in cui è stato commesso il fatto; - la richiesta del Ministro della Giustizia, cui sia eventualmente subordinata la punibilità, è riferita anche all'Ente medesimo. Tali regole riguardano i reati commessi interamente all'estero da soggetti apicali o sottoposti. Quanto all'ambito di applicazione della disposizione in esame, è soggetto alla normativa italiana - quindi anche al Decreto 231 - ogni Ente costituito all'estero in base alle disposizioni della propria legislazione domestica, che abbia, però, in Italia la sede dell'amministrazione o l'oggetto principale, sul punto la Giurisprudenza ha osservato che: " *Si deve affermare il principio di diritto secondo il quale la persona giuridica è chiamata a rispondere dell'illecito amministrativo derivante da un reato-presupposto per il quale sussista la giurisdizione nazionale commesso dai*

propri legali rappresentanti o soggetti sottoposti all'altrui direzione o vigilanza, in quanto l'ente è soggetto all'obbligo di osservare la legge italiana e, in particolare, quella penale, a prescindere dalla sua nazionalità o dal luogo ove esso abbia la propria sede legale ed indipendentemente dall'esistenza o meno nel Paese di appartenenza di norme che disciplinino in modo analogo la medesima materia anche con riguardo alla predisposizione e all'efficacia attuazione di modelli di organizzazione e di gestione atti ad impedire la commissione di reati a fonte della responsabilità amministrativa dell'ente stesso. Deve, pertanto, essere recepito l'analogo principio di diritto recentemente affermato dalla giurisprudenza di merito la dove ha ritenuto applicabile la disciplina del decreto n. 231 ad una società straniera priva di sede in Italia, ma operante sul territorio nazionale, in relazione ai delitti di omicidio e lesioni personali colpose, Cass. Pen. Sez. VI n. 11626 del 11/02/2020)". Ne deriva il problema del riconoscimento da parte dell'ordinamento italiano dell'efficacia esimente dei Modelli organizzativi adottati in base a leggi straniere. Tali Modelli potranno ritenersi idonei a spiegare efficacia esimente laddove rispondano ai requisiti previsti dal Decreto 231 e risultino efficacemente attuati. Infine, occorre dare atto che la Legge 146 del 2006, che ha ratificato la Convenzione e i Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 e il 31 maggio 2001, ha previsto all'articolo 10 la responsabilità degli Enti per alcuni reati aventi carattere transnazionale, quali ad esempio associazione per delinquere anche di tipo mafioso, associazione finalizzata al traffico di sostanze stupefacenti, traffico di migranti. Ai fini della qualificabilità di una fattispecie criminosa come *"reato transnazionale"*, è necessaria la sussistenza delle condizioni indicate dal legislatore. In particolare: - nella realizzazione della fattispecie, deve essere coinvolto un gruppo criminale organizzato; - il fatto deve essere punito con la sanzione non inferiore nel massimo a 4 anni di reclusione; - è necessario che la condotta illecita sia, alternativamente: - commessa in più di uno Stato; - commessa in uno Stato ma abbia effetti sostanziali in un altro Stato; - commessa in un solo Stato, sebbene una parte sostanziale della sua preparazione o pianificazione o direzione e controllo debbano avvenire in un altro Stato; - commessa in uno Stato, ma in essa sia coinvolto un gruppo criminale organizzato protagonista di attività criminali in più di uno Stato. La responsabilità "amministrativa" presuppone l'accertamento delle condotte nell'ambito del processo penale a carico degli autori dei reati, ma è autonoma rispetto alla responsabilità della persona fisica che ha commesso il reato. In altri termini l'ente potrà essere dichiarato responsabile anche se la persona fisica che ha commesso il reato non è imputabile ovvero non è stata individuata, oppure nel caso in cui il reato si estingua per una causa diversa dall'amnistia. In via preliminare, in fase di indagine, laddove l'Autorità Giudiziaria accerti l'esistenza del *fumus* del reato è ammesso il sequestro per quote del patrimonio dell'ente. Accertata la responsabilità, le sanzioni amministrative applicabili all'ente consistono sia in **sanzioni di natura pecuniaria**, commisurata sia alla gravità del reato che alla capacità patrimoniale dell'ente, che **misure interdittive,** quali la sospensione o revoca di licenze e concessioni, il divieto di contrattare con la Pubblica Amministrazione, l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi. La sanzione è erogata con sentenza nel contesto garantistico del processo penale, ove sia accertata la sussistenza di tutti i requisiti oggettivi e soggettivi previsti dal legislatore. È altresì prevista la **confisca di beni** o la **pubblicazione della sentenza**. Infine, occorre considerare che la responsabilità dell'impresa può ricorrere anche se il delitto-presupposto si configura nella forma del tentativo (art. 26, Decreto n. 231), vale a dire quando il soggetto agente compie atti idonei in modo non equivoco a commettere il delitto e l'azione non si compie o l'evento non si verifica (art.56 c.p.). In tal caso, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà. Inoltre, l'Ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento. Sul **piano soggettivo**, l'Ente risponde se non ha adottato le misure necessarie atte ad impedire la commissione di reati del tipo di quello realizzato. In particolare, se il reato è commesso da soggetti apicali, l'Ente è responsabile se non dimostra che: - ha adottato ma anche efficacemente attuato, prima della commissione del fatto, Modelli di organizzazione e gestione idonei a impedire reati della specie di quello commesso (art. 6, comma 1, lett. A) Decreto 231); - ha istituito un Organismo dotato di autonomi poteri di iniziativa e controllo, il quale abbia effettivamente vigilato sull'osservanza dei Modelli; - il reato è stato commesso per fraudolenta elusione dei Modelli da parte del soggetto apicale infedele. Ove la società si sia dotata di un MOGC, se il fatto è realizzato da un soggetto sottoposto, la Pubblica Accusa deve provare che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza da parte degli apicali. Questi obblighi non possono ritenersi violati se prima della commissione del

reato l'Ente abbia adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi (art. 7, comma 2). Tale Modello deve prevedere, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento delle attività nel rispetto della legge e a scoprire ed eliminare tempestivamente eventuali situazioni di rischio. Dunque, l'efficace attuazione del Modello richiede, in via principale: i) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività o vi sia una modifica normativa che possa incidere negativamente nell'Ente in virtù dell'attività svolta; ii) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello; iii) adeguate iniziative di formazione e informazione del personale.

3 I reati "PRESUPPOSTO"

Il legislatore ha inizialmente focalizzato la propria attenzione ai soli reati contro la Pubblica Amministrazione salvo intervenire successivamente a più riprese per rafforzare la normativa nazionale ed adeguarla alle convenzioni internazionali. Le fattispecie di reato suscettibili di configurare la responsabilità amministrativa dell'Ente (cd. reati-presupposto) sono soltanto quelle espressamente richiamate dal legislatore nel Decreto (principio di tassatività), notevolmente ampliato nel corso degli anni in virtù di modifiche apportate dal legislatore anche sotto la spinta europeista e per effetto di provvedimenti normativi successivi. Segue la rubrica dei reati di cui al D.Lgs. n. 231/01, fonte di responsabilità amministrativa dell'ente.

Art. 24 D.Lgs. n. 231/2001 - modificato dalla L. n. 137/2023 Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture.

-Malversazione di erogazioni pubbliche (art. 316-*bis* c.p.) [modificato dal D.L. n. 4/2022 e convertito con L. n. 13/2022]; - Indebita percezione di erogazioni pubbliche (art. 316-*ter* c.p.) [modificato dalla L. n. 3/2019 convertito con L. n. 13/2022]; - Turbata libertà degli incanti (art. 353 c.p.) [introdotto dalla L. n. 137/2023]; - Turbata libertà del procedimento di scelta del contraente (art. 353-*bis* c.p.) [introdotto dalla L. n. 137/2023]; - Frode nelle pubbliche forniture (art. 356 c.p.) [introdotto dal D.Lgs. n. 75/2020]; - Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640, comma 2, n.1, c.p.) [modificato dal D.Lgs. n. 75/2020 e modificato dalla L. n. 90/2024]; - Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.) [modificato dal D. L. n. 13/2022]; - Frode ai danni del Fondo europeo agricolo (art. 2. L. 23.12.1986, n. 898) [articolo aggiunto dal D. Lgs. n. 75/2020]; - Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-*ter* c.p.) [modificato dal D.Lgs. n. 150/2022].

Art. 24 bis D.Lgs. n. 231/2001 - articolo aggiunto dalla L. n. 48/2008 ultima modifica L. n. 90/2024. Delitti informatici e trattamento illecito di dati.

- Documenti informativi (art. 491-bis c.p.); - Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) [modificato dalla L. n. 90/2024]; - Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.) [modificato dalla L. n. 90/2024]; - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) [modificato dalla L. n. 90/2024]; - detenzione, diffusione e installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) [modificato dalla L. n. 90/2024]; - Estorsione informatica (art.629, comma terzo, c.p.) [aggiunto dalla L. n. 90/2024]; - Danneggiamento di informazioni, dati e programmi

informatici (art. 635-bis c.p.) [modificato dalla L. n. 90/2024]; - Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-ter c.p.) [modificato dalla L. n. 90/2024]; - Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) [modificato dalla L. n. 90/2024]; - Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635 quater.1 c.p.) [introdotto dalla L. n. 90/2024]; - Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.) [modificato dalla L. n. 90/2024]; - Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.); - Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art.1, comma 11, D.L. n. 105/2019).

Art. 24 ter D.Lgs. n. 231/01 - articolo aggiunto dalla L. n. 94/2009 e modificato dalla L. 6n. 9/2015. Delitti di criminalità organizzata.

- Associazione per delinquere (art. 416 c.p.p.); - Associazione di tipo mafioso (art. 416-bis c.p.) [articolo modificato dalla L. n. 69/2015]; - Scambio elettorale politico-mafioso (art. 416 ter c.p.) [modificato dall'art. 1, comma 1, L. del 1/4/2014 n. 63 a decorre dal 18/4/2014 ai sensi di quanto disposto dall'art. 2 della medesima legge]; - Sequestro di persona a scopo di estorsione (art. 630 c.p.); - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 9 ottobre 1990, n. 309) [introdotto dal comma 7 bis del D.Lgs. n. 202/2016]; - Tutti i delitti se commessi avvalendosi delle condizioni previste dall´art. 416-bis c.p. per agevolare l'attività delle associazioni previste dallo stesso articolo [L. n. 203/91, oggi art. 416 bis 1 modificato dalla L. n. 60/2023]; - Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, comma 2, lett. a), numero 5), c.p.p.).

Art. 25 D.Lgs. n. 231/2001 - articolo aggiunto dalla L. n. 94/2009 e modificato dalla L. n. 69/2015 e dal D.Lgs. n. 75/2020, dalla L. n. 112/2024 e dalla L. n. 114/2024. Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione.

- Peculato (art. 314, comma 1, c.p.) [aggiunto da D.Lgs. n. 75/2020 e dalla L. n. 112/2024]; - Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.) [aggiunto dalla L. n. 112/2024]; - Peculato mediante profitto dell'errore altrui (art. 316 c.p.) [aggiunto dal D.Lgs. n. 75/2020 e modificato dalla L. n. 112/2024]; - Concussione (art. 317 c.p.); - Corruzione per l'esercizio della funzione (art. 318 c.p.) [modificato dalla L. n. 190/2012 e dalla L. n. 69/2015 e dalla L. n. 3/2019]; - Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.) [modificato dalla L. n. 69/2019]; - Circostanze aggravanti (art. 319-*bis* c.p.); - Corruzione in atti giudiziari (art. 319-*ter* c.p.) [articolo modificato dalla L. n. 69/2015]; - Induzione indebita a dare o promettere utilità (art. 319-*quater*) [articolo aggiunto dalla L. n. 190/2012 modificato dalla L. n. 69/2015 e dal D.Lgs. n. 75/2020]; - Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.); - Pene per il corruttore (art. 321 c.p.); - Istigazione alla corruzione (art. 322 c.p.); - Traffico di influenze illecite (art. 346-*bis* c.p.) [modificato dalla L. n. 3/2019 e dalla L. n. 114/2024]; - Peculato, concussione, indizione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, abuso d'ufficio, di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-*bis* c.p.) [modificato dalla L. n. 112/2024].

Art. 25-bis D.Lgs. n. 231/2001 - articolo aggiunto dal D.L. n. 350/2001, convertito e modificato dalla L. n. 409/2001; modificato dalla L. n. 99/2009 e dal D.Lgs. n. 125/2016. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.); - Alterazione di monete (art. 454 c.p.); - Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.); - Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.); -

Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.); - Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.); - Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.); - Uso di valori di bollo contraffatti o alterati (art. 464 c.p.); - Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.); - Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

Art. 25-bis.1 D.Lgs. n. 231/2001 - articolo aggiunto dalla L. n. 99/2009 modificato dalla L. n. 75/2026. Delitti contro l'industria e il commercio

-Turbata libertà dell'industria o del commercio (art. 513 c.p.); - Illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.); - Frodi contro le industrie nazionali (art. 514); - Frode nell'esercizio del commercio (art. 515 c.p.); - Vendita di prodotti industriali con segni mendaci (art. 517 c.p.); - Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.); - Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.) [modificato dalla L. 75/2026].

Art. 25-ter D.Lgs. n. 231/2001 - articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. n. 69/2015, nonché dal D.Lgs. n. 19/2023. Reati societari.

-False comunicazioni sociali (art. 2621 c.c.) [modificato dalla L. n. 69/2015]; - Fatti di lieve entità (art. 2621 bis c.c.); - False comunicazioni sociali delle società quotate (art. 2622) [modificato dalla L. n. 69/2015]; - Impedito controllo (art. 2625, comma 2, c.c.); - Indebita restituzione di conferimenti (art. 2626 c.c.); - Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.); - Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.); - Operazioni in pregiudizio dei creditori (art. 2629 c.c.); - Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.) [aggiunto dalla L. n. 262/2005]; - Formazione fittizia del capitale (art. 2632 c.c.); - Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.); - Corruzione tra privati (art. 2635 c.c.) [aggiunto dalla L. n. 190/2012 modificato dalla L. n. 3/2019]; - Istigazione alla corruzione tra privati (art. 2635 bis co 1 c.c.); - Illecita influenza sull'assemblea (art. 2636 c.c.); - Aggiotaggio (art. 2637 c.c.); - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.); - Falso in prospetto (173-bis D.Lgs. n. 58/1988); - False o omesse dichiarazioni per il rilascio del certificato preliminare previsto dalla normativa attuativa della Direttiva (UE) 2019/2121 [ART. 54 aggiunto dal D.Lgs. n. 19/2023].

Art. 25-quater D.Lgs. n. 231/2001 - articolo aggiunto dalla L. n. 7/2003. Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali.

- Associazioni sovversive (art. 270 c.p.); - Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.); - Assistenza agli associati (art. 270 ter c.p.); - Arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.); - Organizzazione di trasferimento per finalità di terrorismo (art. 270-quater.1); - Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies c.p.); - Finanziamento di condotte con finalità di terrorismo (art. 270-quinquies.1 c.p.) - Sottrazione di beni o denaro sottoposti a sequestro (art. 270-quinquies.2 c.p.); - Detenzione di materiale con finalità di terrorismo (art. 270-quinquies.3); - Condotte con finalità di terrorismo (art. 270 sexies c.p.); - Attentato per finalità terroristiche o di eversione (art. 280 c.p.); - Atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis c.p.); - Atti di terrorismo nucleare (art. 280-ter c.p.); - Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.); - Sequestro a scopo di coazione (art. 289-ter c.p.); - Istigazione a commettere alcuno dei delitti

preveduti dai Capi primo e secondo (art. 302 c.p.); - Cospirazione politica mediante accordo (art. 304 c.p.); - Cospirazione politica mediante associazione (art. 305 c.p.); - Banda armata: formazione e partecipazione (art. 306 c.p.); - Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.); - Fabbricazione o detenzione di materie esplodenti (Art. 435 c.p.) [Introdotto e modificato dal D. L. n. 48 dell'11 aprile 2025 convertito dalla L. n. 80 del 9 giugno 2025]; - Impossessamento, dirottamento e distruzione di un aereo (L. n. 342/1976, art. 1); - Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2); - Sanzioni (L. n. 422/1989 art. 3); - Pentimento operoso (D.Lgs. n. 625/1979 art. 5); - Convenzione di New York del 9 dicembre 1999 (art. 2)

Art. 25-quater.1 D.Lgs. n. 231/2001 - articolo aggiunto dalla L. n. 7/2006. Pratiche di mutilazione degli organi genitali femminili.

- Pratiche di mutilazione degli organi genitali femminili (Art. 583-bis c.p.)

Art. 25-quinquies D.Lgs. n. 231/2001 - articolo aggiunto dalla L. n. 228/2003 modificato dalla L. n. 199/2016 e dalla L. n. 238/2021 e dal D.Lgs n. 115/2026. Delitti contro la personalità individuale.

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.): - Prostituzione minorile (art. 600 bis c.p.): - Pornografia minorile (art. 600-ter c.p.); - Detenzione di materiale pornografico (art. 600-quater) [modificato L. n. 238/2021]; - Pornografia virtuale (art. 600-quater.1 c.p.) [aggiunto dall'art. 10, L. 6 febbraio 2006 n. 38]; - Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.): - Tratta di persone (art. 601 c.p.); - Approfittamento della vittima di riduzione in schiavitù o di tratta (art. 601.1 c.p.) [aggiunto dall'art. 3, comma 1, lettera c, D.Lgs. n. 115/2026]; - Acquisto e alienazione di schiavi (art. 602 c.p.); - Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.); - Adescamento di minorenni (art. 609-undecies c.p.);

Art. 25-sexies D.Lgs. n. 231/2001 - articolo aggiunto dalla L. n. 62/2005. Reati di abuso di mercato.

- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 D. Lgs. n. 58/1998); - Manipolazione del mercato (art. 185 D. Lgs. n. 58/1998) **[**Modificato da Legge n.238 del 23 dicembre 2021 e dalla Legge n.132 del 23 settembre 2025]; - Abuso e comunicazione illecita di informazioni privilegiate (art. 187-bis TUF); - Manipolazione del mercato (Art. 187-ter TUF) [modificato dal D.Lgs n.107/2018 modificato dal D. Lgs n.107 del 10 agosto 2018]; - Sanzioni relative alle violazioni delle disposizioni del regolamento (UE) n. 596/2014 del parlamento Europeo e del Consiglio, del 16 aprile 2014 (art. 187-ter.1 TUF) [modificato dal D.Lgs n. 128/2026 del 25/06/2026]; - Responsabilità dell'ente (art. 187-quinquies TUF) [modificato dal D.Lgs n. 128/2026 del 25/06/2026]; - Divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art. 14 REG. UE. n. 596/2014); - Divieto di manipolazione del mercato (art. 15 REG. UE. n. 596/2014); - Divieto di abuso di informazioni privilegiate (art. 89 REG. UE. n. 1114/2023 recepito da D.Lgs. n. 129/2024); - Divieto di divulgazione illecita di informazioni privilegiate (art. 90 REG. UE. n. 1114/2023 recepito da D.Lgs. n. 129/2024); - Divieto di manipolazione del mercato (art. 91 REG. UE. n. 1114/2023 recepito da D.Lgs. n. 129/2024);

Art. 25-septies D.Lgs. n. 231/2001 - articolo aggiunto dalla L. n. 123/2007. 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.

- Omicidio colposo (art. 589 c.p.); - Lesioni personali colpose (art. 590 c.p.); - Sanzione per il datore di lavoro e dirigente (art. 55 D.Lgs. n. 81/2008 e s.m.i.)

Art. 25 octies D.Lgs. n. 231/2001 - articolo aggiunto dal D.Lgs. n. 231/2007; modificato dalla L. n. 186/2014. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio.

- Ricettazione (art. 648 c.p.) [modificato dal D.Lgs. n. 195/2021; D.L. n. 23/2026 e L. n. 54/2026]; - Riciclaggio (art. 648-*bis* c.p.) [modificato dal D.Lgs. n. 195/2021]; - Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.) [modificato dal D.Lgs. n. 195/2021]; - Auto-riciclaggio (art. 648-*ter*.1 c.p.) [modificato dal D.Lgs. n. 195/2021];

Art. 25 octies.1 D.Lgs. n. 231/2001 - articolo introdotto dal D.Lgs. n. 184/2021 modificato dalla L. n. 137/2023. Delitti in materia di strumenti di pagamento diversi dai contanti.

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-*ter* c.p.) [modificato dal D.Lgs. n.184/2021]; - Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-*quater* c.p.) [introdotto dal D.Lgs. n. 184/2021]; - Trasferimento fraudolento di valori (art. 512 -*bis* c.p.) [introdotto dal D.L. n. 105/2023 e convertito con L. n. 137/2023 modificato dal D.L. n. 19/2024 convertito in L. n. 56/2024]; - Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-*ter*, comma 2, c.p.) [modificato dal D.Lgs. n. 184/2021];

Art. 25-octies.2 D.Lgs. n. 231/2001 - articolo aggiunto dal D.L.gs. n. 211/2025. Reati in materia di violazione di misure restrittive.

- Violazione delle misure restrittive dell'Unione Europea (art. 275-bis c.p.); - Violazione degli obblighi informativi imposti da una misura restrittiva dell'Unione Europea (art. 275-ter c.p.); - Violazione delle condizioni dell'autorizzazione allo svolgimento di attività (artt. 275-quater c.p.); - Morte o lesioni come conseguenza di delitti in materia di immigrazione clandestina (art. 12, comma 1bis. D.lgs. 286/1998);

Art. 25-novies D.Lgs. n. 231/2001 - articolo aggiunto dalla L. n. 99/2009; modificato dalla L. n. 93/2023 e dalla L. n. 166/2024. Delitti in materia di violazione del diritto d'autore.

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, comma 1 lett. A bis, L. n. 633/1941); - Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, comma 3, L. n. 633/1941); - Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis, comma 1, L. n. 633/1941 modificato dalla L. n. 166/2024); - Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171 -bis, comma 2, L. n. 633/1941 modificato dalla L. n. 166/2024); - Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta

copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter L n. 633/1941 modificato dalla L. 166/2024); - Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies L. n. 633/1941 modificato dalla L. n. 166/2024); - Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies L. n. 633/1941); - Abusivo utilizzo, duplicazione, riproduzione di opere o materiali protetti (Art. 174-ter L. n. 633/1941 articolo aggiunto dalla L. n. 93/2023);

Art. 25-decies, D.Lgs. n. 231/2001 - articolo aggiunto dalla L. 116/2009 e sostituito dal D.Lgs. n. 121/2011. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.).

Art. 25-undecies D.Lgs. n. 231/2001 - articolo aggiunto dal D.Lgs. n. 121/2011, modificato dalla L. n. 137/2023 e dalla L. n. 82/2025 e L. n. 81/2026. Reati ambientali.

- Inquinamento ambientale (art. 452-bis c.p. modificato dalla L. n. 137/2023 e dalla L. n. 81/2026); - Commercio di prodotti inquinanti (Art. 452 bis 1, comma 2-3 4, c.p. introdotto dal D.Lgs n. 81 del 21/04/2026); - Morte o lesioni come conseguenze del delitto di inquinamento ambientale e di commercio di prodotti inquinanti (art. 452 ter c.p. introdotto dal D.Lgs n. 81/2026); - Disastro ambientale (art. 452-quater c.p. modificato dalla L. n. 137/2023); - Delitti colposi contro l'ambiente (art. 452-quinquies c.p.); - Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p. modificato dalla L. n. 137/2023 e dalla D.L. n. 116/2025); - Impedimento del controllo (art. 452-septies c.p.); - Circostanze aggravanti (art. 452-octies c.p.); - Omessa bonifica (art. 452-terdecies c.p. introdotto dal D.L. n. 116/2025 e convertito dalla L. n. 147/2025); - Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.); - Circostanze aggravanti (art. 452 sexesdecies c.p. introdotto dal D.Lgs. n. 81/2026); - Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.); - Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p. abrogato); - Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (, art. 1, comma 1, e 2, art. 2, art. 3-bis e art. 6 co 4 L. n. 150/1992); - Cessazione e riduzione dell'impiego delle sostanze lesive (articolo 3, comma 6, della L. n. 549/93); - Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee e scarico nelle acque del mare da parte di navi od aeromobili (art. 137 D. Lgs. n. 152/2006); - Abbandono di rifiuti non pericolosi in casi particolari (art. 255-bis D.Lgs n. 152/2006); - Abbandono di rifiuti pericolosi (art. 255-ter D.Lgs. n. 152/2006); - Spedizione Illegale di rifiuti (art. 259- ter D.Lgs. n. 152/2006); - Attività di gestione di rifiuti non autorizzata (art. 256 D.Lgs. n. 152/2006); - Combustione illecita di rifiuti (art. 256-bis D.Lgs. n. 152/2006); - Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (art. 257 D.Lgs. n. 152/2006); - Traffico illecito di rifiuti (art. 259 D.Lgs. n. 52/2006); - Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, comma 4, D. Lgs. n. 152/2006 modificato dal D.L. n. 116/2025 convertito dalla L. n. 147/2025); - Aggravante dell'attività di impresa (art. 259-bis D.Lgs. n. 152/2006); - False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (art. 260- bis D.Lgs. n. 152/2006); - Sanzioni per il superamento valori limite di emissione (art. 279, comma 5, D.Lgs. n. 152/2006); - Inquinamento doloso provocato da navi (art. 8 D.Lgs. n. 202/2007); -

Inquinamento colposo provocato da navi (art. 9 D.Lgs. n. 202/2007); - Cessazione e riduzione dell'impiego delle sostanze lesive (art. 3 L. n. 549/1993); - Produzione e commercio di sostanze ozono lesive (art. 4 introdotto D.Lgs. n.81/2026); - Produzione e commercio di gas ad effetto serra (art. 5 introdotto D.Lgs. n. 81/2026).

Art. 25-duodecies D.Lgs. n. 231/2001 - articolo introdotto dal D.Lgs. n. 109/2012 modificato dalla L. n. 161/2017 e dal D.L. n. 20/2023 e dal D.L. n. 187/2024 e dal D.Lgs. n. 211/2025. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare.

- Permesso di soggiorno per gli stranieri vittime di intermediazione illecita e sfruttamento del lavoro (art. 18-ter D.Lgs. n. 286/1998); - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12 e 12-bis, D.Lgs. n. 286/1998 modificato dal D.Lgs. n. 83/2026); - Disposizioni contro le immigrazioni clandestine (art. 12, comma 1,3,3-bis,3-ter,5 D.Lgs. n. 286/1998 modificato dal D.L. n. 20/2023 e dal D.Lgs. n. 211/2025); - Morte o lesioni come conseguenza di delitti in materia di immigrazione clandestina (art. 12-bis D.Lgs. n. 286/1998).

Art. 25 terdecies D. Lgs n. 231/2001 - articolo introdotto dalla L. n. 167/2017 modificato dal D.Lgs. n. 21/2018. Razzismo e xenofobia.

- Propaganda e istigazione a delinquere per motivi di discriminazione etnica e religiosa (art. 604-bis c.p.); - Circostanze aggravanti (art. 604 ter c.p.);

Art. 25-quaterdecies D.Lgs. n. 231/2001 - introdotto dalla L. n. 39/2019. Reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e gioco d'azzardo esercitati a mezzo di apparecchi vietati.

- Frode in competizioni sportive (art. 1, L. n. 401/1989; modificato dalla L. n. 146/2014); - Esercizio abusivo di attività di giuoco o di scommessa (art. 4, L. n. 401/1989; modificato dalla L. n. 88/2009);

Art. 25 quinquiesdecies D. Lgs n. 231/01 - introdotto dal D.L. n. 124/2019 convertito con L. n. 157/2019 e modificato dal D.lgs. n. 156/2022. Reati Tributari.

- Dichiarazione fraudolenta mediante uso di fatture o di altri documenti per operazioni inesistenti (art. 2, comma 1, e, comma 2-bis, D.Lgs. n. 74/2000 modificato dal D.L. n. 124/2019 e convertito con L. n. 157/2019); - Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000 modificato dal D.L. n. 124/2019 e convertito con L. n. 157/2019); - Dichiarazione infedele (art. 4 introdotto dal D.Lgs. n. 75/2020); - Omessa dichiarazione (art. 5 introdotto dall' art.5 D.Lgs. n. 75/2020); - Emissione di fatture o di altri documenti inesistenti (art. 8, comma 1, e, comma 2-bis, D. Lgs n. 74/2000 modificato dal D.L. n. 124/2019 e convertito con L. n. 157/2019); - Occultamento o distruzione di documenti contabili (art. 10 D. Lgs n. 74/2000 modificato dal D.L. n. 124/2019 e convertito con L. n. 157/2019); - Indebita compensazione (art. 10-quater introdotto dal D.Lgs. n. 75/2020 modificato dal D.Lgs. n. 87/2024); - Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000).

Art. 25-sexiesdecies D.Lgs n. 231/01 introdotto dal D.Lgs n. 75/2020 e modificato dal D.Lgs. n. 141/2024. Contrabbando.

- Sottrazione all'accertamento o al pagamento dell'accisa sui prodotti energetici (art. 40 D.Lgs. n. 504/1995); - Sottrazione all'accertamento o al pagamento dell'accisa sui tabacchi lavorati (art. 40-bis D.Lgs. n. 504/1995 introdotto D.Lgs n. 141/2024); - Circostanza aggravanti del delitto di sottrazione all'accertamento

o al pagamento dell'accisa sui tabacchi (art. 40 ter introdotto D.Lgs n. 141/2024); - Circostanze attenuanti del delitto di sottrazione all'accertamento o al pagamento dell'accisa sui tabacchi (art. 40 quater introdotto D.Lgs n. 141/2024); - Vendita di tabacchi lavorati senza autorizzazione o acquisto da persone non autorizzate alla vendita (art. 40 quinquies introdotto D.Lgs n. 141/2024); - Ultime disposizioni in materia di vendita di tabacchi lavorati (art. 40 sexies introdotto D.Lgs n. 141/2024); - Fabbricazione clandestina di alcole e di bevande alcoliche (art. 41 D.Lgs. n. 504/1995); - Associazione a scopo di fabbricazione clandestina di alcole e di bevande alcoliche (art. 42 D.Lgs. n. 504/1995); - Sottrazione all'accertamento ed al pagamento dell'accisa sull'alcole e sulle bevande alcoliche (art. 43 D.Lgs. n. 504/1995); - Confisca (art. 44 D.Lgs. n. 504/1995); - Circostanze aggravanti (art. 45 D.Lgs. n. 504/1995); - Alterazione di congegni, impronte e contrassegni (art. 46 D.Lgs. n. 504/1995); - Deficienze ed eccedenze nel deposito e nella circolazione dei prodotti soggetti ad accisa (art. 47 D.Lgs. n. 504/1995); - Irregolarità nell'esercizio degli impianti di lavorazione e di deposito di prodotti sottoposti ad accisa (art. 48 D.Lgs. n. 504/1995); - Irregolarità nella circolazione di prodotti soggetti ad accisa (art. 49 D.Lgs. n. 504/1995); - Diritti doganali e diritti di confine (art. 27 D.Lgs. n. 141/2024); - Contrabbando per omessa dichiarazione (art. 78 D.Lgs. n. 26/2024); - Contrabbando per dichiarazione infedele (art. 79 D.Lgs. n. 26/2024); - Contrabbando nel movimento delle merci marittimo, aereo e nei laghi di confine (art. 80 D.Lgs. n. 26/2024); - Contrabbando per indebito uso di merci importate con riduzione totale o parziale dei diritti (art. 81 D.Lgs. n. 26/2024); - Contrabbando nell'esportazione di merci ammesse a restituzione di diritti) (art. 82 D.Lgs. n. 26/2024); - Contrabbando nell'esportazione temporanea e nei regimi di uso particolare e di perfezionamento (art. 83 D.Lgs. n. 26/2024); - Contrabbando di tabacchi lavorati (art. 84 D.Lgs. n. 26/2024); - Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati (art. 85 D.Lgs. n. 26/2024); - Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati (art. 86 D.Lgs. n. 26/2024); - Equiparazione del delitto tentato a quello consumato (art. 87 D.Lgs. n. 26/2024); - Circostanza aggravanti del contrabbando (art. 88 D.Lgs. n. 26/2024).

Art. 25-septiesdecies D.Lgs. n. 231/01 - introdotto dalla L. n. 22/2022. Delitti contro il patrimonio culturale.

- Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.); - Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.); - Appropriazione indebita di beni culturali (art. 518-ter c.p.); - Importazione illecita di beni culturali (art. 518-decies c.p.); - Uscita o esportazione illecite di beni culturali (art. 518-undecies c.p.); - Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies c.p.); - Contraffazione di opere d'arte (art. 518-quaterdecies c.p.); - Furto di beni culturali (art. 518-bis c.p.); - Ricettazione di beni culturali (art. 518-quater c.p. aggiornato dalla L. 54/2026).

Art. 25-duodevicies D.Lgs. n. 231/01 - introdotto dalla Legge n. 22/2022. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici

- Riciclaggio di beni culturali (art. 518- sexies c.p.); - Devastazione e saccheggio di beni culturali e paesaggistici (art. 518-terdecies c.p.).

Art. 25-undevicies D.Lgs. n. 231/2001 - introdotto dalla Legge n. 82/2025 Delitti contro gli animali.

- Uccisione di animali (art. 544-bis c.p.); - Maltrattamento di animali (art. 544-ter c.p.); - Spettacoli o manifestazioni vietate (art. 544-quater c.p.); - Divieto di combattimento tra animali (art. 544-quinquies c.p.); - Uccisione o danneggiamento di animali altrui (art. 638 c.p.); - Circostanze aggravanti (art. 540 septies c.p. introdotto dalla L. n. 82/2025).

Art. 25-vicies D.Lgs. n. 231/2001 - introdotto dal D.Lgs. n. 160/2026 (6 settembre 2026) Reati commessi con l'uso di sistemi di intelligenza artificiale

- Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi (art. 437-bis c.p., nuova introduzione); - Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale, (art. 612-quater c.p., già introdotto dalla L. n. 132/2025).

Delitti tentati (art. 56)

- delitto tentato (art. 56 c.p.)

Art. 12 L. n. 9/2013 - modificato dalla Legge n. 75/2026. Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato. Costituiscono presupposto per la responsabilità degli enti che operano nell'ambito della filiera degli oli vergini di oliva.

- Adulterazione e contraffazione di sostanze alimentari (art. 440 c.p.); - Commercio di sostanze alimentari contraffatte o adulterate (art. 442 c.p.); - Commercio di sostanze alimentari nocive (art. 444 c.p.); - Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali (art. 473 c.p.); - Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.); - Frode nell'esercizio del commercio (art. 515 c.p.); - Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.); - Vendita di prodotti industriali con segni mendaci (art. 517 c.p. modificato dalla L. n. 206/2023); - Contraffazione di indicazioni geografiche denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p. modificato dalla L. n. 75/2026).

Artt. 3 e 10 L. n. 146/2006. Reati transnazionali. Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale.

- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al D.Lgs. n. 25 luglio 1998, n. 286); - Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309); - Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al D.P.R. 23 gennaio 1973, n. 43, art. 86 modificato D.Lgs n. 141/2024); - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.); - Favoreggiamento personale (art. 378 c.p.); - Associazione per delinquere (art. 416 c.p.); - Associazione di tipo mafioso (art. 416-bis c.p.); - Circostanze aggravanti ed attenuanti connessi ad attività mafiose (art. 416 bis 1 c.p. introdotto D.Lgs. n. 21/2018 e modificato dalla L. n. 60/2023).

