MI.ZAR. SRL

Via Gaetano Zompini 24 – 31056 Roncade (TV) – ITALY

MODELLO DI ORGANIZZAZIONE,

GESTIONE E CONTROLLO

Conforme al Decreto Legislativo 8 giugno 2001, n. 231

Approvato dall'Organo Amministrativo il 14/08/2026

Indice delle revisioni

Data Revisione	Motivo Revisione
14/04/2020	Prima emissione
05/08/2020	Nuovi reati di luglio 2020 e certificazione ISO9001 (§2.1.5)
21/12/2021	Nuovo art. 25-octies.1(§8), certificazione ISO45001 (§2.1.6), nuovo statuto (§2.1.2)
01/04/2022	Nuovi art. 25-septiesdecies (§17) e 25-duodevicies (§12)
15/12/2023	Aggiornamenti sul Whistleblowing introdotti dalla legge 10 marzo 2023 n° 24 (§2.6)
29/01/2025	Aggiornamento dei reati informatici
03/10/2025	Aggiornamento per legge 132/2025 su intelligenza artificiale
14/08/2026	Aggiornamento nuovi reati
31/10/2026	Aggiornamento per nuovi reati 25-vicies

INDICE

..... 1
PARTE GENERALE 7
1. Una peculiare forma di responsabilità: la responsabilità "amministrativa da reato" degli enti. 8
1.1. Premessa 8
1.2. I presupposti della responsabilità dell'Ente 8
1.2.1. I destinatari del Decreto 9
1.2.2. Le fattispecie di reato 9
1.2.3. Responsabilità dell'Ente e funzione esimente del Modello 19
1.3. Le sanzioni 21
1.3.1. La sanzione pecuniaria 21
1.3.2. Le sanzioni interdittive 22
1.3.3. La pubblicazione della sentenza di condanna 23
1.3.4. La confisca 23
2. Adozione del Modello da parte di MI.ZAR. SRL 23
2.1. Struttura della società 23
2.1.1. MI.ZAR. SRL e la sua *mission* 23
2.1.2. Oggetto sociale 24
2.1.3. Organigramma aziendale 24
2.1.4. Governo societario: organo amministrativo 24
2.1.5. Certificazione ISO9001 25
2.1.6. Certificazione ISO45001 25
2.2. Struttura e scopo del Modello 25
2.3. Approccio metodologico al modello 27
2.4. Destinatari del Modello 29
2.5. Approvazione, modifiche ed integrazioni del Modello 29
2.6. Il sistema di whistleblowing e il Dlgs n° 24/2023 30
2.7. Intelligenza artificiale: legge 132/2025 31
2.7.1. Nuovi reati-presupposto 32
2.7.2. Valutazione dei rischi 32
2.7.3. Regole di comportamento e controlli 33
2.7.4. Responsabilità e vigilanza 33
2.7.5. Formazione e aggiornamento 33
3. Organismo di Vigilanza 34

3.1. Composizione e requisiti ... 34
3.2. Funzioni e poteri dell'Organismo di Vigilanza ... 36
3.3. Flussi informativi provenienti dall'Organismo di Vigilanza ... 37
3.4. Flussi informativi verso l'Organismo di Vigilanza ... 38
3.5. Informazioni obbligatorie e deleghe ... 38
3.6. Il sistema di whistleblowing ... 39
4. Formazione ed informativa ... 39
4.1. Formazione ed informativa al personale ... 39
4.2. Informativa ai soggetti esterni ed ai consulenti ... 40
5. Sistema Disciplinare ... 40
5.1. Principi generali ... 40
5.2. Misure per i lavoratori dipendenti ... 41
5.3. Misure nei confronti di dirigenti e di amministratori ... 41
5.4. Misure nei confronti di collaboratori, consulenti e altri terzi ... 41
5.5. Sistema disciplinare ... 41
6. Modello e Codice Etico ... 42
7. Allegati richiamati in questo documento ... 42
PARTE SPECIALE ... 43
1. I Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto) ... 44
1.1. I reati ... 44
1.2. Aree a rischio ... 44
1.3. Divieti ... 45
1.4. Procedure specifiche per aree sensibili ... 46
1.5. Presidi adottati ... 47
2. I Delitti informatici e trattamento illecito di dati (art. 24 bis) ... 48
2.1. I reati ... 48
2.2. Aree a rischio ... 48
2.3. Divieti ... 48
2.4. Procedure specifiche per aree sensibili ... 49
2.5. Presidi adottati ... 50
3. Delitti di criminalità organizzata (art. 24 ter) ... 51
3.1. I reati ... 51
3.2. Aree a rischio ... 51
3.3. Divieti ... 51
3.4. Procedure specifiche per aree sensibili ... 52

