MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI TECHBAU S.P.A.

ai sensi e in conformità alle disposizioni di cui a D. Lgs. 231/2001

PARTE GENERALE

Revisione n. 3 approvata il 26/09/2025

STORICO DELLE REVISIONI				
REV.	**DATA**	**DESCRIZIONE DELLE MODIFICHE**	**PREPARATO**	**CONTROLLATO E APPROVATO**
03	26/09/2025	Aggiornamento	Studio Legale Associato Giannangeli Consulich	Consiglio di Amministrazione di Techbau S.p.A.
02	15/12/2023	Aggiornamento	Studio Legale Associato Giannangeli Consulich	Consiglio di Amministrazione di Techbau S.p.A.
01	12/10/2022	Prima emissione	Studio Legale	Consiglio di Amministrazione di Techbau S.p.A.

INDICE

1. DEFINIZIONI 5

2. NORMATIVA DI RIFERIMENTO 7

2.1. Premesse ... 7

2.2. Sanzioni applicabili all'ente ... 9

2.3. Reati Presupposto ... 11

2.4. Forme di esenzione da responsabilità ... 19

2.5. Linee guida di Confindustria ... 21

3. MODELLO DI GOVERNANCE 24

3.1. Sistema di corporate governance di Techbau S.p.A. ... 24

3.2. Il Codice Etico e di comportamento ... 27

3.3. Protocolli relativi alle modalità di gestione delle risorse finanziarie ... 28

4. IL MODELLO ADOTTATO DA TECHBAU S.P.A. 30

4.1. Finalità del Modello ... 30

4.2. Rischio accettabile ... 30

4.3. Il Modello (struttura, destinatari e ambito di applicazione) ... 30

4.4. Approvazione del Modello ... 32

4.5. Aggiornamento e attuazione del Modello ... 32

4.6. Modello e Codice Etico ... 32

4.7. Adozione del Modello nell'ambito del Gruppo ... 33

5. L'ORGANISMO DI VIGILANZA (OdV) 35

5.1. Composizione ... 35

5.2. Revoca e sostituzione ... 36

5.3. Requisiti ... 37

5.4. Funzioni e poteri ... 38

5.5. Flussi informativi da parte dell'OdV ... 40

5.6. Flussi informativi nei confronti dell'OdV ... 40

5.7. Coordinamento tra gli OdV delle società del Gruppo ... 41

6. SEGNALAZIONI WHISTLEBLOWING 42

6.1. Premessa ... 42

6.2. Ambito di applicazione ... 44

6.3. Canale di segnalazione interna ... 46

6.4. Canale di segnalazione esterna ... 52

6.5. Divulgazione pubblica ... 54

6.6. Tutela della riservatezza e protezione dei dati personali ... 55

6.7. Divieto di ritorsione ... 57

6.8. Limitazioni di responsabilità ... 59

6.9. Sistema sanzionatorio 60
7. SELEZIONE, INFORMAZIONE E FORMAZIONE DEL PERSONALE 61
7.1. Selezione del personale 61
7.2. Informazione del personale 61
7.3. Formazione del personale 62
8. SISTEMA DISCIPLINARE 63
8.1. Principi generali 63
8.2. Sanzioni nei confronti dei dipendenti e dei dirigenti 63
8.3. Misure nei confronti dei collaboratori, fornitori, partner commerciali e consulenti 66
8.4. Misure nei confronti degli Amministratori, del Collegio Sindacale e dei Revisori 66

1. DEFINIZIONI

ANAC	Autorità Nazionale Anti-Corruzione
Archivio 231	indica l'archivio istituito presso la sede, che raccoglie tutta la documentazione relativa all'adozione e all'implementazione del Modello;
Autori	indica i soggetti, esterni alla Società, cui Techbau affida la realizzazione di tutto o parte di un progetto editoriale, con cui i rapporti sono regolati da appositi contratti di edizione;
Attività	indica l'attività svolta dall'impresa;
Codice Etico	indica il codice etico adottato dall'impresa;
Concessionari	indica i soggetti cui Techbau affida l'acquisto, la propaganda e la successiva vendita di quanto realizzato, e che agiscono in nome e per conto proprio;
Consulenti	i soggetti che intrattengono con la Società rapporti contrattuali aventi ad oggetto la prestazione di servizi di natura consulenziale
Decreto	indica il D.lgs. 8 giugno 2001 n. 231 e le sue successive modifiche ed integrazioni;
Destinatari	indica tutti i soggetti tenuti al rispetto delle prescrizioni contenute nel Modello, in particolare: tutti coloro che operano in nome e per conto di Techbau, inclusi i procuratori, i sindaci, i membri degli altri eventuali organi sociali, i dipendenti, i collaboratori anche occasionali;
Divulgazione Pubblica	l'atto di rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone
Enti o Ente	ai sensi dell'art. 1 del Decreto, indica gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica cui si applicano le disposizioni del Decreto ed in particolare la responsabilità amministrativa dallo stesso introdotta;
Facilitatore	la persona fisica che assiste una Persona Segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata
Fornitori	i soggetti, sia pubblici che privati, che intrattengono con la Società rapporti contrattuali aventi ad oggetto la fornitura di beni o la prestazione di servizi
GDPR	il regolamento (UE) 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
Modello	indica il Modello di organizzazione, gestione e controllo previsto dal D.lgs. 231/2001;

Organismo di Vigilanza	l'organismo di vigilanza istituito dalla Società ai sensi del D.lgs. 231/2001
Piattaforma	l'applicativo *web based* impiegato dalla Società per la ricezione e la gestione di Segnalazioni Interne
Persona Coinvolta	la persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente
Responsabile Whistleblowing	La persona o organismo a cui è delegata la gestione delle segnalazioni, che attualmente si identifica con il Presidente dell'Organismo di vigilanza
Segnalante	la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo
Segnalazione	la comunicazione, scritta o orale, di informazioni riguardanti Violazioni commesse o che potrebbero essere commesse nell'organizzazione con cui la Persona Segnalante intrattiene un rapporto giuridico
Società	Techbau s.p.a.
Testo Unico Sicurezza	indica il D.lgs. 9 aprile 2008 n. 81. c.d. Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro e successive modifiche, incluso in particolare il D.lgs. 3 agosto 2009 n. 106 e le successive modifiche agli stessi;
Testo Unico Ambientale	indica il D.lgs. 3 aprile 2006 n. 152. c.d. Testo Unico in materia di sicurezza ambientale e successive modifiche, inclusi il D.lgs. 4 marzo 2014 n. 46, Legge 11 agosto 2014 n. 116 e le successive modifiche agli stessi, la LEGGE 68 del 22/05/2015 relativa ai cosiddetti "ecoreati".
TUF	indica il D.lgs. 24 febbraio 1998 n. 58, Testo Unico in materia di intermediazione finanziaria.

2. NORMATIVA DI RIFERIMENTO

2.1. Premesse

Il Decreto Legislativo 8 giugno 2001 n. 231 (di seguito anche il "**Decreto**" o "**D.Lgs. 231/2001**"), recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e di altre strutture associative, anche prive di personalità giuridica (i c.d. "Enti"), a norma dell'art. 11 della Legge 29 settembre 2000, n. 300", ha introdotto per la prima volta in Italia una responsabilità amministrativa da reato a carico degli Enti, che si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto illecito, ciò anche al fine di adeguare la normativa interna in materia di responsabilità delle persone giuridiche ad alcune convenzioni internazionali cui l'Italia aveva già da tempo aderito[1].

Si tratta di una nuova e più estesa forma di responsabilità amministrativa (assimilabile sostanzialmente alla responsabilità penale), che colpisce gli enti (da intendersi come società, associazioni, consorzi, ecc.) per i reati commessi, nel loro interesse o vantaggio, da soggetti ad essi funzionalmente legati (soggetti in posizione apicale e soggetti sottoposti alla direzione e vigilanza di questi ultimi)[2].

Il Decreto prevede che gli enti possano essere ritenuti responsabili, e conseguentemente sanzionati, a fronte del compimento di taluni reati (cd. "**Reati Presupposto**") indicati tassativamente dalla legge e contenuti in un'elencazione che è suscettibile di modifiche ed integrazioni da parte del legislatore.

Il primo criterio fondamentale d'imputazione consiste nel fatto che il reato sia stato commesso nell'interesse o a vantaggio dell'ente (cd. **criterio oggettivo**): ciò significa che la responsabilità dell'ente sorge qualora il fatto sia stato commesso per favorire l'ente, senza che sia necessario il conseguimento effettivo e concreto del risultato.

Il vantaggio costituisce una "*concreta acquisizione di un'utilità economica*", mentre "*l'«interesse» implica solo la finalizzazione del reato a quella utilità, senza peraltro richiedere che questa venga effettivamente conseguita*"[3].

L'ente non è quindi responsabile se l'illecito è stato commesso da uno dei soggetti sopra indicati nell'interesse esclusivo proprio o di terzi; e infatti, l'interesse esclusivo dell'agente o del terzo non determina alcuna responsabilità in capo all'ente, in quanto si verifica un'interruzione nello schema di immedesimazione organica, trattandosi di una situazione di manifesta estraneità della persona giuridica rispetto al fatto di reato.

[1] La Convenzione sulla tutela degli interessi finanziari delle Comunità europee, sottoscritta a Bruxelles il 26 luglio 1995 e del suo primo protocollo ratificato a Dublino il 27 settembre 1996; il protocollo concernente l'interpretazione in via pregiudiziale da parte della Corte di giustizia delle Comunità europee di detta Convenzione, sottoscritto a Bruxelles il 29 novembre 1996; la Convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee, ratificata a Bruxelles il 26 maggio 1997; la Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali, con annesso, ratificata a Parigi il 17 dicembre 1997.

[2] Cfr. art. 5 del Decreto.

[3] Ordinanza Trib. Milano, Sezione XI riesame, 20/12/04.

Il secondo fondamentale criterio di imputazione consiste invece nel fatto che il reato sia stato commesso da parte di una persona fisica legata da un rapporto funzionale con l'ente stesso (cd. **criterio soggettivo**). In particolare, il reato deve essere stato commesso da:

- persone "*che rivestono funzioni di rappresentanza, amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché di persone che esercitano anche di fatto, la gestione e il controllo dello stesso*" (c.d. "**soggetti in posizione apicale**" o "**Soggetti Apicali**", quali, ad esempio, il legale rappresentante, l'amministratore, il direttore generale o le persone che esercitano, anche di fatto, la gestione o il controllo dell'ente);

- "*persone sottoposte alla direzione o alla vigilanza di uno dei soggetti*" apicali (c.d. "**soggetti in posizione subordinata**" o "**Soggetti Sottoposti**", ossia soggetti subalterni, tipicamente lavoratori dipendenti, ma anche soggetti esterni all'ente, ai quali sia stato affidato un incarico da svolgere sotto la direzione e la sorveglianza dei soggetti apicali).

L'appartenenza dell'autore del reato a una o all'altra categoria è determinante ai fini della scelta dei criteri soggettivi di imputazione applicabili al caso concreto che, in relazione alla diversa posizione nell'organizzazione dell'ente, sono necessariamente diversificati (cfr. artt. 6 e 7 del Decreto).

Se il reato è stato commesso da un soggetto in posizione apicale, la responsabilità dell'ente va ricollegata al fatto che "*il vertice esprime e rappresenta la politica dell'ente*"[4], per questo l'ente si identifica nella persona fisica che ha agito a suo vantaggio o nel suo interesse.

Se, invece, il reato è stato commesso da un soggetto in posizione subordinata, la responsabilità dell'ente è collegata all'inosservanza, da parte dello stesso, degli obblighi di direzione o vigilanza, e il reato dipende dall'esistenza di gravi carenze organizzative per le quali si può muovere un rimprovero (cfr. art. 7 del Decreto). L'imputabilità del reato all'ente presuppone comunque la sussistenza (e quindi la prova) del nesso eziologico fra l'inosservanza degli obblighi di direzione e vigilanza e la condotta delittuosa del soggetto sottoposto, tale per cui sia possibile ravvisare nei confronti dell'ente la cd. **colpa di organizzazione**.

La responsabilità dell'ente è agganciata a quella dell'autore materiale dell'illecito, ma è altresì diretta e autonoma e prescinde dall'accertamento della responsabilità di una persona fisica (cfr. art. 8 del Decreto).
La giurisdizione italiana sussiste quando l'azione o l'omissione che costituisce il reato sia avvenuta sul territorio dello Stato italiano, o comunque si sia verificato in Italia l'evento che di tale azione od omissione sia la conseguenza (art. 6 co. 2 c.p.).

[4] Così la Relazione di accompagnamento al Decreto.

Gli enti aventi nel territorio dello Stato la loro sede principale (per la cui individuazione è necessario rifarsi alle norme civilistiche previste per le persone giuridiche e le imprese) rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui il reato è stato commesso.

2.2. Sanzioni applicabili all'ente

Il sistema sanzionatorio delineato dal Decreto è basato su un doppio binario: da una parte la sanzione pecuniaria e dall'altra quella interdittiva.

La **sanzione principale** e indefettibile è quella **pecuniaria**, comminata con il sistema delle quote: per ogni reato è previsto un numero minimo e uno massimo di quote, non inferiore a 100 e non superiore a 1.000, e ciascuna quota corrisponde a una somma di denaro che va da euro 258,00 a euro 1.549,37. Il giudice fissa il numero delle quote sulla base della gravità del fatto e del grado di responsabilità dell'ente, nonché dell'attività svolta dall'ente per eliminare o attenuare le conseguenze del fatto illecito e per prevenire la commissione di ulteriori illeciti. L'importo di ogni quota è invece fissato dal giudice tenendo in considerazione le condizioni economiche e patrimoniali dell'ente. L'ammontare della sanzione pecuniaria, pertanto, viene determinata per effetto della moltiplicazione del primo fattore (numero di quote) per il secondo (importo della quota).
In concreto, dunque, le sanzioni pecuniarie potranno oscillare tra un minimo di euro 25.822,84 (riducibili, ai sensi dell'art. 12 del Decreto, sino alla metà) ed un massimo di euro 1.549.370,69.

La sanzione pecuniaria ha natura amministrativa e si applica sempre, anche qualora l'ente abbia riparato le conseguenze giuridiche derivanti dal reato.

La sanzione pecuniaria è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado:

- l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato, ovvero si è comunque efficacemente adoperato in tal senso;
- è stato adottato o reso operativo un Modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

È, inoltre, prevista la riduzione della metà della sanzione pecuniaria se:

- l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;
- il danno patrimoniale cagionato è di particolare tenuità.

Le **sanzioni interdittive**, invece, si applicano solo per quei reati per i quali sono espressamente previste e sono:

- l'interdizione dall'esercizio dell'attività.
- la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

- il divieto di contrattare con la Pubblica Amministrazione, salvo che per l'ottenimento di un servizio pubblico (tale divieto può essere limitato anche a determinati tipi di contratto o a determinate amministrazioni);
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
- il divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive hanno la caratteristica di limitare o condizionare l'attività sociale, e nei casi più gravi arrivano a paralizzare l'ente (interdizione dall'esercizio dell'attività) e possono essere applicate anche come strumenti cautelari prima della condanna (quando sussistono gravi indizi per ritenere la sussistenza della responsabilità dell'ente per un illecito amministrativo dipendente da reato e vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per il quale si procede).

Le sanzioni interdittive si applicano nei casi espressamente previsti dal Decreto quando ricorre almeno una delle seguenti condizioni:

- l'ente ha tratto dal reato un profitto di rilevante entità e il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione e, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
- in caso di reiterazione degli illeciti.

Le sanzioni interdittive hanno una durata non inferiore a tre mesi e non superiore a due anni e possono essere applicate in via definitiva nelle situazioni più gravi descritte nell'art. 16 del Decreto (se l'ente è utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati oppure quando l'ente è già stato condannato almeno tre volte negli ultimi sette anni).

Si segnala, inoltre, la possibile prosecuzione dell'attività dell'ente (in luogo dell'irrogazione della sanzione) da parte di un commissario nominato dal giudice ai sensi dell'art. 15 del D.Lgs. 231/2001, quando ricorre una delle seguenti condizioni:

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

Accanto a queste sanzioni ci sono altre due sanzioni:

- la **confisca**, che viene sempre applicata in caso di condanna e ha ad oggetto il prezzo o il profitto del reato (salvo per la parte che può essere restituita al danneggiato), ovvero, se ciò non è possibile, somme di denaro o altre utilità di valore equivalente al prezzo o al profitto del reato; sono fatti salvi i diritti acquisiti dal terzo in buona fede. Lo scopo è quello di impedire che l'ente sfrutti comportamenti illeciti ai fini di "lucro". L'art. 53 del Decreto prevede la possibilità di disporre il sequestro preventivo finalizzato alla confisca;

- la **pubblicazione della sentenza**, che può essere disposta quando all'ente viene applicata una sanzione interdittiva; la sentenza è pubblicata per una sola volta, per estratto o per intero, in uno o più giornali scelti dal giudice, e mediante affissione all'albo del comune dove l'ente ha sede. La pubblicazione è a spese dell'ente, ed è eseguita dalla cancelleria del giudice; lo scopo è di portare a conoscenza del pubblico la sentenza di condanna.

2.3. Reati Presupposto

La responsabilità dell'ente può emergere solo dalla commissione dei reati espressamente indicati nel Decreto. L'elenco dei reati è stato via via ampliato da quando il Decreto è entrato in vigore, e ora ricomprende fattispecie assai eterogenee tra loro.