Adeguamento della normativa nazionale al regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 (introdotto dal D.lgs. 129/2024):

- Responsabilità dell'ente (art. 34 D.Lgs. n. 129/2024); - Divieto di abuso di informazioni privilegiate (art. 89 regolamento (UE) 2023/1114); - Divieto di divulgazione illecita di informazioni privilegiate (art. 90 regolamento (UE) 2023/1114); - Divieto di manipolazione del mercato (art. 91 regolamento (UE) 2023/1114).

4 Le sanzioni

L'accertamento della responsabilità amministrativa espone l'Ente a diverse tipologie di sanzioni, le quali in forza del principio di legalità (art. 2 Decreto 231), sono individuate dal Legislatore. In particolare le sanzioni sono di seguito individuate. **sanzioni pecuniarie (artt. da 10 a 12 D.LGS. n. 231/2001): Per l'illecito amministrativo dipendente da reato si applica sempre la sanzione pecuniaria per quote in un numero non inferiore a cento né superiore a mille. Per ciascun illecito, infatti, la legge in astratto determina un numero minimo e massimo di quote commisurate al numero e valore delle quote, della gravità del fatto, del grado di responsabilità della società, delle misure adottate per contrastare o attenuare le conseguenze del fatto e/o prevenire la commissione di ulteriori illeciti. Il valore della singola quota varia da un minimo di € 258 ad un massimo di € 1.549. Tale valore è stabilito tenendo conto delle condizioni economiche e patrimoniali dell'ente, per garantire che la sanzione sia effettivamente punitiva ma non tale da causare la chiusura dell'impresa. Solo per i reati di cui all'art. 25-octies.2 co 2 D.Lgs. n. 231/2001, il valore è stabilito calcolando una specifica percentuale del fatturato globale dell'Ente e, solo nei casi in cui tale quantificazione non sia possibile, secondo un importo fisso. In tutti i casi ove sia provato che prima della conclusione del processo l'Ente abbia agito per riparare integralmente il danno, eliminare le conseguenze dannose del reato o ha adottato ed efficacemente attuato un Modello 231 idoneo a prevenire i reati simili a quelli contestati, le quote possono essere ridotte della metà. sanzioni interdittive (artt. da 13 a 17 D.LGS. n. 231/2001) anche le stesse sono sorrette dal principio di tassatività, inoltre occorre che il reato dell'apicale abbia procurato all'Ente un profitto di rilevante entità e quello del sottoposto sia stato determinato e/o agevolato da gravi carenze organizzative, oppure che vi sia stata reiterazione degli illeciti. Il Decreto indica il seguente catalogo di sanzioni interdittive: (i)** interdizione dall'esercizio dell'attività; (ii) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione del reato; (iii) divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di pubblico servizio; (iv) esclusione da agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli concessi; (v) divieto di pubblicizzare beni o servizi. La scelta della sanzione interdittiva è sorretta da un principio di "frazionamento"posto che deve essere riferita allo specifico settore di attività dell'Ente in cui è stato realizzato l'illecito e, comunque, deve rispondere ai principi di adeguatezza, proporzionalità e sussidiarietà. Il primo principio enunciato si deduce: a) dall'articolo 14, comma 1 del Decreto 231: *"le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente"*; b) dall'articolo 15, comma 2, del Decreto che introduce una simile previsione con riferimento alla sanzione, sostitutiva dell'interdizione, rappresentata dal commissariamento dell'ente; c) dall'art. 69, comma 2, secondo cui la sentenza applicativa delle sanzioni interdittive *"deve sempre indicare l'attività o le strutture oggetto della sanzione"*, escludendo che possa indifferentemente coinvolgere ogni settore in cui l'Ente opera. Tali principi trovano applicazione anche a in fase cautelare, ove i fatti contestati all'Ente ai fini della responsabilità da reato, sono ancora in fase di accertamento. La misura-base di applicazione delle sanzioni interdittive è fissata tra un minimo di 3 mesi e un massimo di 2 anni dall'art. 13, comma 2, del Decreto 231. Vi sono tuttavia talune eccezioni *in pejus*. Infatti, la legge n. 3/2019 recante "*Misure per il contrasto dei reati contro la pubblica amministrazione e in materia di trasparenza dei partiti e movimenti politici*" (cd. legge Spazzacorrotti) ha introdotto una disciplina specifica per l'applicazione delle sanzioni interdittive ad alcuni reati contro la PA, ovvero concussione, corruzione propria semplice e aggravata dal rilevante profitto conseguito dall'Ente, corruzione in atti giudiziari, induzione indebita a dare o promettere utilità, dazione o promessa al pubblico ufficiale o all'incaricato di pubblico servizio di denaro o altra utilità da parte del corruttore, istigazione alla corruzione. In particolare, la legge ha disposto un inasprimento del trattamento sanzionatorio, distinguendo due diverse forbici edittali a seconda della qualifica del reo: le sanzioni interdittive potranno avere una durata compresa tra 4 e 7 anni se il reato è commesso da un soggetto apicale e tra 2 e 4 anni se il colpevole è un soggetto subordinato.La legge ha invece disposto l'applicazione delle sanzioni interdittive nella misura-base di cui all'art. 13, comma 2, del Decreto n. 231 (3 mesi – 2 anni) qualora l'Ente, per gli stessi delitti citati e prima della sentenza di primo grado, si sia adoperato per evitare ulteriori conseguenze del reato e abbia collaborato con l'autorità giudiziaria per assicurare le prove dell'illecito, per individuarne i responsabili e abbia attuato modelli organizzativi idonei a prevenire nuovi illeciti e ad evitare le carenze organizzative che li hanno determinati. In ogni caso, ai sensi dell'articolo 17 del Decreto n. 231, le sanzioni interdittive non si applicano se prima della dichiarazione di apertura del dibattimento di primo grado, l'Ente

ha riparato le conseguenze del reato. In particolare, a tal fine, devono concorrere le seguenti circostanze: l'ente abbia risarcito integralmente il danno ed eliminato le conseguenze dannose o pericolose del reato ovvero si sia adoperato in tal senso; abbia eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e attuazione di un modello organizzativo idoneo a prevenire i reati della stessa specie di quelli verificatosi, abbia messo a disposizione il profitto del reato ai fini della confisca. **Confisca del prezzo o del profitto del reato (art. 19 D.LGS. n. 231/2001) Nei confronti dell'Ente è sempre disposta, con la sentenza di condanna, la confisca del prezzo o del profitto del reato, salvo la parte che può essere restituita al danneggiato. Sono, in ogni caso, fatti salvi i diritti acquisiti dai terzi in buona fede.** Quando non è possibile eseguire la confisca sui beni costituenti direttamente prezzo o profitto del reato, la stessa può avere a oggetto somme di denaro, beni, o altre utilità di valore equivalente al prezzo o al profitto del reato. In via cautelare, può essere disposto il sequestro delle cose che, costituendo prezzo o profitto del reato o loro equivalente monetario, sono suscettibili di confisca. In tema di sequestro preventivo, il comma 1-bis nell'articolo 53 del Decreto n. 231 (aggiunto in sede di conversione del Decreto Legge n. 101 del 2013), stabilisce che, in caso di sequestro finalizzato alla confisca per equivalente ex articolo 19, comma 2, del Decreto n. 231, il custode giudiziario consente agli organi societari di impiegare società, aziende, titoli, quote azionarie o somme liquide oggetto di sequestro per garantire la continuità e lo sviluppo aziendale. La gestione di tali beni, dunque, di regola rimane in capo agli organi sociali, mentre solo in caso di violazione della destinazione ai fini di sviluppo e continuità aziendale è prevista la devoluzione di poteri gestori in capo a un amministratore giudiziario. Quest'ultimo esercita un potere di sola vigilanza degli organi societari, fungendo da raccordo tra l'autorità giudiziaria e l'impresa. In questo modo si intende bilanciare le esigenze penal-preventive sottese al Decreto 231 con le garanzie di tutela dell'integrità patrimoniale degli operatori economici e della libertà di iniziativa economica costituzionalmente sancita. **Pubblicazione della sentenza (art. 18 D.LGS. n. 231/2001) si tratta di una misura capace di recare un grave impatto sull'immagine dell'Ente. La pubblicazione della sentenza di condanna in uno o più giornali, per estratto o per intero, può essere disposta dal giudice, unitamente all'affissione nel comune dove l'Ente ha la sede principale, quando è applicata una sanzione interdittiva. La pubblicazione è eseguita a cura della cancelleria del giudice competente e a spese dell'Ente.** L'accertamento della responsabilità della società, nonché la determinazione della sanzione, spetta al giudice penale all'esito del procedimento relativo ai reati da cui scaturisce la responsabilità amministrativa. L'Ente partecipa al procedimento penale con il proprio rappresentante legale, salvo che questi sia indagato o imputato del reato da cui dipende l'illecito amministrativo. In quest'ultimo caso, il rappresentante legale non potrà provvedere alla nomina del difensore di fiducia dell'Ente, in quanto vige un divieto generale ed assoluto disposto dall'art. 39 D.lgs. 231/2001. In tali casi, la nomina del difensore dell'Ente va rilasciata da un soggetto specificamente delegato (*procuratore ad litem*), utilizzando i normali strumenti previsti all'interno della compagine organizzativa, quali lo statuto o il proprio atto costitutivo. Nello specifico, l'organo deputato al conferimento della procura *ad litem* è l'Assemblea dei Soci, fatta esclusione per i soci che rivestano la qualità di indagato/imputato nel medesimo procedimento. Laddove il legale rappresentante, stante tale situazione di incompatibilità, abbia provveduto alla nomina del difensore di fiducia dell'Ente, tale nomina è da ritenersi priva di qualsiasi efficacia ed eventuali istanze saranno ritenute inammissibili.

5 Esenzione della responsabilità dell'ente

Il Decreto n. 231, agli articoli 6 e 7, introduce specifiche forme di esonero dalla responsabilità dell'Ente, differenziate in base alla categoria di appartenenza dell'autore del reato. Ai sensi dell'articolo 6 del Decreto, qualora il reato sia stato commesso da **soggetti apicali**, l'Ente non risponde qualora dimostri che concorrano congiuntamente le seguenti condizioni: *a) l'organo dirigente dell'Ente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire i reati della specie di quello verificatosi; b) il compito di vigilare sul funzionamento e sull'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e controllo*

(ODV); c) le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti modelli ove adottati; d) non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b). Ai sensi dell'articolo 7 del Decreto, qualora il reato sia stato commesso da **soggetti sottoposti alla direzione o alla vigilanza dei soggetti apicali**, l'Ente è responsabile qualora la pubblica accusa dimostri che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o di vigilanza. In ogni caso, se l'Ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire reati della specie di quello verificatosi e l'organismo di vigilanza ha diligentemente svolto le sue funzioni, si presume esclusa l'inosservanza degli obblighi di direzione o vigilanza e, quindi, la responsabilità dell'Ente. Affinché il modello 231 adottato abbia funzione di esimente, l'art. 6, comma 2, del Decreto 231 indica le caratteristiche essenziali per la costruzione di un modello di organizzazione, gestione e controllo. Il Modello deve dunque soddisfare le seguenti esigenze (requisiti di efficacia del Modello): *a) individuare le attività nel cui ambito possono essere commessi i r eati (cosiddetta "mappatura" delle attività a rischio); b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire; c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati; d) prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli. L'effettività del Modello è invece legata alla sua efficace attuazione che, a norma dell'art. 7, comma 4, del Decreto, richiede: a) una verifica periodica e l'eventuale modifica dello stesso quando siano scoperte significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività (aggiornamento del Modello); b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.* In sintesi, il D. Lgs n. 231/2001 non disciplina analiticamente la natura e le caratteristiche del modello di organizzazione, ma detta alcuni principi di ordine generale parametrati in funzione dei differenti soggetti che potrebbero commettere un reato. La finalità del modello è di attuare un sistema di prevenzione tale da non poter essere aggirato se non intenzionalmente, in totale sintonia con il concetto di elusione fraudolenta previsto dall'art. 6 del decreto. Il modello non è da intendersi quale strumento statico, ma deve essere considerato, al contrario, un apparato dinamico che permette alla società di eliminare, attraverso una corretta e mirata implementazione dello stesso nel corso del tempo, eventuali mancanze che, al momento della sua creazione, non era possibile individuare.

6 Il modello di gestione, organizzazione e controllo adottato da AEGI SRL

6.1 Descizione della Società

Nome: AEGI SRL

Sede legale: Lovero (SO), via Roma 49/E (23030)

Partita IVA: 00619240146 **Codice fiscale e n. iscr. Al Registro Imprese**: 00619240146

Codice LEI: 81560051C005DA77E234

Data atto di costituzione: 06/10/1990 Principale oggetto sociale: La Società ha quale scopo principale l'assemblaggio di computer e produzione di software, commercio di articoli di telefonia sia fissa che mobile, nonché l'installazione di impianti telefonici in genere e reti cablate, nonché impianti elettrici civili ed industriali, l'attività di copisteria, commercio all'ingrosso e al minuto di computer e articoli di elettronica, macchine, mobili, arredamenti tecnici per gli uffici ed

affini, articoli di ottica, di cine-foto-ottica, di geodesia, di foto-ottica o cinefoto, di apparecchi radio televisioni con relativi accessori, macchine attrezzature e articoli tecnici per l'agricoltura l'industria commercio e l'artigianato. In via secondaria la società si occupa di assumere o cedere partecipazioni in società o enti con scopo analogo o affine al proprio, operazioni bancarie, commerciali e finanziarie utili al conseguimento dell'oggetto sociale.

6.2 Rapporti con i soci

I soci della società AEGI SRL, indicati per quota sono:

- Ghilotti Achille 30% - valore nominare 3.150,00;
- Pini Andrea 28% - valore nominare 2.940,00;
- Sala Christian 28% - valore nominare 2.940,00;
- Ghilotti Gabriella 14%- valore nominale 1.470,00.

I rapporti societari sono stati valutati anche quale area di rischio con riferimento ai possibili illeciti rilevanti ai sensi del Decreto 231 che attraverso di essi si potrebbero realizzare. Si è quindi prestata particolare attenzione alle ragioni che hanno ispirato detti contratti, ai corrispettivi pattuiti e ai sistemi di controllo posti a valle dell'esecuzione dei contratti stessi.

6.3 Struttura organizzativa

La struttura organizzativa è rappresentata nell'organigramma cui si rimanda.

6.4 Sistemi di gestione

Nell'ambito del miglioramento dei propri processi, la Società provvederà ad adottare, secondo un approccio integrato, le seguenti certificazioni:

- ISO 9001 – **Sistema di Gestione per la Qualità;**
- ISO 27001 – **Sistemi di gestione per la sicurezza delle informazioni;**
- ISO 14001 – **Certificazione del Sistema di Gestione Ambientale;**
- ISO 45001 – **Sistema di Gestione per la Salute e la Sicurezza sul Lavoro;**
- SA 8000 – **Certificazione della Responsabilità Sociale dell'Impresa.**

I predetti strumenti sono funzionali al perseguimento degli scopi per i quali sono rilasciati nonché ai fini della prevenzione dei reati ex D.Lgs. n. 231/01. Pertanto, all'atto dell'adozione l'OdV informerà il Coniglio di Amministrazione della necessita di procedere l'adeguamento del modello ai predetti strumenti.

6.5 Obiettivi e finalità del Modello

Il Presente Modello ha l'obiettivo di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività aziendali, attraverso un sistema di controlli interno idoneo a prevenire la commissione di comportamenti illeciti da parte dei propri amministratori, dipendenti, collaboratori e partner d'affari. In particolare si propone di perseguire le seguenti finalità: - diffondere la necessaria consapevolezza in tutti coloro che operano in nome e per conto della società di poter incorrere, in caso di violazione delle disposizioni contenute nel modello, in un illecito sanzionabile, sul piano penale ed amministrativo, non solo nei propri confronti, ma anche nei confronti della società; - sottolineare che, tali forme di comportamento illecito, sono sistematicamente condannate dalla società, in quanto sono contrarie ai principi etico - sociali cui si attiene, oltre che alle disposizioni di legge; - informare tutti gli interessati che la violazione delle prescrizioni contenute nel modello organizzativo di gestione e controllo comporterà l'applicazione di sanzioni, tra cui in *extremis* anche la risoluzione del rapporto contrattuale; - consentire alla società, grazie ad una costante azione di monitoraggio sui "processi e attività a rischio di reato", di intervenire tempestivamente per prevenire e contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello; - migliorare l'efficacia e la trasparenza nella gestione delle attività aziendali.

6.6 Destinatari

I destinatari del Modello sono: - i soggetti che nell'ambito della Società rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione ed il controllo della stessa (i cc.dd. soggetti apicali); - le persone sottoposte alla direzione o alla vigilanza di uno dei soggetti in posizione apicale, ossia i dipendenti della Società, ivi compresi i dirigenti nonché i soggetti utilizzati dalla Società nell'ambito di somministrazione di lavoro e di appalto di servizi; - i collaboratori e, in generale, i consulenti esterni, i *partners* commerciali (imprese individuali e/o società) e tutti coloro che abbiano rapporti contrattuali con la Società per lo svolgimento di qualsivoglia prestazione lavorativa, ivi compresi gli agenti e gli appaltatori di servizi.