Nello specifico, i reati a cui si applica la disciplina sono i seguenti:

1. **Reati commessi nei rapporti con la pubblica amministrazione e contro il patrimonio dello Stato o di altro ente pubblico (artt. 24 e 25 del Decreto):**
   - malversazione di erogazioni pubbliche (art. 316 *bis* c.p.);
   - indebita percezione di erogazioni pubbliche (art. 316 *ter* c.p.);
   - corruzione (artt. 318, 319, 320, 321 e 322 *bis* c.p.);
   - corruzione in atti giudiziari (art. 319 *ter* c.p.);
   - induzione indebita a dare o promettere utilità (art. 319 *quater* c.p.);
   - istigazione alla corruzione (art. 322 c.p.);
   - truffa in danno dello Stato o di un ente pubblico (art. 640 comma 2 n. 1 c.p.);
   - truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 *bis* c.p.);
   - frode informatica a danno dello Stato o di altro ente pubblico (art. 640 *ter* c.p.);
   - traffico di influenze illecite (art. 346 *bis* c.p.);
   - concussione (art. 317 c.p.);
   - frode nelle pubbliche forniture (art. 356 c.p.);
   - frode ai danni del Fondo agricolo europeo (art. 2 della Legge 898/1986);
   - peculato (art. 314 c.p.), se il fatto offende gli interessi finanziari dell'Unione Europea;
   - indebita destinazione di denaro o cose mobili (art. 314 *bis* c.p.);
   - peculato mediante profitto dell'errore altrui (art. 316 c.p.), se il fatto offende gli interessi finanziari dell'Unione Europea;
   - turbata libertà degli incanti (art. 353 c.p.);
   - turbata libertà del procedimento di scelta del contraente (art. 353 *bis* c.p.).

2. **Delitti informatici e trattamento illecito di dati (art. 24 *bis* del Decreto):**
   - falsità in documenti informatici pubblici o aventi efficacia probatoria (art. 491 *bis* c.p.);
   - accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.);
   - detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 *quater* c.p.);

- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 *ter* c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 *quinquies* c.p.);
- omessa comunicazione o comunicazione non veritiera di informazioni, dati, elementi di fatto rilevanti in materia di perimetro di sicurezza cibernetica nazionale (art. 1, comma 11, D. L. n. 105/2019);
- estorsione commessa mediante le condotte di cui agli artt. 615 *ter*, 617 *quater*, 617 *sexies*, 635 *bis,* 635 *quater* e 635 *quinqiues* ovvero con la minaccia di compiere (art. 629, co. 3 c.p.);
- detenzione, diffusione e installazione abusive di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635 *quater*.1 c.p.).

3. Delitti di criminalità organizzata (art. 24 *ter* del Decreto):

- associazione per delinquere (art. 416 c.p.);
- associazioni di tipo mafioso, anche straniere (art. 416 *bis* c.p.);
- scambio elettorale politico-mafioso (art. 416 *ter* c.p.);
- sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.);
- associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del DPR 309/09);
- 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 armi più comuni da sparo (art. 407 comma 2, lettera a, numero 5 c.p.).

4. Reati in materia di falsità in monete, in carte di pubblico credito e in valori di bollo (art. 25 *bis* del Decreto):

- 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 di monete falsificate ricevute in buona fede (art. 457 c.p.);
- spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 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 commi 1 e 2 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.).

5. **Delitti contro l'industria e il commercio (art. 25 *bis*.1 del Decreto):**
   - 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 internazionali (art. 514 c.p.);
   - frode nell'esercizio del commercio (art. 515 c.p.);
   - vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
   - vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
   - fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 *ter* c.p.);
   - contraffazione di indicazioni geografiche o denominazione di origine dei prodotti agroalimentari (art. 517 *quater* c.p.).

6. **Reati societari (art. 25 *ter* del Decreto):**
   - false comunicazioni sociali (art. 2621 e 2621 *bis* c.c.);
   - false comunicazioni sociali delle società quotate (art. 2622 c.c.);
   - impedito controllo (art. 2625 comma 2 c.c.);
   - indebita restituzione dei 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 di interessi (art. 2629 *bis* c.c.);
   - 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.);
   - istigazione alla corruzione tra privati (art. 2635 *bis* 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 commi 1 e 2 c.c.);
   - false o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54, D.Lgs. 19/2023).

L'art. 25 ter del D.Lgs. 231/2001 – alle lettere d) ed e) – prevede la responsabilità dell'ente per il reato di falso in prospetto, continuando però a richiamare la contravvenzione di cui all'art. 2623 c.c., comma 1 (art. 25 *ter*, lett. d) ed il

delitto di cui all'art. 2623, comma 2 c.c. (art. 25 *ter*, lett. e), oggi abrogati. Prudenzialmente riteniamo opportuno integrare il Modello come se tale rinvio non fosse soltanto formale, ossia rivolto al reato di falso in prospetto così come concepito – inizialmente – nell'art. 2623 c.c., bensì concernente anche le successive modifiche della disciplina sanzionatoria dell'illecito in questione, ora diversamente disciplinato dall'art. 173 bis T.U.F. (D.Lgs. 58/1998).

Inoltre, in virtù delle novelle legislative introdotte con il D.Lgs. 39/2010:

- l'art. 2624 c.c. falsità nelle relazioni o nelle comunicazioni delle società di revisione è stato abrogato;
- l'art. 2625, comma 1 c.c. è stato così modificato:
  1. le parole: «o di revisione» sono soppresse;
  2. le parole: «ad altri organi sociali o alle società di revisione» sono sostituite dalle seguenti: «o ad altri organi sociali»;
- sono stati inseriti i nuovi reati di "falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale" (art. 27 D.Lgs. 39/2010) e di "impedito controllo" (art. 29 del medesimo decreto).

Stante la finalità preventiva degli illeciti penali del presente modello, in via prudenziale – e per le stesse ragioni esposte poco sopra per l'abrogato art. 2623 c.c. – è opportuno integrare il modello come se la responsabilità amministrativa dell'ente sussistesse anche per il compimento dei nuovi reati e delle fattispecie così come oggi riformulate.

7. Reati commessi con finalità di terrorismo o di eversione dall'ordine democratico (art. 25 *quater* del Decreto):

- 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.);
- addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 *quinquies* c.p.);
- organizzazione di trasferimenti per finalità di terrorismo anche internazionale (art. 270 *quater.1* 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.);
- 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.);
- sequestro di persona a scopo di terrorismo o di eversione (art. 289 *bis* 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.);
- impossessamento, dirottamento e distruzione di un aereo (art. 1 della L. n. 342/1976);

- danneggiamento delle installazioni a terra (art. 2 della L. n. 342/1976).

8. **Pratiche di mutilazione degli organi genitali femminili** (art. 583 *bis* c.p.) **(art. 25 *quater*.1 del Decreto).**

9. **Reati contro la personalità individuale (art. 25 *quinquies* del Decreto):**
   - riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
   - prostituzione minorile (art. 600 *bis* commi 1 e 2 c.p.);
   - pornografia minorile (art. 600 *ter* c.p.);
   - detenzione di materiale pornografico (art. 600 *quater* c.p.), anche qualora si tratti di materiale di pornografia virtuale (art. 600 *quater.1* c.p.);
   - iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 *quinquies* c.p.);
   - tratta di persone (art. 601 c.p.);
   - 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.).

10. **Reati di abuso di informazioni privilegiate e di manipolazione di mercato (art. 25 *sexies* del Decreto):**
    - abuso di informazioni privilegiate (art. 184 T.U.F.);
    - manipolazione del mercato (art. 185 T.U.F.).

L'ente è altresì chiamato a rispondere delle sanzioni amministrative previste dagli articoli 187 *bis* e *187* ter del T.U.F., che puniscono i fatti di abuso di informazioni privilegiate e manipolazione del mercato, salve le sanzioni penali quando il fatto costituisce reato. In questo caso, ai sensi dell'art. 187 *quinquies* l'ente risponde per gli illeciti amministrativi commessi nel suo interesse o a suo vantaggio.

11. **Reati di omicidio e lesioni colpose commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (art. 25 *septies* del Decreto):**
    - omicidio colposo (art. 589 c.p.);
    - lesioni personali colpose, gravi o gravissime (art. 590, comma 3, c.p.), qualora il reato sia stato commesso con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

12. **Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio (art. 25 *octies* del Decreto):**
    - ricettazione (art. 648 c.p.);
    - riciclaggio (art. 648 *bis* c.p.);
    - impiego di denaro, beni o utilità di provenienza illecita (art. 648 *ter* c.p.);
    - autoriciclaggio (art. 648 *ter.1* c.p.).

13. **Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25 *octies*.1 del Decreto):**
    - indebito utilizzo e falsificazione di carte di credito e di pagamento (art. 493 *ter* c.p.);
    - 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.);
    - frode informatica nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale(art. 640 *ter* c.p.);
    - trasferimento fraudolento di valori (art. 512 *bis* c.p.).

14. **Delitti in materia di violazione del diritto di autore (art. 25 *novies* del Decreto):**
    - duplicazione, fabbricazione, vendita, noleggio, introduzione nel territorio dello Stato di programmi informatici, contenuti di banche dati, opere di ingegno (musicali, libri, pubblicazioni, ecc.) (artt. 171, 171 *bis*, 171 *ter*, 171 *septies*, 171 *octies* della L. n. 633/1941).

15. **Induzione a non rendere o a rendere dichiarazioni mendaci all'autorità giudiziaria** (art. 377 bis c.p.) **(art. 25 *decies* del Decreto).**

16. **Reati ambientali (art. 25 *undecies* del Decreto):**
    - inquinamento ambientale (art. 452 *bis* c.p.);
    - disastro ambientale (art. 452 *quater* c.p.);
    - inquinamento ambientale e disastro ambientale colposo (art. 452 *quinquies* c.p.);
    - traffico e abbandono di materiale ad alta radioattività (art. 452 *sexies* c.p.);
    - associazione per delinquere e associazione di tipo mafioso aggravata dalla finalità di commettere delitti ambientali (art. 452 *octies* c.p.);
    - attività organizzate per il traffico illecito di rifiuti (art. 452-*quaterdecies* c.p.);
    - 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.);
    - scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi o aeromobili (art. 137 del D.Lgs. 152/2006);
    - abbandono di rifiuti in casi particolari (art. 255-*bis* del D.Lgs. n.152/2006);
    - abbandono di rifiuti pericolosi (art. 255-*ter* del D.Lgs. n.152/2006);
    - attività di gestione di rifiuti non autorizzata (art. 256 del D.Lgs. 152/2006);
    - combustione illecita di rifiuti (art. 256-*bis* del D.Lgs. n.152/2006);
    - inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (art. 257 del D.Lgs. 152/2006);
    - violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 del D.Lgs. 152/2006);

- traffico illecito di rifiuti (art. 259 del D.Lgs. 152/2006);
- aggravante dell'attività d'impresa (art. 259-*bis* del 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* del D.Lgs. 152/2006);
- superamento dei valori limite di emissione e di qualità dell'aria (art. 279 comma 5 del D.Lgs. 152/2006);
- violazione delle misure a tutela dell'ozono stratosferico e dell'ambiente (art. 3 comma 6 della L. 549/1993);
- 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, art. 2, art. 3-bis e art. 6 della l. n.150/1992);
- inquinamento doloso o colposo di nave (artt. 8 e 9 del D.Lgs. 202/2007).

17. Reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25 *duodecies* del Decreto).

- Si tratta del reato di cui all'art. 22, comma 12 *bis* del D.Lgs. 25 luglio 1998 n. 286 che disciplina il "Lavoro subordinato a tempo determinato e indeterminato" dei cittadini extracomunitari.

18. Razzismo e xenofobia (art. 25 *terdecies* del Decreto):

- Propaganda, istigazione e incitamento, fondate in tutto o in parte sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra (art. 3 della L. 13 ottobre 1975, n. 654).

19. Frodi in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 *quaterdecies* del Decreto):

- frode in manifestazioni sportive (art. 1 della L. 13 dicembre 1989 n. 401);
- esercizio abusivo di attività di giuoco o di scommessa (art. 4 della L. 13 dicembre 1989 n. 401).

20. Reati "transnazionali" (art. 10 Legge 146/2006).

L'art. 10 della L. 16 marzo 2006 n. 146 prevede la responsabilità amministrativa dell'ente, limitatamente al caso in cui il abbiano natura "transnazionale"[5] ai sensi dell'art. 3 della medesima legge, per i delitti di:

- associazione per delinquere (art. 416 c.p.);
- associazione di tipo mafioso anche straniere (art. 416 *bis* c.p.);
- associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291 *quater* del D.P.R. 23 gennaio 1973 n. 43);

[5] Si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché: a) sia commesso in più di uno Stato; b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

- associazione finalizzata al traffico illecito di sostanze stupefacenti (art. 74 del D.P.R. 9 ottobre 1990 n. 309);
- atti diretti a procurare l'ingresso illegale dello straniero nel territorio nazionale e favoreggiamento della sua permanenza al fine di trarvi ingiusto profitto (art. 12 commi 3, 3 *bis*, 3 *ter* e 5 del D.Lgs. 25 luglio 1998 n. 286);
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 *bis* c.p.);
- favoreggiamento personale (art. 378 c.p.).

21. Reati tributari (art. 25 *quinquiesdecies* del Decreto):

- dichiarazione fraudolenta mediante l'uso di fatture o altri documenti per operazioni inesistenti (art. 2 comma 1 del D.Lgs. 74/2000);
- dichiarazione fraudolenta mediante l'uso di fatture o altri documenti per operazioni inesistenti, quando l'ammontare degli elementi passivi fittizi è inferiore ad euro 100.000,00 (art. 2 comma 2 *bis* del D.Lgs. 74/2000);
- dichiarazione fraudolenta mediante altri artifici (art. 3 del D.Lgs. 74/2000);
- emissione di fatture o altri documenti per operazioni inesistenti (art. 8 comma 1 del D.Lgs. 74/2000);
- emissione di fatture o altri documenti per operazioni inesistenti, se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo di imposta, è inferiore ad euro 100.000,00 (art. 8 comma 2 *bis* del D.Lgs. 74/2000);
- occultamento o distruzione di documenti contabili (art. 10 del D.Lgs. 74/2000);
- sottrazione fraudolenta al pagamento di imposte (art. 11 del D.Lgs. 74/2000);
- dichiarazione infedele (art. 4 del D.Lgs. 74/2000), se commessa nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'IVA per un importo complessivo non inferiore a 10.000.000 di euro;
- omessa dichiarazione (art. 5 del D.Lgs. 74/2000), se commessa nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'IVA per un importo complessivo non inferiore a 10.000.000 di euro;
- indebita compensazione (art. 10 *quater* del D.Lgs. 74/2000), se commessa nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'IVA per un importo complessivo non inferiore a 10.000.000 di euro.

22. Reati di contrabbando (art. 25 *sexiesdecies* del Decreto): fattispecie previste dal D.Lgs. n. 141/2024.

23. Delitti contro il patrimonio culturale (art. 25 *septiesdecies* del Decreto):

- furto di beni culturali (art. 518 *bis* c.p.);
- appropriazione indebita di beni culturali (art. 518 *ter* c.p.);
- ricettazione di beni culturali (art. 518 *quater* c.p.);
- falsificazione in scrittura privata relativa a beni culturali (art. 518 *octies* c.p.);
- violazioni in materia di alienazione di beni culturali (art. 518-novies 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.).

24. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25 *duodevicies* del Decreto):

- riciclaggio di beni culturali (art. 518 *sexies* c.p.);
- devastazione e saccheggio di beni culturali e paesaggistici (art. 518 *terdecies* c.p.).

25. Delitti contro gli animali (Art. 25-undevicies del Decreto):

- Uccisione o danneggiamento di animali altrui (art. 638 c.p.);
- Divieto di combattimenti tra animali (art. 544-quinquies c.p.);
- Spettacoli o manifestazioni vietati (art. 544-quater c.p.);
- Maltrattamento di animali (art. 544-ter c.p.);
- Uccisione di animali (art. 544-bis c.p.).

26. Commissione, nelle forme del tentativo, di uno dei delitti indicati (art. 26 del Decreto).

27. Reati commessi all'estero.

A norma dell'art. 4 del D.Lgs. 231/2001, l'ente può essere chiamato a rispondere in Italia in relazione a reati (contemplati dallo stesso D.Lgs. 231/2001) commessi all'estero.

I presupposti su cui si fonda la responsabilità dell'ente per reati commessi all'estero sono:

- il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'ente, ai sensi dell'art. 5 comma 1 del D.Lgs. 231/2001;
- l'ente deve avere la propria sede principale nel territorio dello Stato italiano;
- l'ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p.;
- l'ente può rispondere nei casi in cui nei suoi confronti non proceda lo Stato nel quale è stato commesso il fatto;
- nei casi in cui la legge prevede che il colpevole sia punito a richiesta del Ministro della Giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti dell'ente stesso.

2.4. Forme di esenzione da responsabilità

Il Decreto, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede una forma specifica di esonero da detta responsabilità qualora l'ente dimostri di aver adottato tutte le misure organizzative opportune e necessarie al

fine di prevenire la commissione di reati da parte di soggetti che operino per suo conto. La presenza di un'adeguata organizzazione è, dunque, misura e segno della diligenza dell'ente nello svolgere le proprie attività, con particolare riferimento a quelle in cui si manifesta il rischio di commissione dei reati previsti dal Decreto: l'accertata esistenza di un'efficiente ed efficace organizzazione esclude, dunque, la "colpa" dell'ente ed esclude l'applicazione delle relative sanzioni.

Nello specifico, al Consiglio di Amministrazione compete l'adozione e l'efficace attuazione del Modello di organizzazione, gestione e controllo, ai sensi dell'art. 6, comma 1, lett. a), nonché la nomina dei membri dell'Organismo di Vigilanza, ai sensi della successiva lett. b).

E infatti, l'ente va esente da pena se prova:

- di aver adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione e di gestione dei rischi-reato idoneo a prevenire i reati della specie di quello verificatosi in concreto (di seguito il "**Modello**" o "**MOG**");
- di aver affidato la vigilanza sul funzionamento e sull'osservanza del Modello, nonché il compito di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (di seguito l'"**Organismo di Vigilanza**" o "**OdV**");
- che le persone che hanno commesso il reato l'abbiano fatto eludendo fraudolentemente il Modello;
- che non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

La responsabilità dell'ente è presunta qualora l'illecito sia commesso da una persona fisica che ricopre posizioni di vertice o responsabilità; ricade di conseguenza sull'ente l'onere di dimostrare la sua estraneità ai fatti. Viceversa, la responsabilità dell'ente è da dimostrare nel caso in cui chi ha commesso l'illecito non ricopra funzioni apicali all'interno del sistema organizzativo aziendale; l'onere della prova ricade in tal caso sull'organo accusatorio.

Se il reato è stato commesso da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'ente è responsabile se l'accusa riesce a dimostrare che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. Tali obblighi si presumono osservati qualora l'ente, prima della commissione del reato, abbia adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

L'art. 6 del Decreto, al secondo comma, indica il contenuto del Modello, che dovrà presentare le seguenti caratteristiche:

- individuare le attività nel cui ambito esiste la possibilità che siano commessi i Reati Presupposto;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Con riferimento all'efficace attuazione del Modello, il Decreto prevede, inoltre, la necessità di una verifica periodica e di una modifica dello stesso, qualora siano scoperte significative violazioni delle prescrizioni ovvero qualora intervengano mutamenti nell'organizzazione o nell'attività dell'ente.

Lo stesso Decreto (art. 6 comma 3) prevede che i modelli possano essere adottati, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (denominati anche linee guida) redatti da associazioni rappresentative di categoria.

Le linee guida vengono comunicate al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare entro 30 giorni osservazioni sulla idoneità a prevenire i reati dei modelli elaborati in conformità alle linee guida delle associazioni di categoria.

2.5. Linee guida di Confindustria

Nel 2021 Confindustria ha provveduto ad aggiornare le Linee Guida per la costruzione dei modelli organizzativi.

I punti fondamentali che le Linee Guida individuano nella costruzione dei Modelli possono essere così riassunti:

- attività di individuazione delle aree sensibili, volta a evidenziare le funzioni aziendali nell'ambito delle quali sia possibile la realizzazione degli eventi pregiudizievoli previsti dal Decreto;
- predisposizione di un sistema di controllo in grado di prevenire i rischi 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 integrato e di 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;
- applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle norme del Codice etico e delle procedure/protocolli previsti dal modello;
- individuazione dei requisiti dell'organismo di vigilanza, riassumibili in:
    - autonomia e indipendenza;
    - professionalità;
    - continuità di azione;

- previsione di modalità di gestione delle risorse finanziarie;
- obblighi di informazione dell'organismo di controllo.

Il mancato rispetto di punti specifici delle Linee Guida non inficia la validità del Modello, il quale deve essere necessariamente redatto con specifico riferimento alla realtà concreta della Società, anche discostandosi dalle Linee Guida di Confindustria che, per loro natura, hanno carattere generale.

1.6. Gruppi di Società e d.lgs. 231/01

Il **gruppo di società** è una «aggregazione di imprese» per la quale risultino soddisfatti i seguenti requisiti:

1)l'aggregazione sia costituita da più imprese, ciascuna con una propria autonomia giuridica;
2)le singole imprese siano società per azioni oppure, più raramente, a responsabilità limitata;
3)sussista un legame finanziario tale da attribuire di fatto alla società capogruppo il controllo e la direzione di tutte le imprese del gruppo.

Secondo le Linee Guida di Confindustria di cui sopra, il Gruppo non può essere considerato diretto centro di imputazione della responsabilità da reato e pertanto non rientra tra i soggetti indicati all'art. 1 del D. Lgs. 231 del 2001.

Tuttavia, ogni singola società appartenente al gruppo può essere chiamata a rispondere ai sensi del d.lgs. 231/01.

La responsabilità amministrativa dipendente da reato nell'ambito dei gruppi di società è stata delineata e circoscritta dalla giurisprudenza milanese[6] e più recentemente dalla giurisprudenza di legittimità[7], la quale ha chiarito che **la controllante può essere ritenuta responsabile per il reato commesso nell'ambito di attività della controllata solo se**:

a) dalla commissione del reato derivi un interesse o un vantaggio immediato e diretto anche per la controllante;

b) le persone fisiche appartenenti alla controllante abbiano partecipato alla commissione del reato presupposto, apportando un proprio contributo causalmente rilevante, provato in via corretta e specifica.

Ciò implica, da un lato, che se la controllante non ha riportato dal reato commesso nell'interesse della controllata né un interesse né un vantaggio, non potrà essere ritenuta responsabile *ex* d. lgs. 231/2001; dall'altro, che se i soggetti aziendali della controllante non hanno concorso nel reato presupposto commesso dai soggetti aziendali della controllata, la controllante non potrà essere ritenuta responsabile *ex* d. lgs. 231/2001.

[6] G.i.p. Tribunale di Milano, ord. 20.9.2004; Tribunale di Milano, ord. 14.12.2004; G.i.p. Tribunale di Milano, 27.2.2007.

[7] Cfr., *ex multis*, Cass., Sez. V, n. 24583 del 2011 (conf. Cass., n. 4324 del 2013); Cass., Sez. III, n. 28725 del 2018.

Per le società controllanti esiste comunque un ulteriore rischio da valutare in sede di *risk assessment* prima della elaborazione del Modello di organizzazione: il rischio che i propri soggetti aziendali, apicali o subordinati, commettano uno dei reati di cui agli artt. 24 ss. D. lgs. 231/2001 nell'interesse della/delle controllate, ma anche nel cd. interesse di gruppo, vale a dire l'interesse trascende quello perseguito dalle singole società del gruppo e che le accomuna nel raggiungimento dei medesimi obiettivi, sotto la guida della capogruppo (cd. direzione unitaria).

Quanto alle implicazioni di tali previsioni in relazione alla redazione del Modello e all'attività dell'Organismo di Vigilanza, si rinvia al paragrafo 3.7.

3. MODELLO DI GOVERNANCE

3.1. Sistema di corporate governance di Techbau S.p.A.

Techbau S.p.A. (di seguito anche solo "**Techbau**" o "**Società**"), nata nel 2010, è un General Contractor e Sviluppatore Immobiliare attivo nel settore delle Costruzioni che realizza progetti nei diversi ambiti dell'ingegneria civile e delle infrastrutture, sia in Italia sia all'estero.

Techbau si è affermata a livello nazionale per la realizzazione di edifici ad uso logistico, industriale, data center e studentati, a cui affianca la comprovata esperienza in realizzazioni ad uso residenziale, uffici, retail park e hotel.

La sede legale è situata a Milano, in Piazza Giovine Italia, 3 – 20123; al suo interno non vengono eseguite attività e non sono presenti asset aziendali, in quanto è solo una sede di appoggio ai fini fiscali, e dunque non è inclusa nel campo di applicazione del Sistema di Gestione Integrato (SGI).

La sede principale dell'organizzazione è invece a Castelletto Sopra Ticino (NO), mentre a Roma è localizzata la sede distaccata. Presso le sedi si svolgono le attività amministrative e tecnico-gestionali legate alla progettazione e gestione delle commesse. Presso i cantieri vengono eseguite attività di ingegneria, gestione e controllo cantiere, supervisione delle lavorazioni dei subappalti e supporto in attività operative con eventuale utilizzo di mezzi d'opera.

Nel 2022 Techbau ha subito una riorganizzazione societaria dovuta all'acquisizione da parte di un fondo immobiliare, BentallGreenOak IV TB LUX S.A.R.L. (BGO), che ha rilevato il 50% del capitale sociale dell'azienda. Anche grazie alla spinta innovativa dovuta all'entrata di un fondo internazionale, Techbau ha visto una importante crescita con ampliamento dei propri orizzonti commerciali.

Il modello di *corporate governance* di Techbau è strutturato in modo tale da assicurare e garantire all'Impresa la massima efficienza ed efficacia operativa nella realizzazione delle attività sociali. In particolare, la Società è amministrata da un Consiglio di Amministrazione (di seguito "**C.d.A.**"), composto dal Presidente, dall'Amministratore Delegato e da due Consiglieri, mentre il controllo sull'attività di gestione è affidato ad un Collegio Sindacale composto da tre membri effettivi e due supplenti ed è nominata una Società di revisione internazionale.

All'organo amministrativo spettano collegialmente tutti i poteri di gestione ordinaria e straordinaria dell'Impresa. Il C.d.A. può nominare il direttore generale, direttori di funzione, institori e procuratori per determinati atti o categorie di atti, nonché delegare, nei limiti di cui all'art. 2381 c.c., parte delle proprie attribuzioni ad uno o più dei suoi componenti. La rappresentanza della Società spetta al Presidente, nonché agli Amministratori Delegati, nei limiti della delega loro conferita dal Consiglio, e agli altri Direttori e Responsabili della Società che hanno rapporti esterni, nei limiti dei poteri conferiti dall'organo amministrativo, e ai Procuratori Speciali, che possono essere nominati per singoli atti o per categorie di atti, ciascuno nell'ambito dei propri poteri.

La struttura organizzativa di Techbau è orientata a garantire una separazione di compiti, ruoli e responsabilità, nonostante molte attività siano svolte in team interfunzionali e in pieno coordinamento fra le varie funzioni preposte e la Direzione Generale; ciò al fine di migliorare l'efficienza sui vari processi aziendali e garantire un controllo più pervasivo sull'esercizio delle attività sociali.

La suddivisione dei compiti e dei ruoli è quella delineata nell'organigramma aziendale generale e in quelli di dettaglio che vengono annualmente rivisti ed aggiornati per dare seguito ai cambiamenti organizzativi.

Techbau S.p.A. e le società partecipate Techbau Green Energy S.r.l., Aurelia Garden S.p.A., Corte dei Principi S.r.l., Fabrica X S.r.l., Logi-Tech S.r.l., Rubattino 87 S.r.l. e Via Bombay n. 1 S.r.l. hanno stipulato un contratto di prestazione di servizi aziendali e amministrativi forniti dalla prima in favore delle seconde.

Ciascuna delle società partecipate sopra menzionate ha adottato un Modello Organizzativo ai sensi del D.Lgs. 231/2001 che disciplina il monitoraggio delle aree a rischio reato, comprese quelle in cui vengono erogati i servizi di Techbau S.p.A.

Per il monitoraggio di tali aree a rischio reato, pertanto, i dipendenti di Techbau devono attenersi alle prescrizioni indicate nei Modelli delle società partecipate, in relazione alle parti rilevanti nell'ambito dell'erogazione dei servizi previsti nel Contratto.

Techbau si impegna pertanto a riconoscere i Modelli e i Codici Etici adottati da tali Società, a rispettarli, ad attuarli nelle aree di propria competenza e a trasmettere all'Organismo di Vigilanza tutta la documentazione relativa alle attività svolte per conto e nell'interesse delle stesse.

La politica aziendale della Società pone, tra i suoi obiettivi, il rispetto delle prescrizioni contenute nel D.Lgs. 231/01 che disciplina la responsabilità amministrativa degli enti.

Tale finalità viene perseguita con volontà imprenditoriale, mettendo a disposizione le risorse necessarie, e il raggiungimento di tali obiettivi viene valorizzato da un'attenta gestione di tutti i processi, vigilando sulla loro efficacia e garantendo con gli opportuni sistemi di controllo un livello di prevenzione del rischio che risponda alle esigenze del D.lgs. 231/01.

La scelta di adozione del Modello si ritiene che possa costituire, così come il Codice Etico ed altri elementi del sistema di controllo, un potente strumento di sensibilizzazione nei confronti di tutti i soggetti che operano in nome o/e per conto della Società affinché nell'espletamento delle loro attività siano indotti a comportamenti ispirati dall'etica ed in linea con le regole e le procedure contenute nel Modello.

Nella predisposizione del presente Modello si è tenuto conto del sistema di controllo già operante in azienda ove giudicato idoneo a soddisfare le finalità di prevenzione dei rischi di commissione dei reati contemplati dal D.Lgs. 231/01.

L'impresa può oggi vantare di occupare una significativa posizione tra le società che effettuano costruzione di opere analoghe. Uno dei suoi principali punti di forza è costituito dall'attenzione verso la Clientela, la Committenza e l'utilizzatore dell'opera stessa, in essere o potenziale, accompagnata dalla flessibilità di adattare il servizio verso tali richieste.

L'impresa intende mantenere e consolidare la posizione acquisita, migliorando costantemente i risultati ottenuti. Date queste premesse l'impresa considera i propri Sistemi di Gestione per la Qualità, per la Sicurezza sul Lavoro e per la Tutela Ambientale come uno dei principali strumenti di miglioramento. La significatività del messaggio espresso è stata comunicata a tutto il personale e resa pubblica verso l'interno mediante affissione in bacheca attraverso i seguenti documenti:

- "Politica per la Qualità"
- "Politica per la Salute e Sicurezza dei lavoratori"
- "Politica per la Salvaguardia dell'Ambiente"
- "Politica per la Prevenzione della Corruzione"
- "Politica per la Privacy e Sicurezza delle informazioni"
- "Politica della Sostenibilità"
- "Politica per gli Acquisti Sostenibili"
- "Politica BIM"
- "Politica per la Parità di Genere"

I Sistemi di gestione prevedono al loro interno le attività di controllo necessarie a verificare la conformità ai rispettivi standard:

- UNI EN ISO 9001 per i Sistemi di gestione per la qualità;
- UNI EN ISO 14001 per i Sistemi di gestione per l'ambiente;
- UNI EN ISO 45001 per i Sistemi di gestione per la Salute e la Sicurezza sul Lavoro;
- UNI EN ISO 27001: sistema di gestione per la sicurezza delle informazioni;
- UNI EN ISO 37001: sistema di gestione per la prevenzione della corruzione;
- UNI/PdR74:2019: sistema di gestione BIM;
- UNI/PdR125:2022: sistema di gestione per la parità di genere.

La corretta implementazione di ogni sistema di gestione specifico è monitorata dal personale interno di Techbau in possesso di competenze e capacità specificamente individuate, nonché da parte di personale esterno appositamente selezionato per gestire al meglio tutti i requisiti e controlli del sistema di gestione.

Il sistema informativo costituisce un elemento che garantisce l'efficienza e funzionalità del sistema di controllo.

Le modalità di controllo sono definite nel dettaglio nei documenti predisposti per ottemperare al GDPR (regolamento UE/2016/679).

3.2. Il Codice Etico e di comportamento

Il Codice Etico, che costituisce parte essenziale del modello, esprime l'insieme dei valori, dei doveri e delle responsabilità che sono stati perseguiti nel corso degli anni nella conduzione degli affari e delle attività aziendali di Techbau, nel rispetto delle regole d'impresa.
Esso sintetizza i principi di legalità e, più in generale, di correttezza ai quali si uniforma nello svolgimento di tutte le sue attività e nelle sue relazioni (interne ed esterne).

Il Codice Etico, in particolare, rappresenta l'impegno nel perseguire i più alti standard di moralità, oltre che di legalità. In effetti la Società si è sempre prefissa di improntare la propria attività al più rigoroso rispetto, non soltanto delle leggi e di ogni altra disciplina normativa applicabile, ma altresì dei principi etici coerenti alla sua natura istituzionale ed ai suoi scopi statutari, nonché dei principi di deontologia professionale. Perciò, indipendentemente da quanto è prescritto dal Decreto, il Codice Etico ha la funzione di compendiare la "carta dei valori" e di indicare i canoni di comportamento strumentali alla loro attuazione, costituendo il criterio di orientamento dell'attività quotidiana per tutti coloro che operano nell'interesse della Società.

La funzione del Codice Etico, per portata oggettiva e soggettiva e dettaglio prescrittivo, si distingue da quella propria del Modello (che risponde specificamente a tassative disposizioni del Decreto). Ciononostante i dettami del Codice Etico contribuiscono altresì a prevenire i reati e perciò, per quanto di ragione, sono qui intesi come un complemento dei protocolli e delle procedure aziendali e, come tali, applicati ai Destinatari del Modello. Perciò nei confronti di questi ultimi, anche l'inosservanza dei canoni di comportamento del Codice Etico sarà sanzionabile secondo le previsioni del Sistema Disciplinare di volta in volta a loro applicabili.

I Destinatari del Codice Etico sono la Società, i Dipendenti ed i soggetti terzi che operano sotto la direzione e vigilanza della Società stessa.