7 Metodologia adottata per la costruzione e aggiornamento del Modello 231

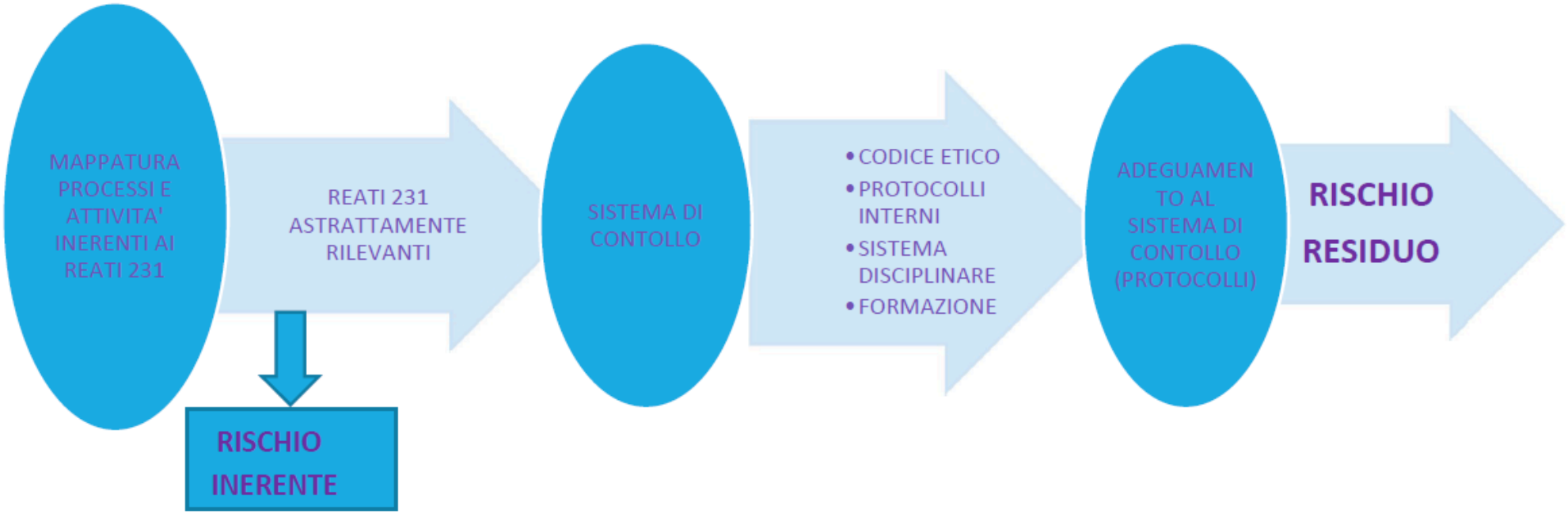
Ai sensi dell'art. 6, comma 3, del Decreto, i modelli di organizzazione, gestione e controllo possono essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia. AEGI SRL decide di aderire alle linee guida di Confindustria emanate del giugno 2021 " *Linee Guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/01* ", con le quali sono stati indicati i lineamenti della responsabilità da reato, il sistema disciplinare e i meccanismi sanzionatori, la composizione e i poteri dell'organismo di vigilanza, nonché il fenomeno dei gruppi di imprese. In particolare, i punti fondamentali che le linee guida di Confindustria indicano per la costruzione del Modello possono essere così riepilogati: *(i) individuazione delle aree di rischio, volta a verificare in quale area/settore dell'attività aziendale sia possibile la realizzazione dei reati previsti dal Decreto; (ii) predisposizione di un sistema di controllo in grado di prevenire i rischi di commissione di Reato attraverso l'adozione di appositi protocolli*. Le componenti più rilevanti del Sistema di controllo ideato da Confindustria sono: **Codice Etico;** sistema organizzativo; **procedure manuali ed informatiche; poteri autorizzativi e di firma;** sistemi di controllo e gestione; **comunicazione al personale e sua formazione.** Le componenti del sistema di controllo devono essere ispirate ai seguenti principi: - verificabilità, documentabilità, coerenza e congruenza di ogni operazione (per ogni operazione vi deve essere un adeguato supporto documentale su cui si possa procedere in ogni momento all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa); - applicazione del *principio di separazione delle funzioni* (a tal fine occorre che: a nessuno vengano attribuiti poteri illimitati; i poteri e le responsabilità siano chiaramente definiti e conosciuti all'interno

dell'organizzazione; i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative assegnate); - documentazione dei controlli (l'effettuazione dei controlli deve essere documentata); - previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice Etico e delle procedure previste dal Modello; - individuazione di un Organismo di Vigilanza, dotato dei requisiti di autonomia e indipendenza, professionalità e continuità di azione, al quale le varie funzioni aziendali debbono inviare una serie di informazioni. Per la predisposizione del proprio Modello di organizzazione e gestione, la Società ha quindi tenuto conto delle suddette linee guida predisposte da Confindustria. **Individuazione delle attività a rischio** Ai sensi dell'art. 6, comma 2 lett. a) del Decreto, il Modello deve " *individuare le attività nel cui ambito possono essere commessi reati* ". Pertanto, nella costruzione del presente Modello, si è prima di tutto provveduto all'identificazione dei processi societari sensibili alla commissione dei Reati di cui al Decreto, procedendo ad un'accurata verifica delle attività poste in essere dalla Società nonché delle sue strutture organizzative, onde individuare, per ogni singolo settore, i relativi rischi di Reato in concreto prospettabili. Il lavoro di realizzazione del Modello si è sviluppato nel rispetto dei principi fondamentali della documentazione e della verificabilità delle attività. Si è innanzitutto proceduto a raccogliere ed esaminare la documentazione ufficiale utile alla realizzazione dell'analisi e disponibile presso la Società, quali: - Statuto e Regolamento; - Organigramma; - Deleghe e procure; - Procedure operative formalizzate; - Elementi relativi alle sanzioni disciplinari previste dai C.C.N.L. applicabili; - Elenco fornitori; - Elenco clienti; - Bilanci approvati dall'anno 2022 al 2024. Si è poi proceduto ad effettuare una mappatura di tutta l'attività della Società, articolata sulla base dei processi aziendali, singolarmente esaminati quanto ai precisi contenuti, alle concrete modalità operative, alla ripartizione delle competenze, alla sussistenza o insussistenza di rischio di commissione di Reato. In ragione dell'attività della Società, si è ritenuto di concentrare maggiore attenzione sulla valutazione della sussistenza dei profili di rischio in relazione a talune tipologie di Reato, quali, in particolare: Reati informatici, Reati ambientali, i Reati societari, i Reati contro la Pubblica Amministrazione, i Reati tributari Delitti di criminalità organizzata, Reati in materia di sicurezza del lavoro, Indebita percezione di erogazioni truffa in danno dello Stato di un Ente Pubblico o Dell'Unione Europea per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un Ente Pubblico e Frode nelle pubbliche forniture; Delitti informatici e trattamento illecito dei dati; i Reati contro il patrimonio dello Stato o di Enti pubblici, i Reati di abuso di mercato, i Reati di riciclaggio ed autoriciclaggio, i Reati contro l'industria ed il commercio, il Reato d'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, il Reato d'impiego di cittadini di paesi terzi il cui soggiorno è irregolare,. Per quanto invece attiene agli illeciti contro la libertà individuale; ai Reati di razzismo e xenofobia; alla frode in competizione sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati**;** ai Reati relativi al finanziamento di organizzazioni terroristiche, ai Reati transnazionali si è ritenuto che la specifica attività svolta dalla Società non presenti profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio della stessa. Si è pertanto ritenuto esaustivo il richiamo ai principi contenuti sia nel presente Modello che nel Codice Etico della Società, ove si vincolano gli esponenti aziendali, i collaboratori ed i *partners* commerciali al rispetto dei valori di solidarietà, di tutela della personalità individuale, di correttezza, di trasparenza, di moralità, di rispetto delle leggi e dei provvedimenti delle autorità pubbliche (ed, *in primis*, dell'autorità giudiziaria). L'identificazione delle aree a rischio di commissione di Reati è stata effettuata mediante interviste condotte singolarmente con i Responsabili di ciascuna Funzione che descrivono le modalità operative di ciascuna Ufficio, il tutto documentato mediante specifiche questionari. Le categorie di attività identificate nel cui ambito è stata riscontrata la sussistenza del rischio di commissione delle fattispecie di Reato sono le seguenti: - Gestione dei sistemi informativi; - Gestione del processo di realizzazione, acquisto e diffusione di contenuti web ed utilizzo software tutelati da diritto d'autore. - Gestione delle ispezioni amministrative, fiscali e previdenziali da parte degli Enti Pubblici competenti e dei rapporti con le autorità pubbliche di controllo o autorità di vigilanza; - Gestione dei rapporti con le Pubbliche Amministrazioni; - Selezione, assunzione e gestione amministrativa del personale; - Assegnazione e gestione di incarichi di consulenza e collaborazione; - Attività di ciclo attivo (definizione del pricing, gestione della raccolta e stoccaggio dei rifiuti, fatturazione attiva, gestione del credito); - Ciclo passivo (gestione degli acquisti e dei rapporti con i fornitori di beni e servizi e dei rapporti con l'Autorità); - Gestione degli omaggi, liberalità, sponsorizzazioni; - Gestione della tesoreria; - Gestione dei contenziosi giudiziali e stragiudiziali (es. civili, tributari, giuslavoristici, amministrativi,

penali), in tutti i gradi di giudizio e nomina dei professionisti esterni; - Gestione della contabilità, della formazione del bilancio, delle comunicazioni sociali in genere; - Gestione dei rapporti con i soggetti ai quali la legge attribuisce poteri di controllo (Soci, ecc.); - Gestione delle operazioni societarie che possano incidere sull'integrità del capitale sociale; - Gestione della salute e della sicurezza sui luoghi di lavoro; - Gestione dei rischi in materia ambientale; - Gestione dei rapporti con l'amministrazione finanziaria e degli adempimenti fiscali; **Identificazione e analisi degli attuali presidi di rischio** Per le suddette aree a rischio si è poi richiesto ai soggetti responsabili della gestione delle relative attività di descrivere le procedure operative e i concreti controlli esistenti, riconoscibili come idonei a presidiare il rischio individuato. Il risultato di siffatta attività è stato documentato in specifiche schede. **Gap analisys** La situazione di rischio e dei relativi presidi riportata dalle schede è stata confrontata con le esigenze e i requisiti imposti dal Decreto al fine di individuare le carenze del sistema organizzativo aziendale esistente. Nei casi in cui siano state identificate attività a rischio ritenute non sufficientemente presidiate dal sistema di controlli in essere, si è proceduto ad individuare, con il supporto dei soggetti responsabili di tali attività, gli interventi ritenuti più efficaci ed idonei a prevenire in concreto le ipotesi di rischio identificate. **Definizione dei protocolli** Per le aree a rischio di reato, per le quali non fosse già presente un sufficiente presidio di controllo, si sono definiti protocolli che contengono la disciplina più idonea a governare il profilo di rischio individuato. Ne fanno parte il codice entico, i protocolli operartivi e i flussi informativi OdV.

sintesi riepilogativa RISK ASSESTEMENT

Sintesi riepilogativa Risk Assestement.png



8 Struttura del modello

Il presente Modello si compone di - una **Parte Generale**, ove sono definiti i contenuti e le finalità del Decreto; le funzioni ed i principi del Modello, le caratteristiche ed il funzionamento dell'Organismo di Vigilanza, i flussi informativi, l'attività di formazione e informazione, il sistema disciplinare; - una **Parte Speciale**, ove sono esaminate le attività aziendali che presentano profili di rischiosità in relazione alle tipologie di reato previste dal D.Lgs. n. 231/2001. In particolare, per ogni singola fattispecie di reato, limitatamente ai casi che potrebbero configurarsi in capo alla Società, tale Parte Speciale contiene l'indicazione del reato (denominazione e testo dell'articolo), una breve descrizione delle modalità di realizzazione dell'illecito, le sanzioni in capo all'Ente quali previste dal Decreto, l'individuazione delle aree a rischio reato e definizione dei comportamenti che devono essere tenuti dai soggetti apicali e dai soggetti sottoposti che operano nelle relative aree, al fine di prevenire la commissione dei reati individuati nell'ambito della normativa di riferimento. Il Modello si completa con i seguenti **Allegati** che ne costituiscono parte integrante: - il Codice Etico: descrive i comportamenti cui i destinatari del modello devono aderire; - organigramma societario; - Risk Assessment (Premessa); - Risk Assesment; - Sistema disciplinare: sono indicate le sanzioni disciplinari per i soggetti destinatari. Inoltre costituiscono parte integrante del Modello, anche se non allegati, i seguenti documenti interni: sistema di deleghe e procure vigenti. L'approvazione del MOG e tutte le successive modifiche e integrazioni, sono di competenza dell'Amministratore Unico. Gli interventi di adeguamento o aggiornamento della Sezione 231 e della Sezione Anticorruzione e Trasparenza sono previsti in occasione di: - novità normative; - modifiche del business, della Governance e della struttura organizzativa di AEGI SRL che determinano un impatto sull'attuazione del sistema di controllo definito nel presente documento; - variazioni nei processi e nelle attività aziendali o aree di business; - verificarsi di eventi straordinari (gravi violazioni, contestazioni, sanzioni ecc.); - violazioni e/o esiti negativi di verifiche sull'efficacia del suddetto sistema di controllo interno; - eventuali spunti di miglioramento emersi nel corso di segnalazioni e/o contestazioni da parte di soggetti esterni. L'OdV valuta, con continuità, l'adeguatezza del MOG, ne promuove gli eventuali aggiornamenti e li sottopone all'approvazione dell'Amministratore Unico. Le procedure, l'organigramma, i mansionari, il Documento di Valutazione dei rischi aziendali ed in generale tutti documenti richiamati nel modello ed allegati, essendo documenti operativi e soggetti a revisione costante, non comporteranno necessariamente l'aggiornamento dell'intero modello ma necessiteranno di essere approvati dalle funzioni aziendali preposte e messi a conoscenza dell'OdV incaricato. I " **Destinatari** " del MOGC e si impegnano al rispetto del contenuto dello stesso: - Presidente del Coniglio di Amministrazione; - i Soci; - i Dirigenti; - i Soggetti Apicali; - i Dipendenti della Società (con riferimento a qualsiasi forma contrattuale: assunzione a tempo determinato, indeterminato, stage, ecc.), nonché i Lavoratori Somministrati e in regime di distacco (cosiddetti Soggetti Interni sottoposti ad altrui direzione). Inoltre, in forza di apposite clausole contrattuali e limitatamente allo svolgimento delle attività sensibili a cui essi eventualmente partecipano, devono essere considerati Destinatari i seguenti Soggetti Esterni: - i Collaboratori, i Consulenti, i Fornitori e, più in generale, i soggetti che svolgono attività di lavoro autonomo nella misura in cui operano per conto o nell'interesse della Società, nell'ambito delle cosiddette Aree a rischio. Tutti i suddetti Destinatari sono tenuti a conoscere ed a rispettare le disposizioni contenute nel MOG e devono collaborare nelle verifiche dirette al periodico esame della sua efficienza per correggerne eventuali disfunzioni.

9 Organismo Di Vigilanza (OdV)

9.1 Requisiti dell'organismo di vigilanza

In conformità alle disposizioni dagli articoli 6, comma 1, lett. *b)* e 7, commi 3 e 4 del D. Lgs. n. 231/2001, l'Organismo di Vigilanza e Controllo con struttura monocratica o collegiale, incaricato di vigilare sul corretto funzionamento e osservanza del Modello e promuovere l'aggiornamento. La nomina è deliberata dal Consiglio di Amministrazione e deve essere accettata dall'incaricato e/o ciascun membro designato. Dell'avvenuto conferimento dell'incarico – ovvero di qualunque successivo cambiamento nella composizione dei relativi membri – sarà formalmente data comunicazione ai livelli aziendali interessati, anche mediante la illustrazione dei poteri, compiti, dell'Organismo di Vigilanza. L'OdV deve possedere requisiti di: - **autonomia**: all'OdV deve essere assicurata completa autonomia decisione, piena autodeterminazione e libertà di azione. Tale autonomia va garantita rispetto ai vertici societari, rimanendo estraneo a qualsiasi forma di interferenza e pressione da parte degli stessi. L'autonomia impone la capacità di autodeterminarsi fissando le proprie regole comportamentali e procedurali attraverso l'adozione un regolamento. Tale requisito si realizza anche attraverso l'istruzione di un budget adeguato che l'OdV potrà gestione in autonomia senza che occorra alcuna autorizzazione. Inoltre non deve essere demandato all'OdV alcun compito di gestione all'interno dell'ente e non deve essere reso partecipe di alcuna decisione operativa. -**Indipendenza**: l'organismo di vigilanza è un organismo terzo, gerarchicamente collocato al vertice della linea di comando, libero da legami di subordinazione rispetto al vertice aziendale, quindi capace di adottare provvedimenti ed iniziative insindacabili. - **Professionalità**: è inerente ai requisiti soggettivi dell'organismo. verificati previa analisi del *curriculum vitae* e delle concrete esperienze lavorative di ognuno. In particolare, sono richieste specifiche conoscenze in materia legale, di metodologie ed attività di controllo, valutazione e gestione dei rischi, organizzazione aziendale, finanza, revisione e gestione, ecc., oltre che capacità specifiche in relazione all'attività ispettiva. - **Continuità di azione**: necessità dell'istaurazione di un organismo in grado di svolgere un'attività di vigilanza con assiduità e regolarità; ciò presuppone necessariamente un'interazione con tutto il management della società. All'OdV sono, quindi, assegnati poteri di controllo ed accesso a tutti le informazioni rielevanti o che si ritengono siano fondamentali al compimento della propria funzione. In tale contesto è consentito all'OdV di condurre interviste, sopralluoghi, verifiche e audit con cadenza periodica. - **Onorabilità**: considerato il ruolo da ricoprire, l'Odv deve un soggetto dall'indubbia moralità, ne deriva che è causa di ineleggibilità e di incompatibilità alla carica presenza di una delle circostanze di cui all'articolo 2382 del codice civile, l'avvio di indagini nei confronti la condanna con sentenza anche in primo grado per aver commesso uno dei reati di cui al decreto, la condanna ad una pena l'interdizione, anche temporanea, dai pubblici uffici, l'interdizione temporanea dagli uffici direttivi delle persone giuridiche.