In ragione della suddetta diversa e maggiore sua funzione, Destinatari di detto Codice Etico, in quanto tale, si intendono anche i collaboratori parasubordinati (non fattivamente e strutturalmente inseriti nell'organizzazione aziendale), i lavoratori autonomi, gli (eventuali) agenti/distributori, nonché i fornitori, e, più in generale, le controparti contrattuali della Società che non siano destinatarie del Modello, con riferimento altresì ai Revisori Legali, nel senso che la Società si aspetta che i relativi canoni di comportamento siano da costoro condivisi e scrupolosamente osservati. Perciò il Codice Etico sarà allegato al – e considerato come parte integrante del – contratto con i suddetti soggetti, che verrà quindi sciolto ove la Società venga a conoscenza, nei limiti di quanto consentitole dalla natura e dalla disciplina di ciascun rapporto, di comportamenti difformi dai relativi principi e canoni di comportamento. A tal fine, ribadita l'inapplicabilità dei non Destinatari del Modello del Sistema Disciplinare, si potrà fare ricorso ad appositi rimedi su base contrattuale

quali, ad esempio, clausole risolutive espresse ai sensi dell'art. 1456 c.c. o la previsione di clausole penali ex art. 1382 c.c.

I principi e le norme di comportamento dettate dal Codice Etico sono di arricchimento ai processi decisionali ed orientano la condotta della Società nei rapporti con i Destinatari.

I criteri di condotta enunciati nel Codice Etico hanno lo scopo di indirizzare i comportamenti dei Destinatari affinché li uniformino a criteri di correttezza, lealtà e trasparenza al fine di soddisfare le esigenze che l'applicazione del Modello intende perseguire.

I principi su cui si basa il Codice Etico, con particolare riferimento a quanto attiene al Modello, sono:

- la legalità;
- l'equità e l'eguaglianza;
- l'integrità e la correttezza professionale;
- la trasparenza e la diligenza;
- l'imparzialità;
- la leale concorrenza;
- la prevenzione dei conflitti di interesse;
- la riservatezza;
- la tutela della persona;
- la protezione della salute e la salubrità dei luoghi di lavoro;
- la tutela ambientale;
- l'innovazione e la ricerca.

3.3. Protocolli relativi alle modalità di gestione delle risorse finanziarie

Con riferimento alle attività sensibili, il Modello prevede anche specifici protocolli dedicati alle modalità di gestione delle risorse finanziarie, anche infragruppo. Finalità principale di tali protocolli è impedire la costituzione di fondi fuori bilancio.

Le procedure aziendali predisposte in attuazione di tali protocolli assicurano, per quanto possibile in funzione delle dimensioni della Società, la separazione e l'indipendenza tra i soggetti che concorrono a formare le decisioni di impiego delle risorse finanziarie, coloro che attuano tali decisioni e coloro ai quali sono affidati i controlli circa l'impiego delle risorse finanziarie.

Tutte le operazioni che comportano utilizzazione o impegno di risorse economiche o finanziarie devono avere adeguata causale ed essere documentate e registrate, con mezzi manuali o informatici, in conformità a principi di correttezza professionale e contabile; il relativo processo decisionale deve essere verificabile. Tutte le operazioni inerenti ad attività

o prestazioni atipiche o inusuali devono essere specificamente e chiaramente motivate e comunicate all'Organismo di Vigilanza.

I protocolli e le procedure attuative relativi alle modalità di gestione delle risorse finanziarie sono aggiornati anche su proposta o segnalazione dell'Organismo di Vigilanza, il quale indirizza al management indicazioni relative a opportune integrazioni ai sistemi gestionali delle risorse finanziarie (in entrata e in uscita), con eventuali accorgimenti pensati proprio al fine del rispetto del D.Lgs. 231/2001 (ad esempio rilevazione delle anomalie in particolari operazioni o pagamenti che non risultano giustificati dall'economia della transazione).

4. IL MODELLO ADOTTATO DA TECHBAU S.P.A.

4.1. Finalità del Modello

Il Modello di Techbau s.p.a. ha lo scopo di prevenire la commissione di reati e di reprimere qualsiasi comportamento illecito svolto nell'ambito dell'attività sociale, attraverso la predisposizione di un sistema strutturato ed organico di procedure e attività di controllo.

Questo obiettivo viene perseguito mediante l'individuazione delle attività sensibili nell'ambito delle quali esiste un rischio di commissione di reati. Per ciascuna di tali attività, il sistema organizzativo della Società impone delle regole e dei processi diretti a impedire la commissione dei reati e un adeguato sistema di controllo interno.

Il Modello, così strutturato, si pone come obiettivo di:

- cristallizzare e definire i comportamenti che sono considerati illeciti dalla Società, oltre che dall'ordinamento, in quanto contrari alle disposizioni di legge ed ai principi etici che Techbau s.p.a. intende osservare nell'esercizio dell'attività aziendale;
- informare e formare tutti coloro che operano in nome e per conto della Società che la commissione di un reato (anche nella forma tentata) – effettuata, in tutto o in parte, a vantaggio o nell'interesse della Società – costituisce una violazione delle regole aziendali e può assumere rilevanza nei loro confronti sul piano penale e nei confronti della Società per quanto riguarda la responsabilità amministrativa da reato *ex* D.Lgs. 231/2001;
- controllare i settori di attività sensibili.

4.2. Rischio accettabile

Un concetto critico nella costruzione del Modello è quello di rischio accettabile. Infatti, ai fini dell'applicazione delle norme del Decreto è importante definire una soglia che permetta di porre un limite alla quantità e qualità degli strumenti di prevenzione da introdurre per inibire la commissione del reato.

In relazione al rischio di commissione dei reati di cui al D.Lgs. 231/2001, la soglia di accettabilità è rappresentata da un sistema preventivo tale da non poter essere aggirato se non intenzionalmente. In altre parole, ai fini dell'esclusione di responsabilità amministrativa dell'ente, le persone che hanno commesso il reato devono aver agito eludendo fraudolentemente il Modello ed i controlli adottati.

4.3. Il Modello (struttura, destinatari e ambito di applicazione)

Il presente Modello è costituito da:

- una "**Parte Generale**", che descrive la normativa rilevante e le regole generali di funzionamento del Modello e dell'Organismo di Vigilanza;
- una "**Parte Speciale**", focalizzata sulle aree di attività e i processi strumentali ritenuti "sensibili", le norme di comportamento e gli altri strumenti di controllo ritenuti rilevanti in relazione ai reati da prevenire e agli assetti organizzativi della Società.

Nel caso in cui si verifichino cambiamenti del contesto interno ed esterno, la Società si impegna ad adeguare il Modello e garantisce la sua osservanza e il suo funzionamento secondo le modalità operative ritenute più appropriate, rispettando principi inderogabili di controllo.

Il Modello si inserisce nel più ampio sistema di organizzazione e controllo già esistente in Techbau s.p.a. e che intende integrare con i seguenti elementi qualificanti:

- la mappatura delle attività sensibili rispetto alla commissione dei reati previsti dal D.Lgs. 231/2001, da sottoporre ad analisi e monitoraggio periodico;
- le regole di comportamento ricomprese anche nel Codice etico di Techbau s.p.a., finalizzate ad impedire il verificarsi dei reati di cui al D.Lgs. 231/2001;
- l'attribuzione ad un Organismo di Vigilanza (OdV) della Società dei compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
- i flussi informativi nei confronti dell'OdV;
- il sistema sanzionatorio idoneo a garantire l'efficace attuazione del Modello contenente le disposizioni disciplinari applicabili in caso di mancato rispetto delle misure indicate nel Modello medesimo;
- la verifica e documentazione di ogni operazione atipica o rilevante;
- la definizione di poteri autorizzativi ed esecutivi coerenti con le responsabilità assegnate;
- una disponibilità a favore dell'OdV di risorse aziendali di numero e valore adeguato e proporzionato ai risultati attesi e ragionevolmente ottenibili;
- le regole e le responsabilità per l'implementazione e per l'aggiornamento periodico del Modello, nonché per la verifica del funzionamento e dell'efficacia del Modello;
- l'attività di sensibilizzazione, informazione e divulgazione a tutti i livelli aziendali e ai destinatari esterni delle regole comportamentali e delle procedure adottate dalla Società;
- l'attività di sensibilizzazione e informazione a tutti i destinatari del Modello relativa al rispetto dei principi normativi di cui al Decreto.

Il Modello è destinato, nello specifico, a tutti i dipendenti e amministratori della Società. Nella parte applicabile, il Modello è destinato anche ai fornitori, ai subappaltatori e ai *partner* commerciali, intesi sia come persone fisiche, sia come società che prestano, secondo diverse forme o modalità, la propria collaborazione a Techbau s.p.a. per lo svolgimento delle proprie attività. Pertanto, i suddetti contratti di appalto, subappalto e/o di *partnership* commerciale che Techbau s.p.a. dovesse stipulare con terzi dovranno necessariamente prevedere specifiche clausole che permettano di garantire il rispetto del Modello o, comunque, il rispetto del Decreto Legislativo n. 231/2001.

In ogni caso Techbau s.p.a., prima di legarsi a terzi con stabili vincoli contrattuali, dovrà svolgere un'adeguata procedura di *due diligence* diretta a verificare, fra l'altro; (i) la reputazione e l'affidabilità del soggetto con cui intende contrattare e dei suoi principali esponenti, soci ed amministratori; (ii) la stabilità finanziaria e patrimoniale della controparte o del *partner*; (iii) la competenza ed esperienza tecnica per rendere il servizio richiesto e oggetto del contratto; (iv) le referenze e i rapporti con le pubbliche autorità.

4.4. Approvazione del Modello

Il Modello, in conformità a quanto disposto dall'art. 6, comma 1, lettera a) del D.Lgs. 231/2001, è stato adottato con atto del Consiglio di Amministrazione del 26 settembre 2025.

Il Consiglio di Amministrazione, nell'adottare il Modello, ha affidato all'OdV l'incarico di assumere le funzioni di organo di controllo con il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza dello stesso, nonché di curarne l'aggiornamento.

4.5. Aggiornamento e attuazione del Modello

Il Modello è sottoposto a verifica periodica e viene modificato nel caso in cui vengano individuate significative violazioni delle prescrizioni o si verifichino mutamenti dell'organizzazione, delle attività della Società o della normativa di riferimento.

Le modifiche e/o integrazioni di carattere sostanziale del Modello, anche laddove proposte dall'OdV, sono rimesse alla competenza del Consiglio di Amministrazione.

È fatto obbligo a chiunque operi nella Società o collabori con essa di attenersi alle pertinenti prescrizioni del Modello, ed in specie di osservare gli obblighi informativi dettati per consentire il controllo della conformità dell'operato alle prescrizioni stesse.

Copia del Modello, dei documenti ad esso allegati e dei suoi aggiornamenti è depositata presso la sede della Società ed è a disposizione di chiunque abbia titolo a consultarla.

La Società provvede a notificare a ciascun destinatario del Modello le prescrizioni riferite alla specifica attività o funzione dallo stesso rivestita all'interno della Società.

Come anticipato, spetta all'OdV il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

4.6. Modello e Codice Etico

Techbau s.p.a. intende improntare lo svolgimento della propria attività, il perseguimento dello scopo sociale e la crescita della Società al rispetto non solo delle leggi e dei regolamenti vigenti, ma anche di principi etici condivisi.

A tal fine, Techbau s.p.a. si è dotata di un Codice etico (il "**Codice etico**"), allegato al presente Modello, approvato dal Consiglio di Amministrazione con delibera del 26 settembre 2025, volto a definire una serie di principi di "deontologia aziendale" che la Società riconosce come propri e dei quali esige l'osservanza da parte degli organi societari, dei propri dipendenti e di tutti coloro che cooperano a qualunque titolo al perseguimento dei fini aziendali.

Il Codice etico ha una portata di carattere generale e rappresenta uno strumento adottato in via autonoma da parte di Techbau s.p.a., anche se richiama principi di comportamento rilevanti ai fini del Modello.

4.7. Adozione del Modello nell'ambito del Gruppo

Quale società capogruppo, Techbau s.p.a. promuove l'adozione e l'efficace attuazione da parte di tutte le società del Gruppo di propri modelli organizzativi. Ciascuna società del Gruppo svolge autonomamente l'attività di predisposizione e adozione del proprio Modello di organizzazione, gestione e controllo ex D.lgs. 231/01, anche tenendo conto dei principi di condotta adottati dal Gruppo.

Come ribadito dalle Linee Guida di Confindustria, ogni società del Gruppo dovrà predisporre un proprio Modello organizzativo in piena autonomia (anche seguendo linee guida previste da parte della capogruppo) e dovrà nominare un proprio Organismo di Vigilanza, promuovendo riunioni tra i singoli Organismi di Vigilanza del Gruppo.

È pertanto responsabilità delle singole società del Gruppo l'attuazione dei principi di controllo previsti nel Modello, in relazione alle attività poste concretamente in essere nei settori a rischio di commissione di reati.

Si precisa che, nell'esercizio dei propri poteri di direzione e coordinamento, Techbau:

- non dirama indicazioni in termini precettivi e vincolanti, nell'attività di elaborazione e revisione dei Modelli adottati dalle società del Gruppo;
- presta un supporto di natura unicamente consulenziale, volto ad agevolare le attività di adozione, aggiornamento, implementazione e monitoraggio dei modelli da parte delle singole società del Gruppo;
- delinea regole specifiche per la correttezza e la trasparenza nei rapporti con le singole società del Gruppo, attraverso comunicazioni rese in forma ufficiale.

Ogni società del Gruppo:

- adotta principi etico-comportamentali specificamente determinati in relazione alla propria operatività e alle fattispecie di reati per essa rilevanti;
- implementa autonomamente ed integra, laddove necessario in base alla specifica operatività e all'effettiva esposizione ai rischi-reato contemplati dal decreto, codici di comportamento, sistema disciplinare e protocolli relativi alle attività del Gruppo.

Sono istituiti canali di comunicazione tra tutte le società del Gruppo riguardanti lo stato di attuazione del sistema adottato ai sensi del Decreto e dei rispettivi Modelli e Codici Etici, eventuali violazioni e sanzioni applicate,

aggiornamenti dei modelli predisposti a seguito dell'introduzione di nuove fattispecie di reato nell'elenco dei reati presupposto, interlocuzioni con i rispettivi Organismi di Vigilanza.

5. L'ORGANISMO DI VIGILANZA (OdV)

5.1. Composizione

È costituito un organismo interno, denominato Organismo di Vigilanza (OdV), cui è affidato il compito di vigilare con continuità sull'efficace funzionamento e sull'osservanza del Modello e di curarne l'aggiornamento. L'Organismo di Vigilanza deve svolgere attività specialistiche che presuppongano la conoscenza di strumenti e tecniche *ad hoc* e deve essere caratterizzato da continuità d'azione. Non può essere individuato nel Consiglio di Amministrazione.

L'Organismo di Vigilanza svolge le sue funzioni al di fuori dei processi operativi della Società ed è svincolato da ogni rapporto gerarchico all'interno dell'organigramma aziendale. L'OdV è una figura che riporta direttamente ai vertici della Società, sia operativi che di controllo, in modo da garantire la sua piena autonomia e indipendenza nello svolgimento dei compiti che gli sono affidati.

La composizione dell'Organismo di Vigilanza è individuata nel verbale di nomina dello stesso.

L'Organismo di Vigilanza può essere monosoggettivo o plurisoggettivo e può essere composto sia da soggetti esterni che da soggetti interni alla Società.

Nelle società di capitali la funzione di OdV può essere anche svolta dal Collegio Sindacale. Con riferimento alle imprese di piccole dimensioni, l'art. 6 co. 4 D.lgs. 231/2001 consente inoltre che i compiti di Organismo di Vigilanza siano assolti dall'organo dirigente.

L'articolazione interna dell'organismo di controllo (essenzialmente quante risorse umane e finanziarie destinare ai controlli) deve essere direttamente correlata alla complessità strutturale della Società (dimensioni, caratteristiche organizzative, dislocazione sul territorio, ecc.). *A priori* non è possibile fissare limiti quantitativi, né in termini di fatturato, né di numero di dipendenti della società interessata; la composizione dell'organismo di controllo va, infatti, valutata caso per caso a seconda dei risultati dell'analisi dei rischi, dalla quale emergano quante e quali aree, processi e funzioni devono essere assoggettate a controllo.

Techbau s.p.a. ha ritenuto di conferire la qualifica di Organismo di Vigilanza ad un organo collegiale di tre membri:

a. nominato dal Consiglio di Amministrazione;
b. composto da tre professionisti, uno interno e due esterni all'Azienda, individuati tra soggetti particolarmente qualificati ed esperti nelle materie rilevanti ai fini del D.Lgs. 231/2001, in modo da garantire all'Organismo adeguata competenza in materia legale, in specie penalistica, contabile, di *risk assessment* ed *internal auditing*, nonché in possesso dei necessari requisiti di onorabilità. I componenti dell'OdV devono essere indipendenti dalla Società e pertanto non devono avere rapporti di parentela con i soci o gli amministratori della Società, o delle Società da questa controllate e/o partecipate nonché delle Società controllanti e/o partecipanti idonei a ridurne l'autonomia di giudizio;

c. dotato di autonomi poteri di intervento nelle aree di competenza. A tal fine, nonché per garantire lo svolgimento con continuità dell'attività di verifica circa l'adeguatezza e l'idoneità del Modello, l'Organismo può avvalersi di personale interno e/o di collaboratori esterni;
d. dotato di un *budget* di spesa ad uso esclusivo per il periodo in cui resta in carica, deliberato dal Consiglio di Amministrazione. L'OdV delibera in autonomia e indipendenza le spese da effettuarsi nei limiti del *budget* approvato e rimanda a chi è dotato dei poteri di firma in Techbau s.p.a. per sottoscrivere i relativi impegni. In caso di richiesta di spese eccedenti il *budget* approvato, l'OdV dovrà essere autorizzato dall'Consiglio di Amministrazione di Techbau s.p.a..

L'Organismo di Vigilanza è nominato per un periodo determinato, con possibilità di rinnovo.

L'Organismo si riunisce con cadenza almeno trimestrale.

Ai fini di una migliore conoscenza e corretto presidio del contesto aziendale, l'Organismo di Vigilanza può richiedere la presenza alle proprie riunioni, anche in forma permanente, di soggetti quali, a titolo di esempio, membri del Collegio Sindacale e responsabili delle funzioni aziendali aventi attinenza con le tematiche del controllo. Questi partecipano alle riunioni esclusivamente in qualità di invitati.

Sono cause di ineleggibilità ed incompatibilità con l'incarico di membro dell'Organismo di Vigilanza, anche a garanzia del requisito di onorabilità:
- essere in conflitto d'interesse, anche potenziale, con la Società;
- essere Revisore Contabile di Techbau s.p.a.;
- avere relazioni di coniugio, parentela o affinità fino al quarto grado con i soggetti di cui ai punti precedenti;
- essere stato condannato con sentenza anche non irrevocabile a pena detentiva che comporta l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle ordinarie persone giuridiche;
- essere stato condannato con sentenza anche non irrevocabile ed anche a seguito di applicazione della pena su richiesta ai sensi degli articoli 444 e 447 c.p.p. per delitti non colposi e per reati richiamati nell'ambito del D.Lgs. 231/2001.

5.2. Revoca e sostituzione

A tutela dell'autonomia ed indipendenza dell'Organismo, modifiche alla sua struttura (quali ad esempio revoche), ai suoi poteri e al suo funzionamento possono essere apportate unicamente a mezzo di decisioni adottate dal Consiglio di Amministrazione.

La revoca dell'OdV può avvenire unicamente per giusta causa.

A tale proposito, per giusta causa dovrà intendersi:

- un grave inadempimento dei propri doveri di vigilanza;
- una sentenza di condanna della Società ovvero una sentenza di patteggiamento ai sensi del Decreto, dalla quale risulti "*l'omessa o insufficiente vigilanza*" da parte dell'OdV;
- la violazione degli obblighi di riservatezza (anche in riferimento a quanto disciplinato dall'art. 6, comma 2 bis, lettera d) del D.Lgs. 231/2001).

In tutti i casi di applicazione in via cautelare di una sanzione interdittiva prevista dal Decreto, il Consiglio di Amministrazione, assunte le opportune informazioni, potrà eventualmente provvedere alla revoca dell'OdV, qualora ravvisi un'ipotesi di omessa o insufficiente vigilanza da parte dello stesso.

Nel caso in cui vengano meno i requisiti di autonomia, indipendenza e professionalità ovvero in caso di insorgenza di una delle cause di ineleggibilità/incompatibilità sopra individuate, il Consiglio di Amministrazione, esperiti gli opportuni accertamenti e sentito l'interessato, stabilisce un termine, non inferiore a 30 giorni, entro il quale deve cessare la situazione di incompatibilità. Trascorso tale termine senza che la predetta situazione sia cessata, il Consiglio di Amministrazione deve dichiarare l'avvenuta decadenza dell'OdV.

Parimenti, una grave infermità che renda il componente dell'Organismo inidoneo a svolgere le proprie funzioni di vigilanza, ovvero un'infermità o altre ragioni di natura personale che, comunque, determinino l'assenza dalle attività per un periodo superiore ai 3 mesi, comporterà la dichiarazione di decadenza dello stesso, da attuarsi secondo le modalità sopra descritte.

Nel caso di dimissioni, revoca o decadenza dell'Organismo di Vigilanza, il Consiglio di Amministrazione dovrà provvedere alla nomina del nuovo Organismo in modo tempestivo.

5.3. Requisiti

L'OdV deve garantire i seguenti requisiti:

a. **autonomia e indipendenza:** mirano a garantire che l'Organismo di Vigilanza non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo e, soprattutto, la possibilità di svolgere il proprio ruolo senza condizionamenti diretti o indiretti da parte dei soggetti controllati. Detti requisiti sono assicurati dall'assenza di alcun riporto gerarchico all'interno dell'organizzazione aziendale e di compiti operativi e dalla facoltà di *reporting* direttamente al Consiglio di Amministrazione;

b. **professionalità:** è un organismo dotato di competenze tecnico-professionali e specialistiche adeguate alle funzioni che è chiamato a svolgere (es. tecniche di intervista, *flow charting*, tecniche di analisi dei rischi, ecc.). Tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio;

c. **continuità di azione:** è un organismo interno all'organizzazione, adeguato in termini di struttura e risorse dedicate, nonché privo di mansioni operative che possano limitare l'impegno necessario allo svolgimento delle funzioni assegnate;

d. **onorabilità e assenza di conflitti di interesse**.

Al fine di attribuire all'Organismo di Vigilanza idonea capacità di reperimento delle informazioni e quindi di effettività di azione nei confronti dell'organizzazione aziendale, sono stabiliti, mediante il presente Modello e, successivamente, mediante appositi documenti organizzativi interni emanati dal Consiglio di Amministrazione o dall'Organismo di Vigilanza, i flussi informativi da e verso l'Organismo medesimo.

5.4. Funzioni e poteri

All'OdV, che risponde della propria attività direttamente all'organo dirigente della Società e che è dotato di un proprio *budget*, sono riconosciuti autonomi poteri di iniziativa e di controllo nell'esercizio delle sue funzioni e non possono essere attribuiti compiti operativi o poteri decisionali, neppure di tipo impeditivo, relativi allo svolgimento delle attività della Società medesima.

All'Organismo di Vigilanza di Techbau s.p.a. è affidato sul piano generale il compito di vigilare:

a. sull'osservanza delle prescrizioni del Modello da parte dei Dipendenti, degli organi sociali, dei consulenti e delle imprese controparti nella misura in cui è richiesta a ciascuno di loro;
b. sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei reati di cui al D.Lgs. 231/2001;
c. sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative;
d. sull'adeguatezza, sull'applicazione e sull'efficacia del sistema sanzionatorio.

All'OdV è affidato, sul piano operativo, il compito di:

1. svolgere le attività di controllo previste dal Modello;
2. verificare costantemente l'efficacia e l'efficienza delle procedure aziendali vigenti, ricorrendo all'ausilio delle competenti funzioni, nonché del Responsabile della Sicurezza (RSPP) per quanto concerne le problematiche concernenti l'igiene, la salute e la sicurezza dei lavoratori;

3. condurre ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura delle attività sensibili e dei processi strumentali;
4. effettuare periodicamente verifiche mirate su determinate operazioni o specifici atti posti in essere da Techbau s.p.a., soprattutto nell'ambito delle attività sensibili o "strumentali" alla realizzazione delle stesse;
5. coordinarsi con il Consiglio di Amministrazione per i programmi di formazione del personale;
6. monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisposizione della documentazione interna necessaria al fine del funzionamento del Modello, contenente le istruzioni, chiarimenti o aggiornamenti. L'OdV deve nella sua attività continuativa realizzare ed applicare procedure operative per la migliore gestione formale dell'attività;
7. raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere a lui trasmesse o tenute a sua disposizione costituendo l'archivio "formale" dell'attività di controllo interno;
8. coordinarsi con le altre funzioni aziendali nell'espletamento delle attività di monitoraggio di loro competenza e previste nei protocolli;
9. verificare l'adeguatezza del sistema di controllo interno in relazione alla normativa vigente ai fini di *compliance* ai sensi del D.Lgs. 231/2001;
10. verificare che gli elementi previsti per l'implementazione del Modello (adozione di clausole standard, espletamento di procedure, ecc.) siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, adottando o suggerendo l'adozione, in caso contrario, di un aggiornamento degli elementi stessi;
11. verificare le esigenze di aggiornamento del Modello;
12. riferire periodicamente al Consiglio di Amministrazione e al Collegio Sindacale in merito all'attuazione delle politiche aziendali per l'attuazione del Modello;
13. controllare l'effettiva presenza, la regolare tenuta e l'efficacia dell'archivio a supporto dell'attività *ex* D.Lgs. 231/2001.

A tal fine, all'OdV sono attribuiti i seguenti poteri:

a. emanare disposizioni intese a regolare l'attività dell'Organismo;
b. svolgere attività ispettiva con modalità predeterminate e comunicate all'organo dirigente;
c. accedere ad ogni e qualsiasi documento aziendale rilevante per lo svolgimento delle funzioni attribuite all'Organismo ai sensi del D.Lgs. 231/2001;
d. chiedere informazioni a chiunque operi per conto della Società nell'ambito delle attività sensibili, anche senza previa autorizzazione dell'organo dirigente;
e. ricorrere a consulenti esterni di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello;
f. disporre che i responsabili delle varie funzioni forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso da parte delle strutture organizzative aziendali;

g. proporre l'attivazione delle procedure sanzionatorie;
h. esprime parere in merito alla adeguatezza e idoneità delle modifiche del Modello elaborate d'iniziativa dell'organo dirigente, prima della loro adozione.

5.5. Flussi informativi da parte dell'OdV

L'OdV riferisce gli esiti delle proprie attività di controllo direttamente al Consiglio di Amministrazione e non dipende gerarchicamente da nessuna delle funzioni aziendali.

All'esito di ogni attività ispettiva l'OdV redige uno specifico **verbale**, conservato presso lo stesso Organismo.

In particolare, l'Organismo di Vigilanza opera secondo le seguenti linee di *reporting*:

1. su *base periodica*, mediante l'invio di una **relazione annuale** diretta al Consiglio di Amministrazione e al Collegio Sindacale, nonché per conoscenza alla società di revisione contabile;
2. *tempestiva*, mediante l'invio di una **relazione** diretta al Consiglio di Amministrazione e comunque al Collegio Sindacale, ove risultino accertati **fatti di particolare rilevanza**.

L'Organismo di Vigilanza potrà essere convocato in qualsiasi momento dal Consiglio di Amministrazione o potrà a propria volta presentare richieste in tal senso per riferire in merito al funzionamento del Modello o a situazioni specifiche.

Gli incontri con i soggetti e gli organi sopra indicati devono essere verbalizzati; le copie dei verbali verranno custodite dall'OdV e dagli organismi di volta in volta coinvolti.

L'Organismo di Vigilanza è informato dell'istituzione da parte della Società di ulteriori e autonomi canali di segnalazione e dell'esigenza di interloquire con i rispettivi Responsabili nell'ipotesi in cui dovesse ricevere delle segnalazioni che sono di competenza di questi ultimi.

5.6. Flussi informativi nei confronti dell'OdV

La trasmissione delle richieste di informazioni e dei flussi informativi all'Organismo di Vigilanza, nonché delle violazioni del Codice etico, deve avvenire all'indirizzo di posta elettronica: **odv@techbau.it**

Con specifico riferimento ai flussi informativi fisiologici, che l'Organismo di Vigilanza riceve periodicamente dai Responsabili di funzione incaricati, è stata istituita la procedura PRO-Q-A03 (Allegato 4).

La trasmissione delle segnalazioni di violazioni del Modello può avvenire all'indirizzo di posta elettronica dell'OdV sopra indicato, **oppure avvalendosi della procedura cd. Whistleblowing con le tutele da questa previste di cui al paragrafo 5 che segue**, a discrezione del segnalante.

5.7. Coordinamento tra gli OdV delle società del Gruppo

A seguito dell'adozione e attuazione del Modello da parte di tutte le Società del Gruppo, verrà assicurata la periodica interlocuzione tra gli OdV di ciascuna di esse.

In particolare sarà compito dell'OdV della capogruppo, e dunque di Techbau, promuovere e rendere effettivo tale coordinamento, ad esempio attraverso la calendarizzazione di riunioni che coinvolgano gli Organismi di Vigilanza di tutte le società del Gruppo, al fine di favorire uno scambio di informazioni su temi essenziali quali gli aggiornamenti normativi eventualmente intercorsi, i fattori problematici riscontrati nell'operatività dei singoli modelli di organizzazione, la formazione del personale.

6. SEGNALAZIONI WHISTLEBLOWING

6.1. Premessa

L'adeguatezza e l'effettività del Codice etico e del Modello dipendono, tra l'altro, dall'esistenza di un efficace sistema di rilevamento delle condotte illecite e delle violazioni che permetta di far emergere le eventuali trasgressioni.

Ad implementare questo profilo è intervenuta dapprima la Legge 179/2017 recante disposizioni per la tutela degli autori di segnalazioni di reati o di irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato (c.d. *whistleblowing*), e da ultimo il D.Lgs. 24/2023, con cui l'Italia ha dato attuazione alla Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

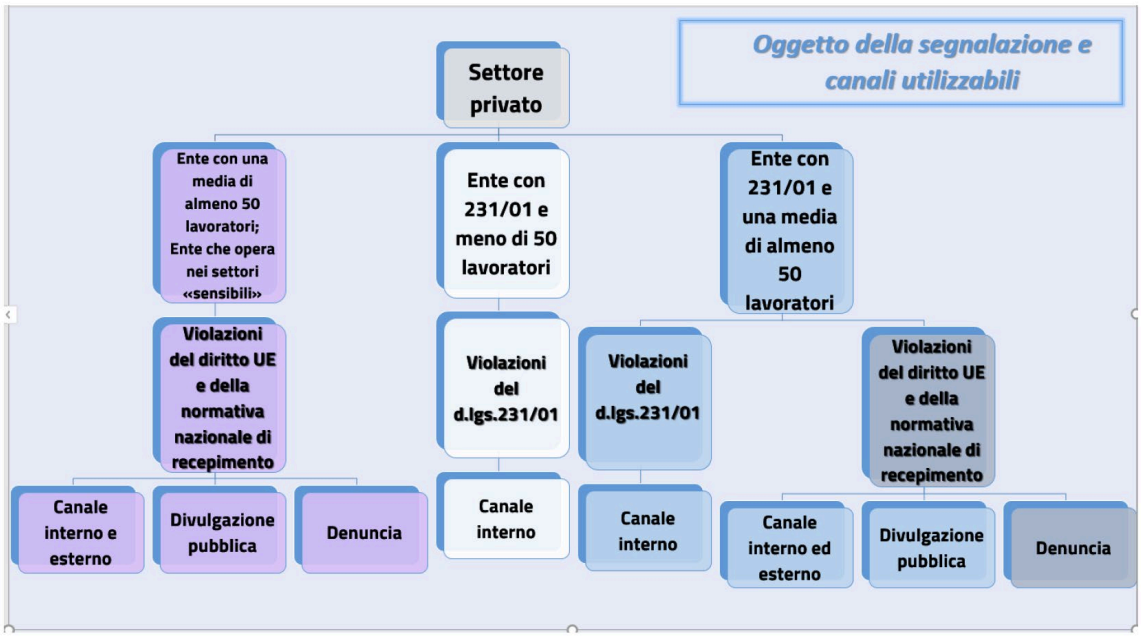
Più in dettaglio, il D.Lgs. 24/2023 prevede che il Modello debba contenere prescrizioni relative tra l'altro:

a. ai canali di segnalazione interna;
b. ai canali di segnalazioni esterna;
c. ai divieti di ritorsione;
d. alla previsione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Secondo la recente riforma, le imprese sono in generale tenute a dotarsi – a seconda delle loro dimensioni, della natura pubblica o privata delle stesse e dell'eventuale adozione di un Modello organizzativo – di strumenti idonei a raccogliere segnalazioni, anche anonime, provenienti dall'interno o dall'esterno e relative a fatti idonei ad integrare la commissione di illeciti amministrativi, contabili, civili o penali, condotte illecite rilevanti ai sensi del D.Lgs. 231/2001, violazioni del Modello organizzativo, atti od omissioni che ledono gli interessi finanziari dell'Unione europea o riguardanti il mercato interno.

L'estensione dell'oggetto della segnalazione varia a seconda della tipologia di soggetto coinvolto. Con specifico riferimento al settore privato, la normativa è stata compendiata dalle Linee guida per le segnalazioni esterne adottate da ANAC in data 12 luglio 2023 secondo il seguente schema:

Settore privato



Stante la natura privata dell'ente e la presenza di almeno di 50 lavoratori dipendenti, **la Società è dunque tenuta ad implementare un canale interno per le segnalazioni relative non solo alle violazioni del D.Lgs. 231/2001 e del presente Modello organizzativo**, **ma anche alle violazioni del diritto UE e della normativa nazionale di recepimento**[8]. Per la segnalazione di queste ultime è inoltre istituito presso ANAC (Autorità Nazionale Anticorruzione) un **canale esterno**; in tali casi il segnalante potrà altresì ricorrere, alle condizioni previste dal Decreto, alla **divulgazione pubblica** o alla **denuncia** all'Autorità giudiziaria o contabile, nei casi di loro competenza.