9.2 Nomina e durata dell'organismo di vigilanza

L'organo amministrativo con proprio atto deliberativo nomina l'OdV e determina il compenso e la durata dell'incarico. Nello stesso atto sono definiti poteri e le cause di decadenza, di revoca e di ineleggibilità dalla carica di membri dell'OdV. La nomina dell'OdV, i suoi compiti ed i suoi poteri, sono tempestivamente comunicati alla struttura organizzativa. La nomina quale componente dell'organismo di vigilanza è condizionata alla presenza dei requisiti soggettivi di cui si è detto. L'OdV con l'accettazione della nomina riconosce tacitamente l'insussistenza di suddetti motivi ostativi. Le predette regole si applicano anche in caso di nomina di un componente dell'OdV in sostituzione di altro membro dell'organismo stesso. In ogni caso, la revoca dalla carica di componente dell'OdV (anche limitatamente ad un solo componente di esso) e la sostituzione potrà avvenire soltanto per giusta causa, mediante una delibera dell'organo amministrativo e con l'approvazione del collegio sindacale. Per "giusta causa" si intende, a titolo esemplificativo la perdita dei requisiti soggettivi; il sopraggiungere di un motivo di incompatibilità; una grave negligenza nell'assolvimento dei compiti connessi con l'incarico conferito all'OdV; "omessa o insufficiente vigilanza" da parte dell'organismo di vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del decreto. In ogni caso, l'OdV è libero di rinunciare in qualsiasi momento all'incarico mediante comunicazione in forma scritta con un congruo preavviso, che si stabilisce in 3 mesi e sarà preannunciato nel regolamento adottato. In caso di rinuncia l'Ente provvederà tempestivamente a nominare un sostituto al fine di garantire la continuità dell'azione. L'Organismo di Vigilanza si dota di un

regolamento di funzionamento che disciplina anche la durata in carica e tutti gli aspetti relativi al funzionamento dell'organismo. **AEGI SRL ha nominato un Organismo di Vigilanza Monocratico con carica triennale, non tacitamente rinnovabile.**

9.3 Poteri e funzioni dell'organismo di vigilanza

Ai sensi dell'art. 6 co 2 lettera b) del Decreto, l'OdV ha il compito **di vigilare** sia sul **funzionamento** che sulla **corretta osservanza** del modello adottato dalla società, inoltre dovrà svolgere un attività di **verifica sull'adeguatezza** del modello in relazione alla dimensione dell'Ente e sull'attività in concreto svolta dalla stessa anche al fine di prevenire la commissione di condotte illecite, infine, sarà cura dell'OdV **vigilare sull'effettività** intesa quale rispondenza tra i comportamenti concreti e quelli formalmente previsti dal modello stesso. Nonché potrà proporre **modifiche o aggiornamenti** ove se ne ravvisi la necessità (in considerazione di eventuali interventi normativi, variazioni della struttura organizzativa, violazioni del modello). Per ciò che attiene alla funzione di vigilanza essa si attua principalmente attraverso: - analisi dei flussi (periodici o ad evento); - acquisizioni documentali; - scambi informativi con l'organo amministrativo e altri organi di controllo. I verbali delle riunioni dell'OdV le informazioni, le notizie e la documentazione raccolta nell'esercizio delle attività di verifica, sono conservati in uno specifico archivio, il cui accesso è consentito esclusivamente ai membri dell'OdV. Lo stesso trattamento di riservatezza si applica ai dati dell'OdV presenti su supporto informatico. L'accesso a tale documentazione verrà comunque garantito su specifica richiesta delle Autorità Giudiziarie. Per ciò che attiene all'attività di aggiornamento del modello sarà compito dell'OdV segnarle all'organo amministrativo la necessità di apportare modifiche e/o aggiornamenti: - ove sia stata riscontrata la commissione di condotte illecite; - in caso di mutamenti dell'attività svolta dalla società che integrare ulteriori rischi non mappati; - in caso di aggiornamenti normativi che possano includere nel catalogico dei reati presupposti fattispecie di reato collegabili all'attività svolta dall'Ente. Inoltre si evidenzia la **funzione di gestione dei flussi informativi da e verso l'OdV,.** I flussi possono **essere periodici o ad evento**. Per **i flussi periodici** si tratta di informazioni che vengono trasmesse periodicamente ad esempio con cadenza trimestrale/semestrale o annuale a seconda della tipologia/dimensione dell'Ente, consentono all'OdV di monitorare l'adeguatezza ed efficacia del modello. Sarà compito dell'OdV adottare una specifica procedura di regimentazione della gestione dei flussi informativi. Dovrà essere individuato il responsabile del flusso, il contenuto del flusso, la modalità di invio del flusso e la tempistica dell'inoltro del flusso. In ogni caso tutti i dipendenti che verranno a conoscenza di notizie relative a comportamenti non in linea con quanto previsto dal modello e codice entico avranno l'obbligo di informare direttamente l'OdV. I **flussi ad evento** attengono a tutte quelle informazioni che vengono inviate immediatamente all'OdV nel caso in cui si verifichino delle criticità o si realizzi un evento che possa generale un reato presupposto. A titolo esemplificativo andranno essere comunicati all'OdV: -tutti gli infortuni sia di minore gravità sia quelli con prognosi superiore a 40 giorni, nonché infortuni mortali che coinvolgano sia dipendenti della società che personale di imprese appaltatrici, ciò al fine di identificare eventuali criticità e proporre modifiche al modello. Allo stesso tempo rientrano tra gli eventi rilevanti le modiche, i conferimenti o revoche di deleghe e sub deleghe ai sensi dell'art. 16 D.Lgs n. 81/08, così come le visite ispettive e le prescrizioni impartite dagli organi di sicurezza pubblica (asl – ispettorato del lavoro - p.a. o polizia giudiziaria). Con riguardo all'aerea HR è considerato obbligo di informare immediatamente l'OdV nel caso in cui sia apportata una variazione del codice disciplinare aziendale. Vanno comunicati all'OdV i cambiamenti e aggiornamenti dell'organigramma societario, nonché la sospensione delle certificazioni rilasciate dagli organi proposti con l'indicazione delle cause di revoca. - Vanno trasmessi gli estratti di verbale dell'organo amministrativo avanti ad aggetto tematiche collegate al D.Lgs n. 231, oltre alle modifiche riguardante la compagine societaria, la proprietà e composizione degli organi sociali. - Vanno segnati i provvedimenti o le notizie provenienti dall'A.G. dai quali si evinca lo svolgimento di indagini in relazione ad ipotesi di reato ai sensi del Decreto. - L'interna Audi e il risk managment hanno l'obbligo di trasmettere all'OdV i report relativi al rischio reato 231 nonché il piano di Audit approvato dall'organo amministrativo. - Con il Decreto Legislativo n. 24/2023, il Gestore delle Segnalazioni deve informare immediatamente l'OdV nel caso in cui pervengano segnalazioni rilevanti ai sensi del D.Lgs. n. 231/2001 ovvero

violazioni del MOG e lo aggiorni periodicamente sull'attività complessiva di gestione delle segnalazioni Allo stesso tempo anche l'OdV ha il dovere di inviare delle informazioni/flussi alle strutture aziendale di riferimento affinché queste ultime possano effettuare un monitoraggio sull'attività svolta dall'OdV; anche in questo caso i flussi possono essere continuativi periodico o ad evento. In particolare: - assicurare il tempestivo e periodico reporting inerente al rispetto del modello ai vertici aziendali anche a mezzo mail; - segnalare agli organi competenti, per gli opportuni provvedimenti, le eventuali violazioni del modello; - in caso di controlli da parte di soggetti istituzionali, ivi inclusa la Pubblica Autorità, fornire il necessario supporto informativo agli organi ispettivi. Più precisamente con periodicità annuale, l'OdV è tenuto ad elaborare e presentare al Consiglio di Amministrazione/Amministratore Unico e Collegio Sindacale una relazione in merito all'attuazione del Modello ed all'attività svolta nonché segnalare eventuali innovazioni legislative in materia di responsabilità amministrativa degli Enti, presentando il piano di vigilanza per l'anno successivo. Rispetto alle segnalazioni di cui sopra l'OdV svolge, altresì, un ruolo di gestione e al controllo. Ogni informazione e segnalazione prevista nel modello è conservata dall'organismo di vigilanza in un apposito archivio in conformità alle disposizioni contenute nel decreto Legislativo n. 196/2003 (privacy). A carico dei componenti l'organismo di vigilanza vi è l'obbligo assoluto e inderogabile di mantenere il segreto sulle attività svolte e sulle informazioni societarie di cui vengono a conoscenza nell'esercizio del loro mandato.

10 Disciplina WHISTLEBLOWING

Ambito di applicazione della riforma. Con il decreto legislativo 10 marzo 2023, n. 24 (di seguito anche " *Decreto* "), pubblicato nella Gazzetta Ufficiale del 15 marzo 2023, è stata recepita nell'ordinamento italiano la direttiva UE 2019/1937 riguardante <la protezione delle persone che segnalano violazioni del diritto dell'Unione> (cd. disciplina *whistleblowing*). L'obiettivo della direttiva europea è stabilire norme minime comuni per garantire un elevato livello di protezione delle persone che segnalano violazioni del diritto dell'Unione, creando canali di comunicazione sicuri, sia all'interno di un'organizzazione, sia all'esterno. Il Decreto abroga e modifica la disciplina nazionale previgente, racchiudendo in un unico testo normativo – per il settore pubblico e per il settore privato – il regime di protezione dei soggetti che segnalano condotte illecite poste in essere in violazione non solo di disposizioni europee, ma anche nazionali, purché basate su fondati motivi e lesive dell'interesse pubblico o dell'integrità dell'ente, al fine di garantire il recepimento della direttiva senza arretrare nelle tutele già riconosciute nel nostro ordinamento. Il quadro di riferimento è stato infine completato con le Linee Guida ANAC (di seguito anche *"LG ANAC"*), adottate con delibera del 12 luglio 2023 e successivamente integrate con quelle approvate con la delibera 478 del 26/11/2025, con le quali sono stati affrontati temi come il canale interno, la gestione delle segnalazioni, la formazione, il ruolo dell'OdV e la gestione delle segnalazioni nei gruppi di società. Il Decreto prevede che la nuova disciplina si applichi, in via generale, a decorrere dallo scorso 15 luglio 2023 (art. 24). Invece, per i soggetti del settore privato che, nell'ultimo anno, hanno impiegato una media di lavoratori subordinati fino a 249 unità, l'obbligo di istituire un canale interno di segnalazione ha effetto a decorrere dal 17 dicembre 2023; fino a quel giorno, continua ad applicarsi la disciplina previgente (art. 6, co. 2-bis del Decreto legislativo 8 giugno 2001, n. 231, di seguito anche " *Decreto 231"*). **Ambito soggettivo di applicazione: i destinatari della nuova disciplina.** I destinatari della nuova disciplina sono sia i soggetti pubblici che privati (artt. 2 e 3). I soggetti del settore pubblico sono le amministrazioni pubbliche, le autorità amministrative indipendenti, gli enti pubblici economici, i concessionari di pubblico servizio, le imprese a controllo pubblico e le imprese *in house*, anche se quotate. I soggetti del settore privato sono quelli che: - hanno impiegato, nell'ultimo anno, la media di almeno 50 lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato; - rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti I.B e II dell'Allegato al Decreto (che ripropone l'Allegato alla Direttiva UE), anche se nell'ultimo anno non hanno raggiunto la media di 50 lavoratori subordinati. Si tratta dei settori dei servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e del finanziamento del terrorismo, nonché della sicurezza dei trasporti; - sono diversi dai soggetti di cui al numero b), sono dotati di un Modello di Organizzazione e Gestione adottato ai sensi del D.Lgs. n. 231/2001, anche se nell'ultimo anno non hanno raggiunto la media di 50 lavoratori subordinati. Ai fini

del computo della media annua dei lavoratori impiegati nel settore privato, nonostante ANAC abbia suggerito di far riferimento al valore medio degli addetti al 31/12 dell'anno solare precedente a quello in corso contenuto nelle visure camerali (rif. LG ANAC, pag. 17), Confindustria ritiene che debba prendersi a parametro di calcolo l'art. 27 del D.Lgs. n. 81/2015, ma con un termine temporale di riferimento pari a un anno anziché due, come previsto dall'art. 2, comma 1, n. 1 del Decreto. **Ambito oggettivo di applicazione – Oggetto della violazione.** Dal punto di vista oggettivo, la nuova disciplina si applica alle violazioni delle disposizioni normative nazionali e dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui i soggetti segnalanti siano venuti a conoscenza in un contesto lavorativo pubblico o privato (art. 1). Per quanto riguarda il settore privato, le segnalazioni possono avere a oggetto: a) violazioni della disciplina nazionale solo con riferimento ai reati 231 e alle violazioni del MOGC dunque: - i reati presupposto per l'applicazione del Decreto n. 231; - le violazioni dei Modelli di Organizzazione e Gestione previsti nel citato Decreto n. 231 non riconducibili alle violazioni del diritto dell'UE come sotto definite; b) violazioni della normativa europea: - illeciti commessi in violazione della normativa dell'UE indicata nell'Allegato 1 al Decreto e di tutte le disposizioni nazionali che ne danno attuazione (anche se queste ultime non sono espressamente elencate nel citato allegato). Si precisa che le disposizioni normative contenute nell'Allegato 1 sono da intendersi come un riferimento dinamico in quanto vanno naturalmente adeguate al variare della normativa stessa. In particolare, si tratta di illeciti relativi ai seguenti settori: contratti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi. - atti od omissioni che ledono gli interessi finanziari dell'Unione Europea (art. 325 del TFUE lotta contro la frode e le attività illegali che ledono gli interessi finanziari dell'UE) come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE. - atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE). Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposta sulle imprese e i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle imprese; - atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea nei settori indicati ai punti precedenti. In tale ambito vanno ricondotte, ad esempio, le pratiche abusive quali definite dalla giurisprudenza della Corte di Giustizia dell'UE. Sono escluse dall'ambito di applicazione della nuova disciplina le segnalazioni legate a un interesse personale del segnalante (es. vertenze di lavoro, discriminazioni, conflitti interpersonali tra colleghi, segnalazioni su trattamenti di dati effettuati nel contesto del rapporto individuale di lavoro in assenza di una lesione dell'interesse pubblico o dell'integrità dell'ente privato o dell'amministrazione pubblica). Le contestazioni escluse in quanto legate a un interesse personale del segnalante non sono, pertanto, considerate segnalazioni *whistleblowing* e, quindi, potranno essere trattate come segnalazioni ordinarie, laddove previsto: - in materia di sicurezza e difesa nazionale; - relative a violazioni già regolamentate in via obbligatoria in alcuni settori speciali, alle quali continua dunque ad applicarsi la disciplina di segnalazione *ad hoc* (servizi finanziari, prevenzione riciclaggio, terrorismo, sicurezza nei trasporti, tutela dell'ambiente). Resta poi ferma la normativa in materia di: i) informazioni classificate; ii) segreto medico e forense; iii) segretezza delle deliberazioni degli organi giurisdizionali; iv) norme di procedura penale sull'obbligo di segretezza delle indagini; v) disposizioni sull'autonomia e indipendenza della magistratura; vi) difesa nazionale e di ordine e sicurezza pubblica; vii) esercizio del diritto dei lavoratori di consultare i propri rappresentanti o i sindacati. **Definizione e contenuto della segnalazione.** Le segnalazioni sono definite come le informazioni, compresi i fondati sospetti, su violazioni già commesse o non ancora commesse (ma che, sulla base di elementi concreti, potrebbero esserlo), nonché su condotte volte ad occultarle (es. occultamento o distruzione di prove). Si deve poi trattare di comportamenti, atti od omissioni di cui il segnalante o il denunciante sia venuto a conoscenza nel contesto lavorativo. Le segnalazioni possono essere effettuate anche da coloro che hanno instaurato con l'ente altri tipi di rapporti giuridici. Ci si riferisce, fra l'altro, ai consulenti, collaboratori, volontari, tirocinanti, azionisti degli stessi soggetti pubblici e privati ove assumano la forma societaria e alle persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza. Al riguardo, con

riferimento agli azionisti, le LG ANAC chiariscono il perimetro di applicazione della disciplina e, in particolare, delle segnalazioni, precisando che si tratta di *"coloro che siano venuti a conoscenza di violazioni oggetto di segnalazione nell'esercizio dei diritti di cui sono titolari in ragione del loro ruolo di azionisti rivestito nell'impresa"* (cit.). La disciplina si applica anche nel caso di segnalazioni che intervengano nell'ambito di un rapporto di lavoro poi terminato, se le informazioni sono state acquisite durante il suo svolgimento, nonché qualora il rapporto non sia ancora iniziato e le informazioni sulle violazioni siano state acquisite durante la selezione o in altre fasi precontrattuali. Quanto al contenuto, le segnalazioni devono essere il più possibile circostanziate, al fine di consentire la valutazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni. In particolare, è necessario che risultino chiari i seguenti elementi essenziali della segnalazione, anche ai fini del vaglio di ammissibilità: - i dati identificativi della persona segnalante (nome, cognome, luogo e data di nascita), nonché un recapito a cui comunicare i successivi aggiornamenti; - le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione e, quindi, una descrizione dei fatti oggetto della segnalazione, specificando i dettagli relativi alle notizie circostanziali e ove presenti anche le modalità con cui si è venuto a conoscenza dei fatti oggetto della segnalazione; - le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati. Inoltre, nel caso di utilizzo del canale analogico, sarebbe utile che il segnalante indichi espressamente di voler beneficiare delle tutele in materia *whistleblowing* (ad es. inserendo la dicitura *"riservata al gestore della segnalazione"*), soprattutto al fine di gestire correttamente l'eventuale invio, per errore, della segnalazione a un soggetto diverso dal gestore. È utile anche che, alla segnalazione, vengano allegati documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti. **Canali di segnalazione e soggetti legittimati a segnalare.** Il Decreto disciplina i canali e le modalità per effettuare una segnalazione. In particolare, quanto ai canali, si distinguono tre fattispecie: a) la segnalazione attraverso un canale interno all'ente; b) la segnalazione mediante un canale esterno all'ente, istituito e gestito dall'ANAC; c) la divulgazione pubblica. Resta ferma, in ogni caso, la possibilità di effettuare denunce all'Autorità giudiziaria e contabile, nei casi di loro competenza. Al riguardo, pur non indicando espressamente un ordine di priorità tra le diverse modalità di segnalazione, il Decreto fissa condizioni specifiche previste dall'art. 6 – sebbene con formule talvolta eccessivamente generiche – per accedere sia alla procedura esterna che alla divulgazione pubblica. Su tale aspetto, anche le LG ANAC ribadiscono una gradualità nella scelta del canale di segnalazione più idoneo al caso concreto, da un lato, ribadendo la priorità del ricorso al canale interno. Con riferimento invece alle tipologie e alle modalità per effettuare le segnalazioni, la disciplina cambia in base alle dimensioni e alla natura pubblica o privata del soggetto di appartenenza del segnalante. Nel settore privato, operano diversi regimi. In particolare, negli enti privati che: - non hanno raggiunto la media di 50 lavoratori e hanno adottato il Modello Organizzativo 231: le segnalazioni possono riguardare solo condotte illecite rilevanti per la disciplina 231 o violazioni del Modello 231 ed essere effettuate unicamente attraverso il canale interno; - hanno impiegato la media di almeno 50 lavoratori e hanno adottato il Modello Organizzativo 231, le segnalazioni possono: i. avere a oggetto condotte illecite o violazione del Modello Organizzativo 231 ed essere effettuate solo attraverso canale interno; ii. avere a oggetto violazioni del diritto UE ed essere effettuate attraverso canale interno, esterno, divulgazione pubblica o denuncia. Quanto ai soggetti legittimati a presentare le segnalazioni, le stesse possono essere fatte da: lavoratori dipendenti e autonomi, liberi professionisti e consulenti, lavoratori e collaboratori che svolgono la propria attività presso soggetti pubblici o privati, i volontari, i tirocinanti, gli azionisti, e le persone con funzione di direzione amministrazione e controllo (art. 3). **Canale interno di segnalazione.** Ai sensi dell'art. 4 del Decreto, gli enti rientranti nel perimetro di applicazione della disciplina sul *whistleblowing* sono obbligati ad attivare un canale di segnalazione interno adeguato, che presenti i requisiti richiesti dalla normativa. Inoltre, con la modifica all'articolo 6, comma 2-bis del Decreto 231, il Decreto *whistleblowing* impone agli enti che adottano il Modello Organizzativo 231 di prevedere, all'interno dello stesso, canali di segnalazione interna conformi alle prescrizioni del Decreto, nonché il divieto di ritorsione e il relativo sistema disciplinare. **Requisiti e strumenti.** I canali di segnalazione interna, per essere ritenuti adeguati, devono essere idonei ad assicurare la riservatezza dell'identità del segnalante e delle persone coinvolte (segnalato, facilitatore, eventuali altri terzi), del contenuto della segnalazione e della documentazione a essa relativa. Per quanto attiene agli strumenti concreti attraverso cui attivare il canale di segnalazione interno, l'articolo 4 del Decreto prevede che le segnalazioni possono

essere effettuate secondo diverse modalità: - in forma scritta: analogica o con modalità informatiche; - in forma orale, attraverso linee telefoniche dedicate o sistemi di messaggistica vocale e, su richiesta del segnalante, attraverso un incontro diretto con il gestore della segnalazione. E' importante evidenziare che da ultimo le ultime LG Guida del 26/11/2025 hanno confermato la preferenza per le piattaforme informatiche, conforme al GDPR, poiché quest'ultima garantiscono un maggior livello di protezione dei dati del segnalatore. Laddove ciò non sia possibile resta la possibilità di poter procedere alla protocollazione riservata in doppia busta, in quest'ultimo caso la vera novità è costituita dalla circostanza che non sarà più indispensabile inserire la copia del documento di identità del segnalante, così come previsto allorquando invece si utilizzi la piattaforma informatica. **Istituzione.** I soggetti cui si applica il Decreto, sentite le rappresentanze o le organizzazioni sindacali, hanno l'onere di definire in un apposito atto organizzativo le procedure per il ricevimento delle segnalazioni e per la loro gestione, predisponendo e attivando al proprio interno appositi canali di segnalazione. Il concetto di riservatezza dell'identità del segnalante deve essere ben distinto dall'anonimato. Le segnalazioni anonime non sono considerate *whistleblowing*. La norma non stabilisce in dettaglio il **contenuto della procedura adottata con l'atto organizzativo**, ma si ritiene opportuno che contenga i seguenti elementi (che saranno oggetto di un'analisi specifica nei paragrafi successivi): - i soggetti legittimati a presentare le segnalazioni, come sopra riportati; - i soggetti che godono delle misure di protezione previste dal Decreto; - l'ambito oggettivo delle segnalazioni ammesse e di quelle estranee all'ambito applicativo della disciplina *whistleblowing*, con le differenti conseguenze in termini di procedura di gestione e misure di tutela garantite; - i presupposti per procedere alla segnalazione interna e le relative condizioni di ammissibilità; - il soggetto, interno o esterno, al quale è affidata la gestione delle segnalazioni, i relativi poteri e gli obblighi, nonché l'eventuale *budget* a disposizione per attività di valutazione e gestione delle segnalazioni, con evidenza della sussistenza dei requisiti richiesti dalla norma; - le modalità per l'eventuale coinvolgimento da parte del gestore di altri soggetti, interni all'ente o esterni, di cui risulti necessario avvalersi per la gestione della segnalazione. A tal fine, l'ente potrebbe riservarsi di procedere autonomamente e, di volta in volta, alle conseguenti designazioni *privacy*, oppure delegare specificamente il gestore a procedere in tal senso; - le modalità concrete scelte dall'impresa per l'utilizzo del canale di segnalazione interno (posta cartacea/piattaforma *on line*, numero telefonico/sistema messaggistica vocale); - la procedura che il soggetto gestore deve seguire per la gestione delle segnalazioni interne, con indicazione delle varie fasi dell'istruttoria e delle tempistiche di riferimento, in linea con quanto previsto dal Decreto; - la procedura da seguire nel caso in cui una persona diversa da quella alla quale è affidata la gestione delle segnalazioni riceva una segnalazione identificabile come *whistleblowing*; - la politica adottata per le ipotesi di segnalazioni anonime o inammissibili; - le modalità e i termini di conservazione dei dati appropriati e proporzionati ai fini della procedura di *whistleblowing*; - i necessari adeguamenti prescritti dall'art. 13 per il trattamento dei dati personali; - i presupposti per ricorrere alla segnalazione esterna; - le modalità attraverso cui verranno comunicate ai soggetti potenzialmente interessati le informazioni sull'utilizzo del canale interno e di quello esterno, nonché la previsione circa l'attività di formazione sulla disciplina e la procedura stessa. **Informativa alle rappresentanze sindacali.** Nell'implementare il canale di segnalazione interno, come detto, l'art. 4 del Decreto prevede che l'impresa sia tenuta a sentire *"le rappresentanze o le organizzazioni sindacali di cui all'art. 51 del D.lgs. n.81 del 2015"*, ovvero le rappresentanze sindacali aziendali (o la rappresentanza sindacale unitaria, di seguito anche "RSU") o le associazioni sindacali comparativamente più rappresentative sul piano nazionale. Le nuove linee guida hanno ancora una volta sottolineato che il parere rilasciato dalle organizzazioni sindacali non ha carattere vincolante ma è obbligatorio richiederlo diversamente alla società o ente potrebbe essere applicata una delle sanzioni previste dall'art. 21 del D.Lgs. n. 24/2023. Nell'informativa che verrà inviata alle organizzazioni sindacali dovrà essere sempre assegnato un termine, non perentorio, entro cui dovrà pervenire il parere e che sia fornita una descrizione del canale, almeno negli elementi essenziali che lo caratterizzano. **Gestione della segnalazione.** La gestione delle segnalazioni interne dovrà essere conforme ai parametri indicati nella presente Parte del Modello 231. I dettagli applicativi specifici verranno individuati nell'ambito dell'atto organizzativo e delle procedure operative adottate dalla Società; a tali documenti, pertanto, il Modello 231 rinvia. **I soggetti destinatari delle segnalazioni.** L'art. 4, comma 2, del Decreto prevede che la gestione del canale di segnalazione interno possa essere affidata a una persona fisica interna all'impresa; a un ufficio interno all'impresa; a un soggetto esterno. Tali soggetti devono essere dotati di autonomia e specificamente e adeguatamente formati

alla gestione delle segnalazioni. I soggetti che gestiranno le segnalazioni devono essere dotati di autonomia e specificamente e adeguatamente formati alla gestione delle segnalazioni In particolare, tale requisito deve essere inteso come: - imparzialità: mancanza di condizionamenti e di pregiudizi nei confronti delle parti coinvolte nelle segnalazioni *whistleblowing*, al fine di assicurare una gestione delle segnalazioni equa e priva di influenze interne o esterne che possano comprometterne l'obiettività; - indipendenza: autonomia e libertà da influenze o interferenze da parte del *management*, al fine di garantire un'analisi oggettiva e imparziale della segnalazione. Per quanto attiene l'individuazione della figura più idonea a cui affidare la gestione del canale di segnalazione, si riportano di seguito alcune considerazioni derivanti dalle più accreditate *best practice* aziendali. **Persona fisica interna all'impresa.** Qualora l'impresa decida di affidare la gestione del canale di segnalazione interno a una persona fisica già presente all'interno della sua organizzazione, tale ruolo potrà essere ricoperto dal responsabile anticorruzione, ove presente, ovvero dai responsabili delle funzioni di *Internal Audit* o *compliance*. Tuttavia, nel caso di medie e piccole imprese nelle quali le funzioni di *Internal Audit* e *compliance* non siano presenti, si potrebbe affidare il ruolo di gestore della segnalazione a una figura priva di mansioni operative, in modo da rispettare il criterio di autonomia previsto dalla normativa. **Ufficio/Organismo interno all'impresa.** Come opzione interna ulteriore rispetto a quella del paragrafo precedente, le imprese possono decidere di affidare la gestione del canale a un loro ufficio interno preesistente o a un organo collegiale/comitato appositamente costituito e composto da soggetti interni che, nel suo complesso, risponda al requisito di autonomia necessario. Tale comitato potrebbe essere composto, ad esempio, dai responsabili delle funzioni di controllo *(compliance* o *Internal Audit*) e di alcune delle altre funzioni aziendali in grado di gestire in maniera appropriata e diligente la segnalazione (si pensi, ad esempio, alle funzioni legali o alle funzioni risorse umane, al responsabile anticorruzione o a Comitati Etici, nonché, all'Organismo di vigilanza 231 - OdV -, se monocratico, o a un suo membro, se collegiale). Laddove l'OdV non sia individuato come gestore dovrà ricevere: - immediata informativa su segnalazioni rilevanti in termini 231 affinché, nell'esercizio della sua attività di vigilanza, possa condividere le proprie eventuali osservazioni e partecipare all'istruttoria o comunque seguirne l'andamento; - un aggiornamento periodico sull'attività complessiva di gestione delle segnalazioni, anche non 231, al fine di verificare il funzionamento del sistema *whistleblowing* e proporre all'ente eventuali necessità di suo miglioramento. A tal fine, nel Modello Organizzativo 231 dovranno essere procedimentalizzati i predetti flussi informativi. Sia nel caso di persona fisica interna, sia nel caso di ufficio interno è necessario un formale atto di nomina con cui si attribuisce al soggetto l'incarico di gestore della segnalazione. **Ufficio esterno all'impresa.** Nel caso in cui le imprese decidessero di affidare la gestione del canale di segnalazione a un soggetto esterno, dovranno verificare che lo stesso abbia i requisiti di autonomia, indipendenza e professionalità necessari. **L'attività di gestione delle segnalazioni.** Le segnalazioni interne sono gestite attraverso l'attivazione e messa a disposizione dei seguenti canali: **Canali in forma scritta: posta ordinaria o piattaforma informatica.** Nel caso in cui l'impresa decidesse di utilizzare la posta ordinaria come canale di segnalazione interno (es. lettere raccomandate), al momento della ricezione, gli uffici o la persona individuati a gestire le segnalazioni devono: - garantire la riservatezza dell'identità del segnalante e del contenuto delle buste; - procedere all'archiviazione della segnalazione attraverso idonei strumenti che permettano di garantire la riservatezza (ad esempio all'interno di archivi protetti da misure di sicurezza). Ad esempio, è possibile prevedere che la segnalazione venga inserita in due buste chiuse, includendo, nella prima, i dati identificativi del segnalante; nella seconda, l'oggetto della segnalazione; entrambe le buste dovranno poi essere inserite in una terza busta riportando, all'esterno, la dicitura *"riservata al gestore della segnalazione"*. La scelta tra piattaforma *on line* e modalità analogica/cartacea è una valutazione rimessa alla singola impresa, in funzione di diverse considerazioni riconducibili al contesto, alla dimensione aziendale, alla funzionalità rispetto allo scopo e al livello di sicurezza e riservatezza garantito dalle soluzioni adottate. Al riguardo le LG ANAC, in linea con il parere reso dal Garante per la protezione dei dati personali, escludono espressamente che la posta elettronica ordinaria e la PEC siano strumenti adeguati a garantire la riservatezza. Canali in forma orale: linee telefoniche o sistemi di messaggistica vocale. Nel caso di utilizzo di una linea telefonica registrata o di un altro sistema di messaggistica registrato, il gestore della segnalazione deve conservare, previo consenso del segnalante alla registrazione, la segnalazione all'interno di un dispositivo idoneo alla conservazione e all'ascolto. Contrariamente, nel caso si utilizzino linee telefoniche non registrate, al momento della ricezione della segnalazione, il personale addetto deve

documentarla mediante resoconto dettagliato del messaggio e il contenuto dev'essere controfirmato dal segnalante, previa verifica ed eventuale rettifica. Del resoconto sottoscritto deve essere fornita copia al segnalante. **Canali in forma orale: incontro diretto.** Ulteriore novità introdotta dal Decreto riguarda la possibilità del *whistleblower* di richiedere un incontro diretto agli uffici o alla persona deputati alla gestione della segnalazione. In tal caso, l'impresa deve garantire lo svolgimento dell'incontro entro un termine ragionevole (ad esempio, entro 10/15 giorni). Per quanto attiene alle modalità di svolgimento dell'incontro (in un luogo adatto a garantire la riservatezza del segnalante) è sempre consigliabile procedere - previo consenso della persona segnalante - alla registrazione dello stesso attraverso dispositivi idonei alla conservazione e all'ascolto. Diversamente sarà necessario stilare un verbale, che dovrà essere sottoscritto anche dalla persona segnalante, che ne riceverà una copia oltre che dal soggetto che ha ricevuto la dichiarazione. **Ricezione della segnalazione.** Il Decreto prevede anzitutto che il gestore della segnalazione debba rilasciare al segnalante l'avviso di ricevimento entro sette giorni dalla presentazione della segnalazione stessa. Si evidenzia che tale riscontro non implica per il gestore alcuna valutazione dei contenuti oggetto della segnalazione, ma è unicamente volto a informare il segnalante dell'avvenuta corretta ricezione della stessa. Tale avviso dev'essere inoltrato al recapito indicato dal segnalante nella segnalazione. In assenza di tale indicazione e, dunque, in assenza della possibilità di interagire con il segnalante per i seguiti, è possibile considerare la segnalazione come non gestibile ai sensi della disciplina *whistleblowing* (lasciando traccia di tale motivazione) ed eventualmente trattarla come segnalazione ordinaria. **Segnalazioni anonime.** Anche alla luce delle indicazioni dell'ANAC, si specifica che le stesse, qualora risultino puntuali, circostanziate e supportate da idonea documentazione, possono essere equiparate dall'impresa alle segnalazioni ordinarie e, in quanto tali, possono essere trattate in conformità ai regolamenti interni, laddove eventualmente implementati. In ogni caso, le segnalazioni anonime dovranno essere registrate dal gestore della segnalazione e la documentazione ricevuta dovrà essere conservata. Infine, il Decreto (art. 4, co. 6) prevede che, qualora la segnalazione interna sia presentata a un soggetto diverso da quello individuato e autorizzato dall'ente e sia evidente che si tratti di segnalazione *whistleblowing*, la stessa vada trasmessa, entro sette giorni dal suo ricevimento e senza trattenerne copia, al soggetto competente, dando contestuale notizia della trasmissione alla persona segnalante. Completata la fase relativa alla trasmissione dell'avviso di ricevimento si passerà alla fase della valutazione e dell'ammissibilità della segnalazione. Di seguito alcune valutazioni che possono essere effettuate in tali fasi. **La procedibilità della segnalazione.** Come visto in precedenza, il Decreto definisce i presupposti soggettivi e oggettivi per effettuare una segnalazione interna. Pertanto, per poter dare corso al procedimento, il gestore della segnalazione dovrà, per prima cosa, verificare la sussistenza di tali presupposti e, nello specifico, che il segnalante sia un soggetto legittimato a effettuare la segnalazione e che l'oggetto della segnalazione rientri tra gli ambiti di applicazione della disciplina. Nel caso in cui la segnalazione riguardi una materia esclusa dall'ambito oggettivo di applicazione, la stessa potrà essere trattata come ordinaria e, quindi, gestita secondo le eventuali procedure già in precedenza adottate dall'ente per tali violazioni, dandone comunicazione al segnalante. **L'ammissibilità della segnalazione.** Una volta verificato che la segnalazione abbia i requisiti soggettivi e oggettivi definiti dal legislatore e, dunque, risulti procedibile, è necessario valutarne l'ammissibilità come segnalazione *whistleblowing*. Ai fini dell'ammissibilità, è necessario che, nella segnalazione, risultino chiare: - le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione e, quindi, una descrizione dei fatti oggetto della segnalazione, che contenga i dettagli relativi alle notizie circostanziali e, ove presenti, anche le modalità attraverso cui il segnalante è venuto a conoscenza dei fatti; - le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati. Alla luce di queste indicazioni, la segnalazione può, quindi, essere ritenuta inammissibile e si potrà procedere all'archiviazione della stessa con congrua motivazione. Inoltre, durante la verifica preliminare gli uffici o la persona deputati alla gestione della segnalazione possono: - nel caso di organo collegiale, nominare tra i propri membri un soggetto con il ruolo di coordinatore per la gestione della segnalazione; - richiedere al segnalante ulteriori elementi necessari per effettuare approfondimenti relativi alla segnalazione. Una volta verificata la procedibilità e l'ammissibilità della segnalazione, il gestore avvia l'istruttoria interna sui fatti e sulle condotte segnalate al fine di valutarne la fondatezza. **Istruttoria e accertamento della segnalazione.** Gli uffici o la persona incaricati di gestire le segnalazioni assicurano che siano effettuate tutte le opportune verifiche sui fatti segnalati, garantendo tempestività e rispetto dei principi di obiettività, competenza e diligenza professionale.