Secondo i dettami legislativi, la gestione del canale di segnalazione deve essere affidata ad una persona o ad un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione ovvero ad un soggetto esterno autonomo e con personale specificamente formato. Secondo quanto riconosciuto anche dalla

[8] Si tratta delle **violazioni** così come definite dall'art. 2 comma 1 lett. a) nn. 2-6 del D.lgs. 24/2023: (*i*) illeciti commessi in violazione della normativa dell'UE indicata nell'Allegato 1 al Decreto e di tutte le disposizioni nazionali che ne danno attuazione, in particolare illeciti relativi ai settori dei contratti pubblici, servizi, prodotti e mercati finanziari, 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 (a titolo esemplificativo si pensi ai reati ambientali, quali scarico, emissione o altro tipo di rilascio di materiali pericolosi nell'aria, nel terreno o nell'acqua oppure raccolta, trasporto, recupero o smaltimento illecito di rifiuti pericolosi); (*ii*) 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'Unione (si pensi, ad esempio, alle frodi, alla corruzione e a qualsiasi altra attività illegale connessa alle spese dell'Unione); (*iii*) atti od omissioni riguardanti il mercato interno che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, § 2 TFUE), tra cui 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; (*iv*) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea nei settori indicati ai punti precedenti tra cui, ad esempio, le pratiche abusive quali definite dalla giurisprudenza della Corte di Giustizia dell'UE (si pensi ad esempio a un'impresa che opera sul mercato in posizione dominante: la legge non impedisce a tale impresa di conquistare, grazie ai suoi meriti e alle sue capacità, una posizione dominante su un mercato, né di garantire che concorrenti meno efficienti restino sul mercato, tuttavia detta impresa potrebbe pregiudicare, con il proprio comportamento, una concorrenza effettiva e leale nel mercato interno tramite il ricorso alle c.d. pratiche abusive – adozione di prezzi c.d. predatori, sconti *target*, vendite abbinate – contravvenendo alla tutela della libera concorrenza.

Linee guida ANAC del 12 luglio 2023 e ribadito dalle Linee guida Confindustria del 27 ottobre 2023, tale funzione può essere ricoperta anche dall'OdV.

È inoltre istituito presso ANAC (Autorità Nazionale Anticorruzione) un canale di segnalazione esterna da utilizzare nei casi specificamente previsti dal D.Lgs. 24/2023 (per l'elencazione specifica si rinvia all'art. 6 del D.Lgs. 24/2023).

6.2. Ambito di applicazione

Forma e contenuto della segnalazione

Le segnalazioni possono essere effettuate in **forma scritta (anche con modalità informatiche) o in forma orale**.

Per **segnalazione** si intende qualsiasi comunicazione, anche anonima, avente ad oggetto la descrizione di comportamenti (attivi o omissivi), riferibili ai componenti degli organi di amministrazione e di controllo, al personale (dirigenti, quadri e dipendenti) e terze parti, rispetto ai quali vi è il ragionevole sospetto o la consapevolezza che siano illeciti o realizzati in violazione del Codice etico, del Modello, della normativa interna aziendale ovvero delle procedure e/o *standard* di *compliance* rilevanti ai sensi del D.Lgs. 231/2001.

Le segnalazioni devono essere circostanziate e fondate su elementi di fatto, precise e concordanti.

In particolare, anche ai fini del vaglio di ammissibilità, è necessario che risultino chiari i seguenti **elementi essenziali della segnalazione**:

- dati identificativi della persona segnalante (nome, cognome, luogo e data di nascita), nonché un recapito a cui comunicare i successivi aggiornamenti;
- circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione, *i.e.* descrizione dei fatti oggetto della segnalazione, con specificazione dei dettagli relativi alle notizie circostanziali e – ove possibile – delle modalità con cui il segnalante è venuto a conoscenza dei fatti oggetto della segnalazione;
- generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

È inoltre utile l'allegazione di documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

Nel caso di segnalazione tramite posta ordinaria, è inoltre opportuno che il segnalante indichi espressamente di voler beneficiare delle tutele in materia *whistleblowing* (es. inserendo la dicitura "riservata al gestore della segnalazione").

Dall'ambito delle segnalazioni sono escluse:

- le contestazioni, rivendicazioni o richieste connesse ad un interesse personale del segnalante che riguardi esclusivamente il proprio rapporto di lavoro ovvero che attenga ai rapporti di lavoro con le figure gerarchicamente superiori (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*;
- in materia di sicurezza e difesa nazionale;
- le indicazioni 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).

Destinatari della disciplina

Grava su **tutti i componenti della Società**, apicali e non, e sui **soggetti terzi che operano, a qualsiasi titolo, per conto o nell'interesse della Società** l'obbligo di denunciare le violazioni – anche solo "sospette" – del Codice etico, del Modello e delle procedure operative di cui vengano a conoscenza, pena l'irrogazione di sanzioni disciplinari.
La segnalazione può dunque essere effettuata da **qualunque persona che abbia acquisito informazioni su potenziali illeciti all'interno del contesto lavorativo**, tra cui a mero titolo esemplificativo dipendenti, collaboratori, membri dell'organo di amministrazione, direzione o vigilanza, volontari, tirocinanti, appaltatori e subappaltatori, fornitori, ex dipendenti con rapporto di lavoro terminato, se le informazioni sono state acquisite durante il suo svolgimento, ovvero candidati non ancora assunti, se le informazioni sulle violazioni sono state acquisite durante la selezione o in altre fasi precontrattuali.

Soggetti tutelati

Le disposizioni in materia di *whistleblowing* tutelano i seguenti soggetti:

- dipendenti della Società;
- lavoratori autonomi e titolari di un rapporto di collaborazione che svolgono la propria attività lavorativa presso la Società;
- lavoratori e collaboratori che svolgono la propria attività lavorativa presso soggetti che forniscono beni o servizi o che realizzano opere in favore della Società;
- liberi professionisti e consulenti che prestano la propria attività nei confronti della Società;
- eventuali volontari e tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la Società;
- persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza della Società, anche qualora tali funzioni siano esercitate in via di mero fatto, quali i componenti del Consiglio di Amministrazione, del Collegio sindacale e dell'Organismo di Vigilanza.

La tutela delle persone segnalanti di cui al comma precedente si applica anche:

- quando il rapporto giuridico non risulta ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
- durante il periodo di prova;
- successivamente allo scioglimento del rapporto giuridico, se le informazioni sulle violazioni sono state comunque acquisite nel corso del suddetto rapporto.

Le misure di protezione previste dalla presente Procedura si applicano altresì:

- ai facilitatori, intesi come le persone fisiche che assistono una persona segnalante nel processo di segnalazione, operanti all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- alle persone del medesimo contesto lavorativo del segnalante o legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro del segnalante che hanno con quest'ultimo un rapporto abituale e corrente.

6.3. Canale di segnalazione interna

Designazione del responsabile

La Società individua il responsabile dell'istituzione, implementazione, gestione e monitoraggio del canale di segnalazione interno (di seguito "**Responsabile *whistleblowing***") nella persona del Presidente dell'Organismo di Vigilanza, il quale è dotato di autonomia[9] e specificamente ed adeguatamente formato alla gestione delle segnalazioni.

La Società, da una parte, si impegna a garantire l'autonomia e indipendenza del Responsabile *whistleblowing* e, dall'altra, quest'ultimo ha il dovere di assicurarsi in ogni momento di essere posto nella condizione di svolgere le indagini e, in generale, i propri compiti in modo autonomo rispetto alle altre funzioni aziendali, di non essere soggetto ad interferenze di alcun tipo nello svolgimento delle stesse e di disporre di tutte le risorse personali e materiali necessarie per svolgerle. Pertanto, nel caso in cui dalla segnalazione stessa o dalla successiva indagine emergano elementi tali da far ritenere sussistente un **conflitto di interessi** – anche solo potenziale – con il Responsabile *whistleblowing*, egli sarà tenuto ad astenersi da ogni attività ulteriore relativa a tale segnalazione.

Il conflitto di interessi può sussistere nel caso in cui il Responsabile *whistleblowing* coincida con il segnalante, con il segnalato o sia comunque una persona coinvolta o interessata dalla segnalazione.

[9] Tale requisito deve essere inteso come:

- imparzialità: mancanza di condizionamenti e di pregiudizi nei confronti delle parti coinvolte nelle segnalazioni, 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.

In tali situazioni la segnalazione è indirizzata al Presidente del Consiglio di Amministrazione, il quale è tenuto al rispetto dell'obbligo di riservatezza previsto dalla disciplina.

Istituzione del canale di segnalazione

La Società adegua il proprio canale di segnalazione agli *standard* prescritti dalla normativa vigente, in modo tale da renderlo accessibile non solo ai dipendenti ma anche a tutti gli ulteriori interlocutori, quali ad esempio fornitori e clienti acquisiti o potenziali, nonché da garantire la riservatezza dell'identità del segnalante, della persona menzionata nella segnalazione e dei contenuti della segnalazione, nei termini dettagliati di seguito.

Le segnalazioni possono essere effettuate:

- **per iscritto** a mezzo ***piattaforma online*** *OurWhisper* a cui si accede dal sito *web* della società: https://www.techbau.it/

- **per iscritto** a mezzo ***posta ordinaria*** al seguente indirizzo:
  Avv. Elio Giannangeli
  Piazza Castello, 21
  20121 – Milano,
  La segnalazione deve essere inserita in due buste chiuse, includendo nella prima i dati identificativi del segnalante, unitamente a un documento di identità e nella seconda l'oggetto della segnalazione. Entrambe le buste devono essere inserite in una terza busta che riporti all'esterno la dicitura "*riservata al gestore della segnalazione*".

- in **forma orale** a mezzo ***piattaforma online*** *OurWhisper* a cui si accede dal sito *web* della società https://www.techbau.it/, tramite allegazione di registrazioni vocali.

Come sopra indicato, si precisa che è facoltà del segnalante utilizzare il canale di posta ordinaria altresì come primo punto di contatto per chiedere un **appuntamento**, in modo che possa riferire oralmente la segnalazione di persona o, previo accordo, anche a distanza tramite piattaforme di videocomunicazione *online*.

Qualora il segnalante faccia richiesta di segnalazione orale mediante **incontro**, il Responsabile *whistleblowing* fissa entro *quindici giorni* un appuntamento, in modo che il primo possa riferire la segnalazione di persona o, previo accordo, anche a distanza tramite piattaforme di videocomunicazione *online*. In caso di segnalazione orale differita:

- viene individuato un luogo idoneo a garantire la riservatezza del segnalante;
- il segnalante è avvertito del fatto che la conversazione verrà registrata;

- qualora il segnalante si opponga alla registrazione, il Responsabile *whistleblowing* redige un apposito verbale, sottoscritto da segnalante, a cui ne viene consegnata una copia;
- il segnalante avrà la possibilità di verificare, rettificare e accettare con sottoscrizione la trascrizione della conversazione.

I riferimenti al canale di segnalazione adottato sono pubblicati sul sito *web* della Società.

Nel caso in cui il segnalante preferisca non rivelare la propria identità, potrà effettuare una **segnalazione anonima**. In tal caso sarà comunque necessario identificare le persone coinvolte nei fatti segnalati, al fine di garantire che l'investigazione derivante dalla segnalazione abbia la maggior efficacia possibile. In ogni caso le segnalazioni anonime devono essere registrate dal Responsabile *whistleblowing* e la documentazione ricevuta deve essere conservata; laddove il segnalante anonimo venga successivamente identificato e abbia subito ritorsioni, allo stesso devono essere garantite le tutele previste per il segnalante. Il Responsabile *whistleblowing* garantisce pertanto anche in tal caso il rispetto della più stretta riservatezza.

Gestione della segnalazione

Secondo quanto stabilito dall'art. 5 del D.Lgs. 24/2023, una volta ricevuta la segnalazione il Responsabile *whistleblowing*:

a. rilascia al segnalante un **avviso di ricevimento** entro *sette giorni* dalla ricezione della segnalazione, a meno di segnalazioni anonime con riferimento alle quali non sia in alcun modo possibile individuare e/o instaurare un canale di comunicazione con il segnalante (i.e. segnalazione anonima tramite posta in cui non sia stato indicato alcun recapito a cui inviare ogni comunicazione necessaria);
b. mantiene le **interlocuzioni con il segnalante** e, se necessario, richiede a quest'ultimo **integrazioni**;
c. dà diligente **seguito alle segnalazioni ricevute**;
d. fornisce un **riscontro** alla segnalazione entro *tre mesi* dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro *tre mesi* dalla scadenza del termine di sette giorni dalla presentazione della segnalazione. Nei casi di particolare complessità, entro il suddetto termine il Responsabile *whistleblowing* informa il segnalante che l'istruttoria è ancora in corso.

Il Responsabile *whistleblowing* è altresì tenuto a dare notizia della segnalazione agli altri membri dell'Organismo di Vigilanza.

Con specifico riferimento al punto c), il Responsabile *whistleblowing* valuta, anche sulla base di eventuali analisi documentali, la sussistenza dei presupposti per l'avvio della successiva fase istruttoria, con conseguente:

- **avvio della fase istruttoria**, nel caso di ammissibilità della segnalazione;

- **chiusura della segnalazione**, nel caso di inammissibilità della segnalazione, con specifica indicazione del motivo.

Ai fini dell'**ammissibilità**, è necessario che nella segnalazione risultino chiare[10]:

- le *circostanze di tempo e di luogo* in cui si è verificato il fatto oggetto della segnalazione, tramite una descrizione dei fatti oggetto della segnalazione che contenga i dettagli relativi alle notizie circostanziali e, ove presenti, 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.

Al contrario, la segnalazione è ritenuta **inammissibile** in caso di:

- mancanza dei dati che costituiscono gli elementi essenziali della segnalazione;
- manifesta infondatezza degli elementi di fatto riconducibili alle violazioni tipizzate dal legislatore;
- esposizione di fatti di contenuto generico tali da non consentirne la comprensione al Responsabile *whistleblowing*;
- produzione di sola documentazione senza la segnalazione vera e propria di violazioni.

Nell'eventualità in cui il Responsabile *whistleblowing* decida di non dare avvio alla fase istruttoria, provvede ad informare il segnalante entro *tre mesi* dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro *tre mesi* dalla scadenza del termine di sette giorni dalla presentazione della segnalazione. Nel caso in cui il segnalante non sia contattabile a causa di segnalazione anonima, provvede ad archiviare la pratica.

Le segnalazioni chiuse in quanto palesemente infondate, anche se anonime, sono trasmesse al Responsabile HR ai fini dell'attivazione di ogni opportuna iniziativa, in particolare affinché valuti se le stesse siano state effettuate al solo scopo di ledere la reputazione ovvero di danneggiare o comunque di recare pregiudizio alla persona e/o alla Società segnalata.

Il Presidente informa inoltre immediatamente l'OdV affinché, nell'esercizio della sua attività di vigilanza, possa condividere le proprie eventuali osservazioni e partecipare all'istruttoria o comunque seguirne l'andamento.

Svolgimento dell'istruttoria

Nel corso della fase istruttoria il Responsabile *whistleblowing*:

- procede ad approfondimenti e analisi specifiche volte a verificare la ragionevole fondatezza della violazione segnalata;

[10] Secondo quanto previsto dalle Linee guida Confindustria adottate nell'ottobre 2023, i dati identificativi della persona segnalante e il recapito a cui comunicare i successivi aggiornamenti sono elementi essenziali affinché la segnalazione venga considerata e gestita come segnalazione *whistleblowing*.

- ricostruisce i processi gestionali e decisionali, seguiti sulla base della documentazione e di ulteriori elementi che ritenesse necessari;
- richiede eventuali integrazioni o chiarimenti al segnalante;
- acquisisce eventuali informazioni dalle strutture aziendali interessate e dalle persone coinvolte nella segnalazione, le quali possono chiedere di essere sentite nonché di produrre osservazioni scritte o documenti;
- acquisisce eventuali informazioni dalle persone coinvolte nella segnalazione, comprese le persone a cui la segnalazione attribuisce la responsabilità delle violazioni segnalate. Tali soggetti (*i*) devono essere coinvolti nel momento e secondo le modalità appropriate per garantire il corretto svolgimento dell'indagine, e (*ii*) hanno il diritto di essere ascoltati nonché di produrre osservazioni scritte o documenti. Nel caso in cui vengano sentiti oralmente, tali soggetti sono avvertiti del fatto che la conversazione verrà registrata ovvero riportata in apposito verbale, che il dichiarante avrà la possibilità di verificare, rettificare e accettare con sottoscrizione, senza tuttavia riceverne copia;
- elabora eventuali indicazioni circa l'adozione delle necessarie azioni di rimedio volte a correggere possibili carenze di controllo, anomalie o irregolarità rilevate sulle aree e sui processi aziendali esaminati.

Qualora per l'analisi e la corretta gestione della segnalazione dovessero risultare necessarie o anche solo opportune competenze tecniche non in possesso del Responsabile *whistleblowing*, quest'ultimo ha facoltà di farsi affiancare da consulenti esterni di comprovata esperienza e professionalità. Tali consulenti esterni, così come tutti i soggetti coinvolti nell'attività istruttoria, sono altresì tenuti, previo specifico avvertimento da parte del Responsabile *whistleblowing* ed eventuale sottoscrizione di appositi documenti, agli obblighi di riservatezza meglio dettagliati nel prosieguo.

In ogni caso, qualora risulti necessario avvalersi dell'assistenza tecnica di professionisti terzi, nonché del supporto specialistico del personale di altre funzioni aziendali il Responsabile *whistleblowing* è tenuto ad oscurare ogni tipologia di dato che possa consentire l'identificazione del segnalante o di ogni altra persona coinvolta, a meno che si tratti di dati necessari all'indagine condotta da tali soggetti.