Inoltre, nel caso in cui la segnalazione riguardasse il gestore della segnalazione, dovranno essere garantite le opportune misure per gestire un potenziale conflitto di interessi. Per tale ragione, sempre in un'ottica di maggior tutela del soggetto segnalante, in riferimento alla disciplina del conflitto di interessi, le linee guida prevedono l'individuazione di un sostituto del gestore prima che si possa verificare l'insorgenza di un possibile conflitto. Infine, laddove non sarà possibile individuare un sostituto, sarà sempre possibile rivolgersi direttamente ad ANAC. Gli uffici o la persona incaricati di gestire le segnalazioni devono assicurare lo svolgimento delle necessarie verifiche, a titolo esemplificativo: - direttamente acquisendo gli elementi informativi necessari alle valutazioni attraverso l'analisi della documentazione/informazioni ricevute; - attraverso il coinvolgimento di altre strutture aziendali o anche di soggetti specializzati esterni (es. IT *specialist*) in considerazione delle specifiche competenze tecniche e professionali richieste; - mediante audizione di eventuali soggetti interni/esterni, ecc. Nel caso in cui risulti necessario avvalersi dell'assistenza tecnica di professionisti terzi, nonché del supporto specialistico del personale di altre funzioni/direzioni aziendali è necessario - al fine di garantire gli obblighi di riservatezza richiesti dalla normativa - oscurare ogni tipologia di dato che possa consentire l'identificazione della persona segnalante o di ogni altra persona coinvolta (si pensi, ad esempio, al facilitatore o ulteriori persone menzionate all'interno della segnalazione). Nel caso sia necessario il coinvolgimento di soggetti interni diversi dal gestore (altre funzioni aziendali), anche ad essi andranno estesi gli obblighi di riservatezza. Qualora tali dati siano necessari all'indagine condotta da soggetti esterni (eventualmente coinvolti dal gestore), sarà necessario estendere i doveri di riservatezza e confidenzialità previsti dal Decreto in capo al gestore anche a tali soggetti esterni mediante specifiche clausole contrattuali da inserire negli accordi stipulati con il soggetto esterno. Qualora la segnalazione abbia a oggetto una violazione del Modello o tematiche attinenti ai dati contabili, è consigliabile operare in sinergia con gli organi competenti, nel rispetto degli obblighi di riservatezza (ad esempio, l'OdV, qualora non sia ovviamente esso stesso il gestore della segnalazione o il Collegio sindacale). Una volta completata l'attività di accertamento, il gestore della segnalazione può: - archiviare la segnalazione perché infondata, motivandone le ragioni e dandone comunicazione al whistleblower; - dichiarare fondata la segnalazione e rivolgersi agli organi/funzioni interne competenti per i relativi seguiti poiché al gestore della segnalazione non compete alcuna valutazione in ordine alle responsabilità, agli eventuali successivi provvedimenti o procedimenti conseguenti. Tutte le fasi dell'attività di accertamento devono essere sempre tracciate e archiviate correttamente a seconda della tipologia del canale di segnalazione utilizzato al fine di dimostrare la corretta diligenza tenuta nel dare seguito alla segnalazione. **Riscontro al segnalante.** Il Decreto dispone che il gestore della segnalazione debba fornire un riscontro al segnalante, entro tre mesi dalla data di avviso di ricevimento o - in mancanza di tale avviso - entro tre mesi dalla data di scadenza del termine di sette giorni per tale avviso. Pertanto, alla scadenza dei tre mesi, il gestore della segnalazione può comunicare al segnalante: - l'avvenuta archiviazione della segnalazione, motivandone le ragioni; - l'avvenuto accertamento del *fumus* di fondatezza della segnalazione e la sua trasmissione degli esiti agli organi interni competenti; - l'attività svolta fino a questo momento e/o l'attività che intende svolgere. In tale ultimo caso, è consigliabile comunicare alla persona segnalante anche il successivo esito finale dell'istruttoria della segnalazione in linea con le LG ANAC. **Canali di segnalazione in condivisione e all'interno dei gruppi – Condivisione del canale per le imprese fino a 249 dipendenti**. Il Decreto, recependo il dettato della Direttiva (art. 8, co. 6), ha previsto all'art. 4, co. 4 per i soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, non superiore a 249, le nuove linee guida hanno confermato la possibilità per gli enti di adottare un'unica piattaforma ramificata in sotto-canali, ciascuno riferito a una società del gruppo. Nelle Linee Guida, l'ANAC ha precisato che, nel caso in cui più soggetti privati decidano di affidare a uno stesso soggetto (esterno) la gestione delle segnalazioni, *"è necessario garantire che ciascun ente acceda esclusivamente alle segnalazioni di propria spettanza tenuto anche conto della attribuzione della relativa responsabilità. Pertanto, dovranno essere adottate misure tecniche e organizzative per garantire che ciascun ente abbia accesso solo alle segnalazioni di propria competenza"*. **Gestione e delega delle segnalazioni interne nei gruppi con imprese sopra i 249 lavoratori dipendenti**. Per queste realtà aziendali le nuove linee guida confermano l'esternalizzazione della gestione del canale essendo vietato dal D.Lgs n. 24/2023 la possibilità di condivisione del canale per le segnalazioni. **Tutela del segnalante e dei soggetti a esso assimilati.** Uno dei principali cardini della disciplina del *whistleblowing* è rappresentato dalle tutele riconosciute al segnalante

per le segnalazioni effettuate nel rispetto della disciplina. In particolare, il Decreto si preoccupa di proteggere il segnalante con: - l'obbligo di riservatezza della sua identità; - il divieto di atti ritorsivi nei suoi confronti; - la limitazione della sua responsabilità per la rilevazione o diffusione di alcune tipologie di informazioni protette. Tali misure di protezione, con alcune eccezioni (su cui v. *infra*), si applicano non solo al soggetto segnalante ma anche ad altri soggetti. In particolare, si tratta dei seguenti soggetti: - facilitatore, ovvero la persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata; - persone del medesimo contesto lavorativo del segnalante, denunciante o di chi effettua una divulgazione pubblica e che sono legate a essi da uno stabile legame affettivo o di parentela entro il quarto grado; - colleghi di lavoro del segnalante, denunciante o di chi effettua una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente; - enti di proprietà - in via esclusiva o in compartecipazione maggioritaria di terzi - del segnalante, denunciante o di chi effettua una divulgazione pubblica; - enti presso i quali il segnalante, denunciante o chi effettua una divulgazione pubblica lavorano. **La riservatezza dell'identità del segnalante.** La prima tutela posta dal legislatore a favore del segnalante è l'obbligo di garantire la riservatezza della sua identità e di ogni altra informazione, inclusa l'eventuale documentazione allegata, dalla quale si possa direttamente o indirettamente risalire all'identità del *whistleblower*. Ai sensi dell'art. 2, co. 1, n. 6), lett. h) del Decreto, l'assistenza fornita dal facilitatore deve essere mantenuta riservata. La riservatezza deve essere garantita per ogni modalità di segnalazione, quindi, anche quando avvenga in forma orale (linee telefoniche, messaggistica vocale, incontro diretto). Nell'ambito del procedimento disciplinare attivato dall'ente contro il presunto autore della condotta segnalata, l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora invece la contestazione sia fondata, in tutto o in parte, sulla segnalazione e l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare o della persona comunque coinvolta nella segnalazione, quest'ultima sarà utilizzabile ai fini del procedimento disciplinare solo previo consenso espresso della persona segnalante alla rivelazione della propria identità. In tali casi, è dato preventivo avviso alla persona segnalante mediante comunicazione scritta delle ragioni che rendono necessaria la rivelazione dei dati riservati. Qualora il soggetto segnalante neghi il proprio consenso, la segnalazione non potrà essere utilizzata nel procedimento disciplinare che, quindi, non potrà essere avviato o proseguito in assenza di elementi ulteriori sui quali fondare la contestazione. Resta ferma in ogni caso, sussistendone i presupposti, la facoltà dell'ente di procedere con la denuncia all'Autorità giudiziaria. **Il divieto e la protezione contro le ritorsioni. La Convenzione dele Nazioni Unite contro la Corruzione (UNCAC) ha imposto a tutti i paesi firmatari della stessa di garantire una tutela nei confronti dei segnalatori.** In tal senso il Decreto, è vietata ogni forma di ritorsione nei confronti del segnalante, intesa come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, che si verifichi nel contesto lavorativo e che determini – in via diretta o indiretta – un danno ingiusto ai soggetti tutelati. Gli atti ritorsivi adottati in violazione di tale divieto sono nulli. La stessa tutela si applica anche nei confronti dei facilitatori e degli altri soggetti assimilati al segnalante, già citati (es. colleghi di lavoro). L'ANAC è l'autorità preposta a ricevere dal segnalante e gestire le comunicazioni su presunte ritorsioni dallo stesso subite e comminare al datore di lavoro una sanzione pecuniaria da 10.000,00 a 50.000,00 euro laddove dovesse accertare l'esistenza di una misura ritorsiva nei confronti del whistleblower. Avverso tale provvedimento sarà sempre possibile per il datore di lavoro impugnare innanzi al Tar competente il provvedimento sanzionatorio. Affinché sia riconosciuta tale forma di tutela, il Decreto prevede le seguenti condizioni: - che il segnalante/denunciante al momento della segnalazione o della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica avesse "fondato motivo" di ritenere le informazioni veritiere e rientranti nel perimetro applicativo della disciplina; - che la segnalazione, denuncia o divulgazione sia stata effettuata secondo la disciplina prevista dal Decreto. La norma all'art. 17, comma 4, fornisce un elenco delle possibili fattispecie ritorsive, sia pur non esaustivo e non tassativo: a) il licenziamento, la sospensione o misure equivalenti; b) la retrocessione di grado o la mancata promozione; c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro; d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa; e) le note di merito negative o le referenze negative; f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria; g) la

coercizione, l'intimidazione, le molestie o l'ostracismo; h) la discriminazione o comunque il trattamento sfavorevole; i) la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione; j) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; m) i danni, anche alla reputazione della persona, in particolare sui *social media*, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi; n) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro; o) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; p) l'annullamento di una licenza o di un permesso; q) la richiesta di sottoposizione ad accertamenti psichiatrici o medici. Accanto a questo elenco si inseriscono ulteriori esempi forniti dalle linee guida di ANAC, come ad esempio il raggiungimento di risultati impossibili in ambito lavorativo. Pertanto, il soggetto che ritenga di aver subito una ritorsione, anche tentata o minacciata, come conseguenza di una segnalazione/divulgazione/denuncia lo comunica all'ANAC, che dovrà accertare il nesso di causalità tra la ritorsione e la segnalazione e, quindi, adottare i conseguenti provvedimenti. Qualora l'Autorità consideri inammissibile la comunicazione, provvederà ad archiviarla; se, invece, dovesse accertarne la fondatezza e il nesso causale tra segnalazione e ritorsione avvierà il procedimento sanzionatorio. In caso di ritorsioni commesse nel contesto lavorativo di un soggetto del settore privato, l'Ufficio preposto informa l'Ispettorato Nazionale del Lavoro per i provvedimenti di competenza. Rimane invece di competenza dell'autorità giudiziaria disporre le misure necessarie ad assicurare la tutela del segnalante (reintegrazione nel posto di lavoro, risarcimento del danno, l'ordine di cessazione della condotta, nonché la dichiarazione di nullità degli atti adottati); sul punto sono da segnalare le seguenti sentenze in ambito whistleblowing: *"Sent. del Trib. di Milano Sez. Lavoro del 06/06/2025 n. 1680. Il Tribunale di Milano, con la sentenza n. 1680/2025 e Sentenza del Trib. di Bergamo Sez. Lavoro, Rv. "Il lavoro nella giurisprudenza", n.1, 1° gennaio 2026, 91, del 06/11/2025 n. 951 che entrambe riconoscevano la natura ritorsiva dei provvedimenti adottai ai lavoratori a seguito di una segnalazione"*. Nei procedimenti dinanzi ad ANAC, l'intento ritorsivo si presume. Opera, infatti, un'inversione dell'onere probatorio e, pertanto, laddove il *whistleblower* dimostri di avere effettuato una segnalazione, denuncia, o una divulgazione pubblica e di aver subito, a seguito della stessa, una ritorsione, l'onere della prova si sposta sulla persona che ha posto in essere la presunta ritorsione. Questa presunzione opera solamente a favore del segnalante e non anche a vantaggio del facilitatore e de soggetti a esso assimilati, che dovranno, quindi, dimostrare che gli atti subiti da parte del datore di lavoro sono conseguenti alla segnalazione effettuata dal segnalante. Si evidenzia che esistono dei casi in cui il segnalante perde la protezione: i) qualora sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di diffamazione o di calunnia o nel caso in cui tali reati siano commessi con la denuncia all'Autorità giudiziaria o contabile; ii) in caso di responsabilità civile per lo stesso titolo, per dolo o colpa grave. In entrambe le ipotesi alla persona segnalante o denunciante verrà irrogata una sanzione disciplinare. Le limitazioni di responsabilità per il segnalante. All'art. 20 del decreto è riconosciuta una ulteriore tutela al segnalante che prevede la limitazione della sua responsabilità rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni, che altrimenti lo esporrebbero a responsabilità penali, civili e amministrative. Il Decreto pone tuttavia due condizioni all'operare delle suddette limitazioni di responsabilità: 1) al momento della rivelazione o della diffusione vi siano fondati motivi per ritenere che le informazioni siano necessarie per svelare la violazione oggetto di segnalazione; 2) la segnalazione sia effettuata nel rispetto delle condizioni previste dal Decreto per beneficiare della tutela contro le ritorsioni. Va evidenziato, quindi, che la limitazione opera se le ragioni alla base della rivelazione o diffusione non sono fondate su semplici illazioni, *gossip*, fini vendicativi, opportunistici o scandalistici. In ogni caso, occorre considerare che non è esclusa la responsabilità per condotte che: - non siano collegate alla segnalazione; - non siano strettamente necessarie a rivelare la violazione; - configurino un'acquisizione di informazioni o l'accesso a documenti in modo illecito. **Rinunce e transazioni.** Il Decreto vieta, in generale, rinunce e transazioni dei diritti e dei mezzi di tutela dallo stesso previsti, a meno che non avvengano in particolari condizioni. Tale previsione, sottraendo in parte la disponibilità del diritto dalla sfera del beneficiario della tutela, risponde all'esigenza di implementare e rendere effettiva la protezione del *whistleblower*. La norma consente, tuttavia, al segnalante e agli altri soggetti tutelati, di poter rinunciare ai propri diritti e mezzi di tutela o farne oggetto di transazione, solo se ciò avviene nelle sedi protette e, quindi, dinanzi ad un

giudice, a seguito di tentativo obbligatorio di conciliazione, o di accordi di mediazione e conciliazione predisposti in sede sindacale o davanti agli organi di certificazione. **Trattamento dei dati personali.** La ricezione e la gestione delle segnalazioni interne determinano in capo all'ente il trattamento dei dati personali delle persone a vario titolo coinvolte nei fatti segnalati. Pertanto, nella definizione del canale di segnalazione interna, occorre prestare particolare attenzione al rispetto della disciplina sulla protezione dei dati personali (Regolamento UE n. 679/2016, c.d. GDPR, e il D.lgs. n. 196/2003, c.d. Codice *privacy*), affinché i trattamenti conseguenti alla presentazione delle segnalazioni siano effettuati in conformità a tale normativa. **Inquadramento dei trattamenti dipendenti dal ricevimento e della gestione di una segnalazione. Il ricevimento e la gestione delle segnalazioni determinano in capo all'ente un trattamento dei dati personali:** - di natura comune, di natura particolare (ex *"dati sensibili"*) e giudiziari (quali condanne penali e reati), eventualmente contenuti nella segnalazione e negli atti e nei documenti a essa allegati; - relativi a tutte le persone fisiche - identificate o identificabili - a vario titolo coinvolte nelle vicende segnalate (segnalante, segnalato, facilitatore, eventuali altri terzi): c.d. interessati; - necessario per dare attuazione agli obblighi di legge previsti dalla disciplina *whistleblowing,* la cui osservanza è condizione di liceità del trattamento ex art. 6, par. 1, lett. c) e parr. 2 e 3, art. 9, par. 2, lett. b) e artt. 10 e. 88 del GDPR (v. Parere del Garante *privacy*); - realizzato al solo fine di gestire e dare seguito alle segnalazioni (art. 12, co. 1 del Decreto); - che, in ragione della particolare delicatezza delle informazioni potenzialmente trattate, della vulnerabilità degli interessati nel contesto lavorativo, nonché dello specifico regime di riservatezza dell'identità del segnalante previsto dal Decreto, presenta rischi specifici per i diritti e le libertà degli interessati (v. Parere del Garante *privacy*) e, pertanto, deve essere preceduto da una valutazione d'impatto sulla protezione dei dati, c.d. D.P.I.A. (art. 13, co. 6 del Decreto e artt. 35 e 36 del GDPR); - rispetto al quale l'esercizio dei diritti degli interessati (es. accesso, rettifica, aggiornamento, cancellazione, limitazione del trattamento, portabilità, opposizione) può essere limitato qualora dal medesimo possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante (art. 13, co. 3 del Decreto e art. 2-undecies del Codice *privacy*). **Ruoli *privacy* nel canale di segnalazione interna.** Il Decreto individua i ruoli ai fini della normativa *data protection* degli enti che attivano il canale di segnalazione interna e dei soggetti coinvolti nella ricezione e nella gestione delle segnalazioni. Quanto agli enti che attivano il canale interno, essi effettuano i trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni in qualità di titolari del trattamento (art. 13, co. 4 del Decreto). In caso di condivisione di risorse per il ricevimento e la gestione delle segnalazioni, gli enti interessati dalla condivisione trattano i dati in qualità di contitolari del trattamento (art. 13, co. 5 del Decreto). Ai fini del trattamento congiunto, pertanto, i contitolari sono tenuti a stipulare un accordo interno che, in maniera trasparente, disciplini le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dalla normativa *privacy* e rifletta adeguatamente i ruoli e i rapporti con gli interessati. Quando l'ente affida - tutta o in parte - la gestione del canale di segnalazione a un soggetto esterno alla sua organizzazione (es. fornitore della piattaforma), quest'ultimo tratta i dati in qualità di responsabile del trattamento e, in quanto tale, deve presentare garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che garantiscano la protezione dei dati. Ai sensi dell'art. 28 del GDPR, l'esecuzione dei trattamenti da parte dei responsabili del trattamento deve essere disciplinata da un contratto o da altro atto giuridico - tra il titolare/i contitolari e il responsabile stesso -stipulato in forma scritta e recante, le caratteristiche del trattamento affidato al responsabile, gli obblighi e i diritti del titolare del trattamento e le istruzioni per il trattamento dei dati da parte del responsabile. Ad ogni modo, deve essere evitato il tracciamento di qualunque informazione che possa ricondurre all'identità ovvero all'attività del segnalante. **Impostazione ed esecuzione dei trattamenti conseguenti alle segnalazioni.** Ai fini della impostazione dei canali di segnalazione interna, il Decreto, oltre a rinviare al GDPR, ai relativi principi e al Codice *privacy*, detta specifiche garanzie per i trattamenti conseguenti alle segnalazioni. In particolare, il Decreto dà specifica attuazione ai principi di: **Trasparenza** (v. art. 5, par. 1, lett. a) del GDPR prescrivendo ai titolari del trattamento di rendere *ex ante* ai possibili interessati un'idonea informativa sul trattamento dei dati personali (art. 13, co. 4 del Decreto), recante, tra le altre, le informazioni su: i) il titolare del trattamento e i relativi dati di contatto; ii) la finalità del trattamento; iii) la base giuridica del trattamento; iv) le modalità del trattamento; v) l'ambito del trattamento e i soggetti cui sono comunicati i dati (es. responsabili, autorizzati del trattamento); vi) il periodo di conservazione dei dati personali. **Limitazione delle finalità** (v. art. 5, par. 1, lett. b) del GDPR

prevedendo che le segnalazioni non possano essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse (art. 12, co. 1 del Decreto); **Minimizzazione dei dati** (v. art. 5, par. 1, lett. c) del GDPR: prevedendo che i dati manifestamente non utili alla trattazione di una specifica segnalazione non siano raccolti o, in caso di raccolta accidentale, siano prontamente cancellati (art. 13, co. 2 del Decreto). **Limitazione della conservazione** (v. art. 5, par. 1, lett. e) del GDPR prevedendo espressamente che le segnalazioni e la relativa documentazione siano conservate per il tempo necessario alla trattazione della segnalazione e, comunque, non oltre 5 anni dalla comunicazione dell'esito finale della procedura (art. 14, co. 1 del Decreto); **Integrità e riservatezza** (v. art. 5, par. 1, lett. f) del GDPR prevedendo l'individuazione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi del trattamento e promuovendo il ricorso a strumenti di crittografia (art. 4, co. 1 e art. 13, co. 6 del Decreto). Per definire i modelli di ricevimento e gestione delle segnalazioni, rilevano, altresì, i principi di: **privacy by design e privacy by default** (v. art. 25 del GDPR), che impongono di considerare le garanzie di protezione dei dati personali sin dalla progettazione del canale di segnalazione (*privacy by design*) e di assicurare che per impostazione predefinita (*privacy by default*) siano trattati solo i dati personali strettamente necessari in relazione alla specifica segnalazione e che tali dati non siano resi accessibili, in via automatica, a un numero indefinito di soggetti; **riservatezza**, su cui si basa l'intera disciplina *whistleblowing*. A tal fine, le LG prescrivono di garantire il divieto di tracciamento dei canali di segnalazione. **Sistema sanzionatorio.** In tema di regime sanzionatorio, le LG ANAC nell'ottica di individuarne il soggetto destinatario distinguono, per le varie fattispecie, tra persona fisica e giuridica ritenuta responsabile e quindi destinataria della sanzione. In particolare: nelle ipotesi di mancata istituzione del canale, di mancata adozione delle procedure o di adozione di procedure non conformi, il responsabile è individuato nell'organo di indirizzo; ii) nelle ipotesi in cui non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute, nonché quando sia stato violato l'obbligo di riservatezza, il responsabile è il gestore delle segnalazioni. Nel dettaglio, le sanzioni amministrative pecuniarie sono le seguenti: a) da 10.000 a 50.000 euro quando accerta che la persona fisica individuata come responsabile abbia commesso ritorsioni; b) da 10.000 a 50.000 euro quando accerta che la persona fisica individuata come responsabile abbia ostacolato la segnalazione o abbia tentato di ostacolarla; c) da 10.000 a 50.000 euro quando accerta che la persona fisica individuata come responsabile abbia violato l'obbligo di riservatezza di cui all'art. 12 del D.Lgs. n. 24/2023. Restano salve le sanzioni applicabili dal Garante per la protezione dei dati personali per i profili di competenza in base alla disciplina in materia di dati personali; d) da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione: in tal caso, responsabile è considerato l'organo di indirizzo sia negli enti del settore pubblico che in quello privato; e) da 10.000 a 50.000 euro quando accerta che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni, ovvero che l'adozione di tali procedure non è conforme a quanto previsto dal decreto; in tal caso, responsabile è considerato l'organo di indirizzo sia negli enti del settore pubblico che in quello privato; f) da 10.000 a 50.000 euro quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute; in tal caso, responsabile è considerato il gestore delle segnalazioni; g) da 500 a 2.500 euro, quando è accertata, anche con sentenza di primo grado, la responsabilità civile della persona segnalante per diffamazione o calunnia nei casi di dolo o colpa grave, salvo che la medesima sia stata già condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria. Sono inoltre previsti specifici obblighi formativi e informativi. **Segnalazione esterna e divulgazione pubblica.** L'articolo 7 del Decreto attribuisce all'ANAC il compito di istituire un canale di segnalazione accessibile non solo ai soggetti appartenenti al settore pubblico ma anche al settore privato, che sia idoneo ad assicurare, analogamente a quanto previsto per il canale interno, anche tramite strumenti di crittografia, la riservatezza dell'identità del segnalante e di coloro che sono coinvolti nella segnalazione, del contenuto della segnalazione stessa e della relativa documentazione. **Le condizioni per la segnalazione esterna.** Per poter ricorrere al canale di segnalazione istituito dall'ANAC, devono sussistere alcune condizioni, ai sensi dell'art. 6 del Decreto. In particolare, il segnalante può ricorrere alla procedura esterna soltanto se ricorre una delle seguenti condizioni: i) nel suo contesto lavorativo non è prevista l'attivazione del canale interno come obbligatoria o, se prevista, non è stata attivata; ii) la segnalazione non ha avuto seguito; iii) ha fondati motivi di ritenere che se effettuasse la segnalazione interna questa non avrebbe seguito o che andrebbe incontro a ritorsioni; (iv) ha fondati motivi di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse. **La**

presentazione e la gestione delle segnalazioni. In attuazione del potere/dovere a essa attribuito, l'ANAC ha disciplinato, nelle LG e nell'apposito Regolamento, le modalità di presentazione e gestione delle segnalazioni esterne. Con riguardo alle modalità di presentazione, le segnalazioni possono essere effettuate: a) tramite piattaforma informatica, delineata come canale prioritario di segnalazione in quanto ritenuto maggiormente idoneo a garantire la riservatezza del segnalante e della segnalazione. Sempre al fine di garantire la massima riservatezza si prevede, inoltre, la figura del *Custode delle identità*. Quest'ultimo è il soggetto che, su esplicita e motivata richiesta del Dirigente dell'Ufficio *Whistleblowing* interno ad ANAC, consente di accedere all'identità del segnalante, la quale tuttavia non è nota al custode stesso; b) oralmente, attraverso un servizio telefonico con operatore. Quest'ultimo è un componente dell'Ufficio ANAC competente, che acquisisce la segnalazione telefonica e la inserisce sulla piattaforma ANAC unitamente al *file* audio della registrazione; c) tramite incontri diretti fissati entro un termine ragionevole, cui consegue l'inserimento della segnalazione nella piattaforma da parte dell'operatore. Nel Regolamento è precisato che per ricorrere all'incontro diretto è necessaria una richiesta motivata. Si prevede che, per essere ammissibile, nella segnalazione devono essere indicati: - la denominazione e i recapiti del *whistleblower*; - i fatti oggetto di segnalazione e l'Amministrazione o Ente in cui essi sono avvenuti; - l'Amministrazione o l'Ente nel cui contesto lavorativo il *whistleblower* opera e il profilo professionale da quest'ultimo rivestito; - la descrizione sintetica delle modalità con cui il *whistleblower* è venuto a conoscenza dei fatti segnalati. La segnalazione esterna è considerata, inoltre, inammissibile per i seguenti motivi: i) manifesta infondatezza per l'assenza di elementi di fatto riconducibili alle violazioni tipizzate nell'art. 2, comma 1, lett. a), del Decreto; ii) manifesta insussistenza dei presupposti di legge per l'esercizio dei poteri di vigilanza dell'Autorità; iii) manifesta incompetenza dell'Autorità sulle questioni segnalate; iv) accertato contenuto generico della segnalazione esterna, tale cioè da non consentire la comprensione dei fatti, ovvero segnalazione esterna corredata da documentazione non appropriata, inconferente o comunque tale da rendere incomprensibile il contenuto stesso della segnalazione; v) produzione di sola documentazione in assenza della segnalazione esterna; vi) mancanza dei dati che costituiscono elementi essenziali della segnalazione esterna; vii) sussistenza di violazioni di lieve entità. L'Ufficio Istruttore di ANAC può valutare la sussistenza dei requisiti di ammissibilità, prevedendo anche la possibilità di integrazione istruttoria, ove necessario, tramite il canale dedicato. Se le segnalazioni ricevute riguardano, invece, violazioni che non rientrano nella competenza di ANAC, l'Ufficio istruttore deve provvedere a inviare la relativa segnalazione all'autorità amministrativa competente oppure all'Autorità giudiziaria (in caso di illeciti penali o erariali). Di tale trasmissione deve essere informato il segnalante. L'autorità che riceve la segnalazione, a sua volta, sarà tenuta a svolgere l'istruttoria, garantendo la riservatezza circa l'identità del segnalante e degli eventuali soggetti coinvolti. In ogni caso, l'Ufficio entro tre mesi o, se ricorrono giustificate e motivate ragioni, sei mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei sette giorni dal ricevimento, comunica al segnalante: i) l'archiviazione predisposta o che intende predisporre; ii) la trasmissione all'Autorità competente già effettuata o che intende effettuare; iii) l'attività già svolta dall'Ufficio di vigilanza competente interno all'Autorità o l'attività che quest'ultimo intende svolgere. Infine, laddove nei termini di cui al precedente comma l'Ufficio non abbia comunicato la determinazione definitiva sul seguito della segnalazione, ma solo le attività che si intendono intraprendere, lo stesso comunica alla persona segnalante l'esito finale della gestione della segnalazione, che può consistere nell'archiviazione, nelle risultanze istruttorie dell'Ufficio di vigilanza competente o nella trasmissione alle Autorità competenti. **La procedura della divulgazione pubblica.** La normativa introduce anche la possibilità per il segnalante di effettuare una divulgazione pubblica beneficiando della protezione. Si tratta di una novità estremamente delicata per le imprese, in ragione delle potenzialità lesive per l'ente di una denuncia effettuata in assenza di giustificati motivi o di fondati elementi di prova. Gli effetti lesivi possono essere risaltati dalla circostanza che essa può essere effettuata anche attraverso *social network* e i nuovi canali di comunicazione (ad es. *Facebook*, *Twitter*, ecc.), i quali non sono presidiati da discipline specifiche, regole deontologiche e controlli da parte di apposite Autorità di vigilanza. Ciò rende di estrema importanza, da un lato, circoscrivere il più possibile il ricorso a tale istituto, e dall'altro, costruire in modo pienamente efficace e conforme sia alle prescrizioni del Decreto, sia alle Linee Guida ANAC i canali interni di segnalazione. Per ricorrere a tale procedura, occorre che: - si sia previamente utilizzato il canale interno e/o esterno, ma non vi sia stato riscontro o non vi sia stato dato seguito entro i termini previsti dal decreto; - il

segnalante ritenga sussistere fondati motivi di un *"pericolo imminente e palese per il pubblico interesse"*, considerato come una situazione di emergenza o di rischio di danno irreversibile, anche all'incolumità fisica di una o più persone, che richieda che la violazione sia tempestivamente svelata con ampia risonanza per impedirne gli effetti; - il segnalante ritenga sussistere fondati motivi per ritenere che la segnalazione esterna possa comportare un rischio di ritorsione oppure non avere efficace seguito, perché ad esempio potrebbe ricorrere un pericolo di distruzione delle prove o di collusione tra l'Autorità preposta a ricevere la segnalazione e l'autore della violazione.

11 Diffusione e formazione del modello 231

L'Ente al fine di garantire l'attuazione del modello ne promuove la diffusione e la formazione ed esso inerente. A tutti i destinatari va garantita l'effettiva conoscenza anche attraverso differenti modalità tali da garantire l'idoneità dell'informazione, tenuto conto del grado di coinvolgimento nei processi sensibili nonché del rapporto in essere con l'Ente. Per garantire la capillare diffusione del modello saranno indette **riunione informativa su finalità e contenuti del modello, note informative interne da consegnare contestualmente alle buste paga per i dipendenti,affissione in bacheca del codice etico e sistema disciplinare e parti integranti del modello; supporti informatici, pubblicazione sui server e sul sito intranet della società e/o invio della documentazione a mezzo e-mail.** Quanto **alle nuove assunzioni**, all'atto della firma del contratto dovrà essere consegnato un set informativo composto da un estratto del modello e dal Codice Etico in modo da garantire le informazioni di maggior rilievo anche considerata l'aria di rischio in cui sono destinati ad operare. Ai **soggetti terzi** sarà inoltrata in forma scritta o elettronica la comunicazione di adozione del modello e del Codice Etico con l'avvertenza che lo stesso è pubblicato sul sito dell'Ente. In ogni casso, in collaborazione con l'OdV, viene pianificata una politica informativa a cadenza periodica a favore di tutti i destinatari. Per le **funzioni apicali o per le aree sensibili** sono destinate sessioni specifiche di formazione programmate nel corso dell'anno in modo da approfondire i reati specifici anche mediante casi concreti. **La partecipazione ai corsi di formazione è obbligatoria**, l'OdV in collaborazione con i vertici stabilisce la frequenza, garantendo la partecipazione e predisponendo un sistema di registrazione e verifica delle presenze. Al termine della formazione sarà accertata le conoscenze acquisite. Come stabilito dalle linee guida Confindustria, per garantire la partecipazione, la formazione può essere erogata in presenza o con il supporto di piattaforme e- learning. In attuazione del D.Lgs. n. 24/2023 deve essere assicurata con cadenza periodica la formazione e l'informazione al personale dirigente e dipendente in materia di whistleblowing, per comprendere le finalità e le tutele previste, nonché promuovere l'integrità e responsabilità all'interno dell'Ente. **AEGI SRL si impegna a promuovere e assicurare l'informazione e la formazione come indicato,nonché adottare il sistema di whistleblowing adeguato ai principi enunciati nel modello.**

12 Conclusione

Il Modello Organizzativo è stato approvato dall'organo amministrativo ed è stato ratificato con determina dell'Amministratore Unico. È fatto obbligo a chiunque operi o collabori con AEGI SRL di rispettare le norme del Modello Organizzativo, nonché osservare gli obblighi informativi e di formazione, in modo che l'operato di ognuno sia conforme alle prescrizioni imposte.

Copia del Modello Organizzativo e dei documenti ad esso allegati, nonché di revisioni e aggiornamenti successivi saranno depositati presso la sede legale di AEGI SRL e sarà a disposizione per la consultazione.

In ogni caso il Modello di organizzazione e Gestione di AEGI SRL è pubblicato sul sito Internet della Società per consentirne la più ampia diffusione ed immediatezza della conoscenza.

FIRME E APPROVAZIONI

REDATTO DA	VERIFICATO DA	APPROVATO DA
Nominativo: _____ Data: _____ _____ Firma grafica / firma elettronica OTP (funzione predisposta, non ancora attiva)	Nominativo: _____ Data: _____ _____ Firma grafica / firma elettronica OTP (funzione predisposta, non ancora attiva)	Nominativo: _____ Data: _____ _____ Firma grafica / firma elettronica OTP (funzione predisposta, non ancora attiva)

Rif. SGI: MOG231 §ART.6 · MAN-231-001 – Modello 231 - Parte generale