Resta inteso che non rientrano nel perimetro di analisi dell'istruttoria, se non nei limiti della manifesta irragionevolezza, le valutazioni di merito o di opportunità, discrezionali o tecnico-discrezionali, degli aspetti decisionali e gestionali operate dalle varie funzioni aziendali.

Tutte le fasi dell'attività istruttoria devono essere tracciate e archiviate, a seconda della tipologia del canale di segnalazione utilizzato.

Chiusura dell'istruttoria

Conclusa l'istruttoria e presa una decisione sull'esito della stessa, **il segnalante è informato dell'esito dell'indagine ovvero della necessità di proseguire nell'attività di accertamento**. In quest'ultima ipotesi, il segnalante è successivamente informato dell'effettiva chiusura dell'indagine e del relativo esito.

Con specifico riferimento alla natura di tale informativa, il Responsabile *whistleblowing* indica al segnalante che la segnalazione (*a*) è stata archiviata in quanto ritenuta infondata; ovvero (*b*) è stata messa a conoscenza degli organi competenti della Società, unitamente a tutti gli elementi e le indicazioni ad essi necessari affinché siano presi gli opportuni provvedimenti.

Al Responsabile *whistleblowing* non compete infatti alcuna valutazione in ordine alle responsabilità individuali e agli eventuali successivi provvedimenti e/o procedimenti conseguenti.

A conclusione di ciascuna attività istruttoria, dopo aver dato seguito alla comunicazione al segnalante ed aver eventualmente interloquito con il soggetto segnalato ovvero valutato le osservazioni scritte presentate da quest'ultimo, **il Responsabile *whistleblowing* redige un report destinato al Consiglio di Amministrazione della Società e all'Organismo di Vigilanza** in cui sono riportati:

- la descrizione puntuale dei fatti segnalati e dei soggetti coinvolti;
- i fatti accertati a seguito delle attività di indagine e le modalità con cui è stata svolta l'istruttoria;
- le evidenze raccolte, ivi incluse le registrazioni delle audizioni, eventuali testimonianze raccolte per iscritto o i verbali delle audizioni nonché ogni altra documentazione rilevante;
- le conclusioni a cui è giunto all'esito delle attività istruttorie e pertanto (*a*) l'indicazione delle ipotesi di inosservanza di disposizioni, procedure o fatti di rilevanza sotto il profilo disciplinare o giuslavoristico, nonché (*b*) eventuali osservazioni e indicazioni in merito alle necessarie azioni correttive da intraprendere.

Non sono riportati i dati del segnalante o altri elementi che ne permetterebbero l'identificazione, salvo suo esplicito consenso.

Buona fede delle segnalazioni

Le segnalazioni devono essere fatte in buona fede.

I segnalanti in buona fede sono coloro che segnalano o rivelano violazioni con la ragionevole convinzione che le informazioni segnalate siano veritiere o che siano state fornite in conformità ai requisiti previsti dal D.Lgs. 24/2023 e dalla presente procedura.

Trasmissione della segnalazione

Chiunque riceva in qualsiasi forma una segnalazione che possa essere qualificata come *whisteblowing* (es. è esplicitata la dicitura "*whistleblowing*" sulla busta, nell'oggetto o nel testo della comunicazione) è tenuto a trasmettere al Responsabile *whistleblowing* l'originale, unitamente all'eventuale documentazione a supporto, entro *sette giorni* dalla

ricezione attraverso i canali di segnalazione sopra descritti e a dare contestuale notizia della trasmissione al segnalante, se conosciuto.

Al soggetto che riceve la segnalazione:

- è fatto divieto di trattenere copia cartacea della stessa;
- è fatto obbligo di eliminare eventuali copie digitali;
- è fatto divieto di intraprendere qualsiasi iniziativa autonoma di analisi o approfondimento della stessa;
- è fatto obbligo di mantenere la riservatezza dell'identità del segnalante, delle persone coinvolte o comunque menzionate nella segnalazione, del contenuto della segnalazione e della relativa documentazione.

La mancata comunicazione di una segnalazione nonché la violazione dell'obbligo di riservatezza potranno comportare l'adozione di provvedimenti disciplinari previste nel presente Modello.

Informazione e sensibilizzazione

Affinché sia garantito un corretto ed efficiente funzionamento del sistema di segnalazione è necessaria la promozione nella Società della cultura del *whistleblowing*.

A tal fine, la Società provvede, tramite idonea attività formativa, ad informare e sensibilizzare i dipendenti in merito al sistema di segnalazione adottato, definendo in modo semplice e comprensibile le finalità e le modalità di utilizzo del canale interno.

6.4. Canale di segnalazione esterna

Con riferimento alle sole violazioni del diritto UE e della normativa nazionale di recepimento[11], ai sensi dell'art. 6 del D.Lgs. 24/2023 il segnalante può effettuare altresì una segnalazione esterna attraverso l'apposito **canale attivato da ANAC** se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

a. non è prevista, nell'ambito del suo contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto dall'art. 4 del Decreto;
b. la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito[12];

[11] Per come indicata all'art. 2, comma 1, lett. a) nn. 3-6 del D.Lgs. 24/2023.

[12] Tale circostanza si verifica quando il soggetto cui è affidata la gestione del canale non abbia intrapreso entro i termini previsti dal Decreto alcuna attività circa l'ammissibilità della segnalazione, la verifica della sussistenza dei fatti segnalati o la comunicazione dell'esito dell'istruttoria svolta. Non sussiste pertanto un diritto del segnalante al buon esito della segnalazione, ma soltanto un diritto di essere informato sull'attività svolta.

c. la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito[13] ovvero che alla stessa segnalazione possa determinare il rischio di ritorsione[14], qualora si tratti di motivi fondati sulla base di circostanze concrete che devono essere allegate alla segnalazione e su informazioni effettivamente acquisibili;
d. la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse[15].

L'ANAC ha disciplinato nelle proprie Linee guida e in un 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;
b. oralmente, attraverso un ***servizio telefonico con operatore***;
c. tramite ***incontri diretti***, per cui è necessaria una richiesta motivata, fissati entro un termine ragionevole, cui consegue l'inserimento della segnalazione nella piattaforma da parte dell'operatore.

Ai fini dell'**ammissibilità** nella segnalazione devono essere indicati:

- la denominazione e i recapiti del segnalante;
- i fatti oggetto di segnalazione e l'ente in cui essi sono avvenuti;
- l'ente nel cui contesto lavorativo opera il segnalante e il profilo professionale da quest'ultimo rivestito;
- la descrizione sintetica delle modalità con cui il segnalante è venuto a conoscenza dei fatti segnalati.

La segnalazione esterna è considerata **inammissibile** per i seguenti motivi:

- manifesta infondatezza per l'assenza di elementi di fatto riconducibili alle violazioni tipizzate nell'art. 2, co. 1, lett. a), del Decreto;
- manifesta insussistenza dei presupposti di legge per l'esercizio dei poteri di vigilanza dell'Autorità;
- manifesta incompetenza dell'Autorità sulle questioni segnalate;

[13] Ad esempio per il rischio che le prove di condotte illecite possano essere occultate o distrutte o vi sia il timore di un accordo tra chi riceve la segnalazione e la persona coinvolta nella segnalazione, o ancora all'ipotesi in cui il gestore della segnalazione sia in conflitto di interessi.
[14] Ad esempio quando si siano già verificate situazioni ed eventi analoghi nell'ente.
[15] Ad esempio nel caso in cui la violazione richieda in modo evidente un intervento urgente da parte di un'Autorità pubblica per salvaguardare un interesse che fa capo alla collettività quale ad esempio la salute, la sicurezza o la protezione dell'ambiente.

- 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;
- produzione di sola documentazione in assenza della segnalazione esterna;
- mancanza dei dati che costituiscono elementi essenziali della segnalazione esterna; vii) sussistenza di violazioni di lieve entità.

Al fine di consentire l'accesso a tale modalità di segnalazione è pubblicato sul *sito web* della Società il *link* diretto alla pagina ANAC dedicata.

6.5. Divulgazione pubblica

Con riferimento alle sole violazioni del diritto UE e della normativa nazionale di recepimento[16], ai sensi dell'art. 15 del D.Lgs. 24/2023, il segnalante può inoltre ricorrere allo strumento della divulgazione pubblica, rendendo cioè di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone.

Il segnalante beneficia della protezione prevista dalla presente procedura se, al momento della divulgazione pubblica, ricorre una delle seguenti condizioni:

a. ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro nei termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
b. ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o 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 motivo deve essere fondato sulla base di circostanze concrete che devono essere allegate alla segnalazione e su informazioni effettivamente acquisibili;
c. ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

Ove il soggetto che effettua una divulgazione pubblica riveli la propria identità, non si pone un problema di tutela della riservatezza, ferma restando l'applicazione delle ulteriori tutele previste dal Decreto; qualora lo stesso ricorra a pseudonimo o *nickname*, l'ANAC tratterà la segnalazione alla stregua di una segnalazione anonima e avrà cura di

[16] Per come indicata all'art. 2, comma 1, lett. a) nn. 3-6 del D.Lgs. 24/2023.

registrarla, ai fini della conservazione, per garantire al divulgatore, in caso di disvelamento successivo dell'identità dello stesso e di effettive ritorsioni, le tutele previste.

6.6. Tutela della riservatezza e protezione dei dati personali

Il canale di segnalazione interna deve garantire la **riservatezza dell'identità del segnalante e delle eventuali altre persone coinvolte nella segnalazione**, nonché **del contenuto della segnalazione e della relativa documentazione**.

Qualsiasi trattamento dei dati personali deve essere effettuato nel rispetto del Regolamento (UE) 2016/679, del D.Lgs. 196/2003 e del D.Lgs. 51/2018. In ogni caso, la segnalazione è sottratta all'accesso previsto dagli artt. 22 e ss. della L. 241/1990, nonché dagli artt. 5 e ss. del D.Lgs. 33/2013.

Il trattamento dei dati personali sarà effettuato dal Responsabile *whistleblowing* in qualità di Titolare del trattamento ai soli fini di dare esecuzione alle procedure stabilite nel presente Modello e, dunque, per la corretta gestione delle segnalazioni ricevute.

Viene resa un'informativa sul trattamento dei dati personali pubblicata sul sito *internet* della Società.

Le segnalazioni non possono essere utilizzate oltre quanto strettamente necessario per dare seguito alle stesse. Per tale ragione, i dati personali manifestamente non utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

Il Responsabile *whistleblowing* vigila sul rispetto delle misure, di natura organizzativa e tecnica, finalizzate a garantire la riservatezza del segnalante e l'integrità e confidenzialità dei dati oggetto di segnalazione; garantisce altresì la sicurezza del canale di segnalazione in termini di confidenzialità, integrità e disponibilità delle informazioni, sia rispetto ai dati oggetto di segnalazione che rispetto all'identità del segnalante, anche nell'ipotesi in cui la segnalazione dovesse successivamente rivelarsi errata o infondata.

Non è tollerato alcun genere di minaccia, ritorsione, sanzione o discriminazione nei confronti del segnalante e del segnalato o di chi abbia collaborato alle attività di riscontro della fondatezza della segnalazione.

Fatti salvi gli obblighi di legge, l'identità del segnalante e qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente, l'identità dello stesso non possono essere rivelate, senza il suo consenso espresso, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli artt. 29 e 32, par. 4 del Regolamento (UE) 2016/679 e dell'art. 2 *quaterdecies* del D.Lgs. 196/2003.

Per il perseguimento di tali obiettivi, il Responsabile *whistleblowing* effettua con periodicità annuale attività di analisi dei rischi in materia di protezione dei dati personali, tenendo anche conto del limite temporale di *cinque anni*, decorrente dalla comunicazione dell'esito della procedura, per la conservazione dei dati oggetto di segnalazione.

L'identità del segnalante e ogni altra informazione da cui possa evincersi, direttamente o indirettamente, tale identità possono essere rivelate solo previo consenso espresso dello stesso:

- nell'ambito del procedimento disciplinare, qualora la contestazione appaia fondata sulla base della segnalazione e la conoscenza dell'identità del segnalante risulti indispensabile per la difesa dell'incolpato;
- nell'ambito del procedimento instaurato a seguito della segnalazione, qualora la rivelazione dell'identità del segnalante o di qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente, tale identità appaia indispensabile anche ai fini della difesa della persona coinvolta.

Le ragioni della rivelazione dei dati riservati vengono previamente comunicate per iscritto al segnalante. Qualora il segnalante neghi il proprio consenso, la segnalazione non può essere utilizzata nel procedimento disciplinare, che pertanto non può essere avviato o proseguito in assenza di elementi ulteriori sui quali fondare la contestazione.

In ogni caso, l'obbligo di tutela del segnalante può essere superato nel caso in cui:

- il segnalante presti il consenso espresso alla rivelazione della sua identità;
- l'identità del segnalante debba essere comunicata all'Autorità Giudiziaria, al Pubblico Ministero o ad altra autorità competente nell'ambito di un'indagine penale, disciplinare o di disciplina;
- sia stata accertata con sentenza di primo grado la responsabilità penale del segnalante per i reati di calunnia o diffamazione o comunque per reati commessi con la segnalazione, ovvero la sua responsabilità civile nei casi di dolo o colpa grave;
- l'anonimato non sia opponibile per legge e l'identità del segnalante sia richiesta dall'Autorità Giudiziaria.

La violazione dell'obbligo di riservatezza può comportare nei confronti dell'interessato l'irrogazione da parte di ANAC delle sanzioni amministrative pecuniarie[17], nonché l'adozione dei provvedimenti disciplinari previsti dal presente Modello.

[17] A tal fine, è istituito presso ANAC l'elenco degli enti del Terzo Settore che forniscono alle persone segnalanti misure di sostegno, pubblicato sul sito istituzionale. Tali misure di sostegno consistono in informazioni, assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni, sui diritti della persona coinvolta e sulle modalità e condizioni di accesso al patrocinio a spese dello Stato.

6.7. Divieto di ritorsione

Nei confronti del segnalante è vietato il compimento di atti ritorsivi, da intendersi come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione interna che provoca o può provocare al segnalante, in via diretta o indiretta, un danno ingiusto.

Il divieto di ritorsioni a danno del segnalante comprende una serie di casi, tra cui a mero titolo esemplificativo e non esaustivo:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- 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;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- 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;
- 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;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

La Società adotta le opportune azioni contro chiunque ponga in essere o minacci di porre in essere atti di ritorsione contro coloro che abbiano presentato segnalazioni in conformità alle prescrizioni indicate nel presente Modello, fatto salvo il diritto degli aventi causa di tutelarsi legalmente qualora siano state riscontrate in capo al segnalante responsabilità di natura penale o civile legate alla falsità di quanto dichiarato o riportato.

Gli atti ritorsivi eventualmente assunti in ragione della segnalazione sono nulli e le persone che sono state licenziate a causa della segnalazione hanno diritto ad essere reintegrate nel posto di lavoro.

L'ANAC è l'autorità preposta a ricevere dal segnalante e gestire le comunicazioni su presunte ritorsioni dallo stesso subite[18].

Affinché sia riconosciuta tale forma di tutela:

- il segnalante, al momento della segnalazione, della denuncia all'autorità giudiziaria o contabile ovvero della divulgazione pubblica, deve aver fondato motivo di ritenere le informazioni veritiere e rientranti nel perimetro applicativo della disciplina;
- la segnalazione, denuncia o divulgazione deve essere stata effettuata secondo la disciplina prevista dal D.Lgs. 24/2023 e dalla presente Procedura.

Eventuali ritorsioni derivanti dalla segnalazione costituiscono una violazione molto grave che può comportare l'irrogazione da parte di ANAC di sanzioni amministrative pecuniarie a carico della Società da 10.000 a 50.000 euro.

Ferma restando l'esclusiva competenza di ANAC in merito all'eventuale applicazione delle sanzioni amministrative di cui all'art. 21 del D.Lgs. 24/2023, la Società può intraprendere le più opportune misure disciplinari e/o legali a tutela dei propri diritti, beni e della propria immagine, nei confronti di chiunque in malafede abbia effettuato segnalazioni false infondate o opportunistiche e al solo scopo di diffamare o arrecare pregiudizio al segnalato o ad altri soggetti citati nella segnalazione.

Rimane invece di competenza dell'Autorità giudiziaria disporre le misure necessarie ad assicurare la tutela del segnalante (es. reintegrazione nel posto di lavoro, risarcimento del danno, l'ordine di cessazione della condotta, nonché la dichiarazione di nullità degli atti adottati).

Come già precisato, il segnalante perde la protezione:

- 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;

[18] Nei procedimenti dinanzi ad ANAC, l'intento ritorsivo si presume. Opera infatti un'inversione dell'onere probatorio e, pertanto, laddove il segnalante 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. Quest'ultima dovrà dimostrare che la presunta ritorsione non è connessa alla segnalazione/denuncia ma dipende da ragioni estranee rispetto alla stessa. La 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. Analogo regime probatorio si applica anche nei procedimenti giudiziari, amministrativi e nelle controversie stragiudiziali aventi a oggetto l'accertamento dei comportamenti vietati, nei quali si presume che la ritorsione sia conseguenza della segnalazione e spetta al datore di lavoro fornire la prova che gli atti ritorsivi non sono conseguenza della segnalazione effettuata dal lavoratore ma sono riconducibili a ragioni estranee.

- in caso di responsabilità civile per lo stesso titolo per dolo o colpa grave.

In queste ipotesi al segnalante viene irrogata una sanzione disciplinare.

La tutela, ancorché tardiva, deve comunque essere applicata anche in caso di sentenza di primo grado non confermata nei successivi gradi di giudizio, di archiviazione e di accertata colpa lieve.

6.8. Limitazioni di responsabilità

Secondo quanto previsto dal D.Lgs. 24/2023, il segnalante non può essere chiamato a rispondere né penalmente, né in sede civile e amministrativa:

- di rivelazione e utilizzazione del segreto d'ufficio (art. 326 c.p.);
- di rivelazione del segreto professionale (art. 622 c.p.);
- di rivelazione dei segreti scientifici e industriali (art. 623 c.p.);
- di violazione del dovere di fedeltà e di lealtà (art. 2105 c.c.);
- di violazione delle disposizioni relative alla tutela del diritto d'autore;
- di violazione delle disposizioni relative alla protezione dei dati personali;
- di rivelazione o diffusione di informazioni sulle violazioni che offendono la reputazione della persona coinvolta.

Le suddette limitazioni di responsabilità operano solamente nel caso in cui:

- 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;
- la segnalazione sia effettuata nel rispetto delle condizioni previste per beneficiare della tutela contro le ritorsioni (fondati motivi per ritenere veritieri i fatti segnalati, la violazione sia tra quelle segnalabili e siano rispettate le modalità e le condizioni di accesso alla segnalazione).

In ogni caso, 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.

Ove l'acquisizione si configuri come un reato (es. accesso abusivo a un sistema informatico o atto di pirateria informatica) resta ferma la responsabilità penale e ogni altra responsabilità civile, amministrativa e disciplinare del segnalante. Non risulta viceversa punibile, ad esempio, l'estrazione (per copia, fotografia, asporto) di documenti cui si aveva lecitamente accesso.

6.9. Sistema sanzionatorio

Il sistema disciplinare previsto dal presente Modello si applica anche nei confronti dei responsabili di ritorsione, ostacolo (anche solo tentato) alla segnalazione, violazione dei doveri di riservatezza, mancata istituzione dei canali di segnalazione, adozione di procedure di segnalazione non conformi alle previsioni del D.Lgs. 24/2023 (*infra* paragrafo 7).

Ci si riferisce, in particolare, a:

i. 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. 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 individuato nel **Responsabile *whistleblowing***.

La gestione delle segnalazioni rientra nelle prerogative riconducibili allo svolgimento dell'attività lavorativa del Responsabile *whistleblowing*. Eventuali inadempimenti prevedono pertanto l'applicazione delle sanzioni sancite da Contratto Collettivo Nazionale, se e in quanto applicabile.

Con riferimento, invece, all'ipotesi della sanzione verso **chi ha adottato un atto ritorsivo**, è sanzionata la **persona fisica individuata come responsabile delle ritorsioni**.

Il segnalante può altresì comunicare ad ANAC le ritorsioni che ritiene di avere subito e quest'ultima, nei casi indicati ai punti precedenti, è tenuta ad applicare al responsabile le seguenti **sanzioni amministrative pecuniarie**:

- da 10.000 a 50.000 euro, quando accerta che sono state commesse ritorsioni, che la segnalazione è stata ostacolata o che si è tentato di ostacolarla ovvero che è stato violato l'obbligo di riservatezza;
- da 10.000 a 50.000 euro, quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme alla normativa vigente, nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute;
- da 500 a 2.500 euro, nei casi di cui all'art. 16, comma 3 del D.Lgs. 24/2023, salvo che la persona segnalante sia stata 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 o contabile.

7. SELEZIONE, INFORMAZIONE E FORMAZIONE DEL PERSONALE

7.1. Selezione del personale

La scelta e la gestione del personale dipendente, così come dei fornitori e dei *partner* commerciali di Techbau s.p.a., deve rispondere a criteri di ragionevolezza, professionalità, integrità, correttezza e trasparenza, secondo quanto previsto dal Codice etico della Società e tenendo conto delle esigenze aziendali in relazione all'applicazione del D.Lgs. 231/2001.

L'OdV, in coordinamento con le funzioni aziendali interessate, analizza lo specifico sistema di valutazione dei canditati in fase di selezione predisposto dalla Società sulla base delle esigenze aziendali e nel rispetto di quanto previsto all'interno del D.Lgs. 231/2001.

7.2. Informazione del personale

Ai fini dell'efficacia del presente Modello, è obiettivo della Società garantire corretta divulgazione e conoscenza delle regole di condotta ivi contenute nei confronti delle risorse già presenti in azienda e di quelle da inserire, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle attività sensibili.
Il sistema di informazione e formazione continua è curato dalle funzioni QHSE e HR.
Sono garantite la diffusione e la conoscenza del sistema di gestione (comprensivo di procedure, istruzioni operative, policy ecc.) predisposto e adottato da Techbau s.p.a. nell'interesse del personale aziendale tramite archiviazione sul server aziendale e comunicazione via e-mail ogniqualvolta si proceda all'emissione di un nuovo documento o all'aggiornamento di un documento esistente.

Il predetto sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'Organismo di Vigilanza che sovrintende all'attività operando in collaborazione con le funzioni aziendali e con i responsabili delle funzioni di volta in volta coinvolte nell'applicazione del Modello.

Il presente Modello è comunicato a tutto il personale aziendale al momento dell'adozione. Il documento integrale è caricato nell'intranet aziendale, mentre la sola Parte Generale è pubblicata sul sito internet della Società nella sezione dedicata (www.techbau.it).

Il Modello sarà oggetto dell'attività di formazione descritta nel paragrafo successivo.

7.3. Formazione del personale

L'attività di formazione, finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001, è differenziata nei contenuti e nelle modalità di erogazione in funzione della qualifica dei destinatari, dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della Società.

È compito delle varie funzioni aziendali:

- provvedere alla definizione di un programma periodico di aggiornamento da condividere con l'OdV di Techbau s.p.a., che preveda, in conformità a quanto indicato nel Modello, un percorso specifico per il personale direttivo e per il personale subordinato;
- predisporre un calendario da comunicare, unitamente al contenuto sintetico del programma, all'OdV.

Sarà di converso cura dell'OdV informare le varie funzioni aziendali in merito a:

- modificazioni della normativa di riferimento in grado di prevedere momenti formativi integrativi;
- necessità di azioni formative integrative conseguenti la rilevazione di errori o devianze dalla corretta esecuzione di procedure operative applicate alle c.d. "attività sensibili".

8. SISTEMA DISCIPLINARE

8.1. Principi generali

Ai sensi degli artt. 6, comma 2, lett. e) e 7, comma 4, lett. b) del D.Lgs. 231/2001, i Modelli di organizzazione, gestione e controllo, la cui adozione ed efficace attuazione (unitamente alle altre situazioni previste dai predetti articoli 6 e 7) costituisce condizione *sine qua non* per l'esenzione di responsabilità della Società in caso di commissione dei reati di cui al Decreto, possono ritenersi efficacemente attuati solo se prevedono un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure in essi indicate.

Tale sistema disciplinare deve rivolgersi tanto ai lavoratori dipendenti quanto ai terzi che operino per conto della o con la Società, prevedendo idonee sanzioni di carattere disciplinare, da un lato, e di carattere negoziale, dall'altro lato.

L'applicazione delle sanzioni disciplinari prescinde dall'avvio o dall'esito di un eventuale procedimento penale, in quanto i Modelli di organizzazione e le procedure interne costituiscono regole vincolanti per i destinatari, la violazione delle quali deve, al fine di ottemperare ai dettami del citato Decreto, essere sanzionata indipendentemente dall'effettiva commissione di un reato o dalla punibilità dello stesso. I principi di tempestività e immediatezza della sanzione rendono non solo non doveroso, ma anche sconsigliabile ritardare l'applicazione della sanzione disciplinare in attesa del giudizio penale.

8.2. Sanzioni nei confronti dei dipendenti e dei dirigenti

Il presente Modello costituisce a tutti gli effetti un regolamento aziendale, quale espressione del potere del datore di lavoro di impartire disposizioni per l'esecuzione e per la disciplina del lavoro e, in quanto disponibile in luogo accessibile a tutti, costituirà altresì codice disciplinare di Techbau s.p.a.. Il codice disciplinare della Società, adottato in conformità alle vigenti previsioni di legge (tra cui R.D. 8 gennaio 1931, n. 148) e della contrattazione nazionale e territoriale di settore, è integrato sulla base della previsione esposta nel seguito.

I soggetti cui pertanto il presente regolamento è diretto sono obbligati ad adempiere a tutte le obbligazioni e prescrizioni ivi contenute ed uniformare il proprio comportamento alla condotta ivi descritta.

Costituisce illecito disciplinare del dipendente o del dirigente della Società:

a. la mancata, incompleta o non veritiera documentazione dell'attività svolta, così come prescritta, in particolare, per le attività sensibili;
b. la mancata attività di documentazione, conservazione e controllo degli atti e delle attività previste dai Protocolli di controllo con la finalità di impedire la trasparenza e la verificabilità delle stesse attività;
c. l'ostacolo ai controlli, l'impedimento ingiustificato all'accesso alle informazioni ed alla documentazione opposto ai soggetti preposti ai controlli delle procedure e delle decisioni, incluso l'Organismo di Vigilanza, o altre condotte

idonee alla violazione o elusione del sistema di controllo, quali la distruzione o l'alterazione della documentazione prevista dal Modello;

d. l'omissione o la violazione, anche isolata, dei protocolli e delle prescrizioni del Modello finalizzati a garantire la sicurezza e la salute sul posto di lavoro;
e. la violazione ripetuta e ingiustificata di altri protocolli del Modello (ad esempio la non osservanza delle procedure prescritte, l'omissione di comunicazione all'OdV delle informazioni richieste, l'omissione nello svolgimento dei controlli, l'adozione di un comportamento non conforme alle prescrizioni del Modello stesso);
f. la violazione dei doveri di riservatezza, mancata istituzione dei canali di segnalazione, adozione di procedure di segnalazione non conformi alle previsioni del Decreto, l'integrazione di condotte ritorsive nei confronti dei segnalanti o di ostacolo (anche solo tentato) alla segnalazione (su cui *infra*).

La sanzione disciplinare, graduata in ragione della gravità della violazione, è applicata al dipendente o al dirigente, anche su segnalazione e richiesta dell'Organismo di Vigilanza, nel rispetto della vigente normativa di legge e di contratto.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate deve tener conto dei principi di proporzionalità e di adeguatezza rispetto alla violazione contestata; tali sanzioni saranno quindi applicate in relazione:

- all'intenzionalità del comportamento (in caso di dolo) o al grado di negligenza, imprudenza o imperizia con riguardo alla prevedibilità dell'evento (in caso di colpa);
- alla rilevanza degli obblighi violati;
- al comportamento complessivo del lavoratore, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- al livello di responsabilità gerarchica e/o tecnica delle persone coinvolte nei fatti censurati;
- alle conseguenze reali o potenziali in capo alla Società;
- alle altre particolari circostanze che accompagnano la violazione disciplinare;
- alla effettiva commissione di un reato doloso o colposo come conseguenza della violazione di un protocollo o di una procedura.

Ai fini dell'eventuale aggravamento (o attenuazione) della sanzione, sono inoltre considerati i seguenti elementi:

- professionalità, precedenti prestazioni lavorative, precedenti disciplinari, circostanze in cui è stato commesso il fatto;
- comportamento immediatamente susseguente al fatto, con particolare riferimento all'eventuale ravvedimento operoso;
- eventuale commissione di più violazioni nell'ambito della medesima condotta, nel qual caso sarà applicata la sanzione prevista per la violazione più grave;
- eventuale concorso di più soggetti nella commissione della violazione;
- eventuale recidiva del suo autore.

L'applicazione delle sanzioni indicate nei punti seguenti non pregiudica in ogni caso il diritto della Società di agire nei confronti del soggetto responsabile al fine di ottenere il risarcimento di tutti i danni patiti a causa o in conseguenza della condotta accertata.

L'applicazione da parte della Società delle sanzioni disciplinari avverrà nel rispetto delle procedure previste dall'articolo 7 della Legge 30 maggio 1970, n. 300 (c.d. Statuto dei Lavoratori) ed eventuali normative speciali: si tratta delle sanzioni previste dall'apparato sanzionatorio di cui al vigente CCNL di riferimento.

A titolo esemplificativo:

2. incorrerà nel provvedimento del **richiamo verbale** o **ammonizione scritta** il lavoratore che ponga in essere azioni od omissioni di lieve entità disattendendo le procedure interne previste dal presente Modello (ad esempio che non osservi le procedure prescritte, ometta di dare comunicazione all'OdV delle informazioni prescritte, ometta di svolgere la propria funzione di controllo, anche su soggetti sottoposti alla sua direzione ecc.) o adotti, nell'espletamento di attività nelle aree sensibili, un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una violazione delle prescrizioni comunicate dalla Società;

3. potrà essere inflitto il provvedimento della **multa** al lavoratore che disattenda più volte le procedure interne previste dal presente Modello o adotti, nell'espletamento di attività nelle aree sensibili, un comportamento più volte non conforme alle prescrizioni del Modello stesso, prima ancora che dette mancanze siano state singolarmente accertate e contestate, dovendosi ravvisare in tali comportamenti la ripetuta disapplicazione delle prescrizioni comunicate dalla Società;

4. incorrerà nel provvedimento della **sospensione dal servizio e dalla retribuzione** il lavoratore che nel disattendere le procedure interne previste dal presente Modello o adottando, nell'espletamento di attività nelle aree sensibili, un comportamento non conforme alle prescrizioni del Modello stesso, compia atti che espongano la Società ad una situazione oggettiva di pericolo ovvero atti contrari all'interesse della Società che arrechino danno, dovendosi ravvisare in tali comportamenti la determinazione di un danno o di una situazione di pericolo per l'integrità dei beni dell'azienda o il compimento di atti contrari ai suoi interessi parimenti derivanti dall'inosservanza delle prescrizioni comunicate dalla Società;

5. sarà inflitto il provvedimento del **licenziamento con indennità sostitutiva del preavviso** al lavoratore che adotti, nell'espletamento delle attività nelle aree sensibili un comportamento non conforme alle prescrizioni del presente Modello e che determini la realizzazione di un reato previsto dal Decreto, dovendosi ravvisare in tale comportamento un danno notevole o una situazione di notevole pregiudizio;

6. potrà incorrere nel provvedimento del **licenziamento senza preavviso** il lavoratore che adotti, nell'espletamento delle attività nelle aree sensibili, un comportamento palesemente in violazione alle prescrizioni del presente Modello e tale da determinare la concreta applicazione a carico della Società di misure previste dal Decreto, dovendosi ravvisare in tale comportamento il compimento di atti tali da far venir meno radicalmente la fiducia della società nei suoi confronti, ovvero il verificarsi delle mancanze richiamate ai punti precedenti con la determinazione di un grave pregiudizio per l'azienda.

8.3. Misure nei confronti dei collaboratori, fornitori, partner commerciali e consulenti

Ogni comportamento posto in essere dai collaboratori, dai fornitori, dai *partner* commerciali e consulenti della Società in violazione delle previsioni di cui al Decreto o al Codice etico, potrà determinare l'applicazione di penali o, nel caso di grave inadempimento, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla Società, anche indipendentemente dalla predetta risoluzione del rapporto.

A tal fine è previsto che i contratti stipulati dalla Società con terzi contengano il richiamo esplicito dell'esistenza del Modello e del Codice etico e l'inserimento di specifiche clausole che diano atto della conoscenza del Modello, del Codice etico e del Decreto da parte del terzo contraente. Occorrerà inoltre un'esplicita assunzione di impegno da parte di quest'ultimo – e da parte dei dipendenti e dei collaboratori di questo – ad astenersi da comportamenti idonei a configurare le ipotesi di reato di cui al Decreto e ad adottare idonei sistemi di controllo, a prescindere dall'effettiva consumazione del reato e dalla sua punibilità. Tali clausole dovranno poi necessariamente disciplinare le conseguenze in caso di violazione delle previsioni ivi contenute, tra le quali, ad esempio, la possibilità per la Società di risolvere il rapporto in conseguenza di eventuali inadempimenti da parte dei predetti soggetti alle prescrizioni dello stesso Modello o del Codice etico.

8.4. Misure nei confronti degli Amministratori, del Collegio Sindacale e dei Revisori

Le violazioni rilevanti delle pertinenti prescrizioni del Modello commesse da persone che rivestono, o che di fatto esercitano, funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, o che esercitano funzioni di controllo o di revisione legale della Società, sono segnalate dall'Organismo di Vigilanza, al Consiglio di Amministrazione per le determinazioni del caso e, per conoscenza, al Collegio Sindacale o ad organo equivalente, ove esistente.

L'organo deputato all'individuazione e irrogazione della sanzione da applicare agli amministratori è l'Assemblea, in base al principio di proporzionalità.

Nei casi più gravi e quando la violazione sia tale da ledere il rapporto di fiducia con la Società, l'Assemblea può disporre quale sanzione la revoca dalla carica.

Si considerano altresì violazioni rilevanti delle prescrizioni del Modello la violazione dei doveri di riservatezza, mancata istituzione dei canali di segnalazione, adozione di procedure di segnalazione non conformi alle previsioni del decreto, l'integrazione di condotte ritorsive nei confronti dei segnalanti o di ostacolo (anche solo tentato) alla segnalazione.