3.5. Presidi adottati ... 52
4. Delitti contro l'industria e il commercio (art. 25 bis 1) ... 53
4.1. I reati ... 53
4.2. Aree a rischio ... 53
4.3. Divieti ... 53
4.4. Procedure specifiche per aree sensibili ... 54
4.5. Presidi adottati ... 54
5. Reati societari (art. 25 ter) ... 55
5.1. I reati ... 55
5.2. Aree a rischio ... 56
5.3. Divieti ... 57
5.4. Procedure specifiche per aree sensibili ... 58
5.5. Presidi adottati ... 60
6. Reati in materia di sicurezza e salute sul lavoro (art. 25 septies) ... 61
6.1. I reati ... 61
6.2. Aree a rischio ... 61
6.3. Divieti ... 61
6.4. Procedure specifiche per aree sensibili ... 62
6.5. Presidi adottati ... 63
7. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25 octies) ... 64
7.1. I reati ... 64
7.2. Aree a rischio ... 65
7.3. Divieti ... 65
7.4. Procedure specifiche per aree sensibili ... 66
7.5. Presidi adottati ... 67
8. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1) ... 68
8.1. I reati ... 68
8.2. Aree a rischio ... 68
8.3. Divieti ... 68
8.4. Procedure specifiche per aree sensibili ... 69
8.5. Presidi adottati ... 70
9. Delitti in materia di violazione del diritto d'autore (art. 25 novies) ... 70
9.1. I reati ... 70
9.2. Aree a rischio ... 71

9.3. Divieti ... 71
9.4. Procedure specifiche per aree sensibili ... 72
9.5. Presidi adottati ... 73
10. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies) ... 74
10.1. I reati ... 74
10.2. Aree a rischio ... 74
10.3. Divieti ... 74
10.4. Procedure specifiche per aree sensibili ... 74
10.5. Presidi adottati ... 75
11. REATI AMBIENTALI (art. 25 undecies) ... 76
11.1. I reati ... 76
11.2. Aree a rischio ... 76
11.3. Divieti ... 77
11.4. Procedure specifiche per aree sensibili ... 77
11.5. Presidi adottati ... 77
12. Reato di impiego di lavoratori irregolari (art. 25-duodecies) ... 78
12.1. I reati ... 78
12.2. Aree a rischio ... 78
12.3. Divieti ... 78
12.4. Procedure specifiche per aree sensibili ... 78
12.5. Presidi adottati ... 79
13. Reato di razzismo e xenofobia (art. 25 terdecies) ... 80
13.1. I reati ... 80
13.2. Aree a rischio ... 80
13.3. Divieti ... 80
13.4. Procedure specifiche per aree sensibili ... 80
13.5. Presidi adottati ... 81
14. FRODE IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O DI SCOMMESSA E GIOCHI D'AZZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI" (art. 25 quaterdecies) ... 82
14.1. I reati ... 82
14.2. Aree a rischio ... 82
14.3. Divieti ... 82
14.4. Procedure specifiche per aree sensibili ... 82
14.5. Presidi adottati ... 82

15. REATI TRIBUTARI (art. 25 quinquiesdecies) 83
15.1. I reati 83
15.2. Aree a rischio 83
15.3. Divieti 84
15.4. Procedure specifiche per aree sensibili 84
15.5. Flussi informativi verso l'Organismo di Vigilanza 84
15.6. Presidi adottati 84
16. REATI CONTRABBANDO (art. 25 sexiesdecies) 86
16.1. I reati 86
16.2. Aree a rischio 86
16.3. Divieti 86
16.4. Procedure specifiche per aree sensibili 86
16.5. Flussi informativi verso l'Organismo di Vigilanza 87
16.6. Presidi adottati 87
17. DELITTI CONTRO IL PATRIMONIO CULTURALE (art. 25 septiesdecies.) 88
17.1. I reati 88
17.2. Aree a rischio 89
17.3. Divieti 89
17.4. Procedure specifiche per aree sensibili 89
17.5. Flussi informativi verso l'Organismo di Vigilanza 89
17.6. Presidi adottati 89
18. RICICLAGGIO DI BENI CULTURALI E DEVASTAZIONE E SACCHEGGIO DI BENI CULTURALI E PAESAGGISTICI (art. 25 duodevicies) 90
18.1. I reati 90
18.2. Aree a rischio 90
18.3. Divieti 90
18.4. Procedure specifiche per aree sensibili 90
18.5. Flussi informativi verso l'Organismo di Vigilanza 90
18.6. Presidi adottati 90
19. Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25-octies.2) 91
19.1. I reati 91
19.2. Aree a rischio 91
19.3. Divieti 91
19.4. Procedure specifiche per aree sensibili 91
19.5. Flussi informativi verso l'Organismo di Vigilanza 92

19.6. Presidi adottati 92
20. Delitti contro gli animali (art. 25-undevicies) 93
20.1. I reati 93
20.2. Aree a rischio 93
20.3. Divieti 93
20.4. Procedure specifiche per aree sensibili 93
20.5. Flussi informativi verso l'Organismo di Vigilanza 93
20.6. Presidi adottati 93
21. REATI COMMESSI CON L'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE (art. 25-vicies del D.Lgs. 231/2001) 94
21.1. I reati 94
21.2. Aree a rischio 95
21.3. Divieti 96
21.4. Procedure specifiche per aree sensibili 97
21.5. Flussi informativi verso l'Organismo di Vigilanza 98
21.6. Presidi adottati 99

PARTE GENERALE

1. Una peculiare forma di responsabilità: la responsabilità "amministrativa da reato" degli enti.

1.1. Premessa

Il D. Lgs. 8 giugno 2001, n. 231 rubricato "*Disciplina della responsibilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300*" (di seguito D. Lgs. n. 231 del 2001) costituisce l'attuazione di impegni assunti dall'Italia a livello comunitario ed internazionale, introducendo nell'ordinamento italiano una peculiare forma di **responsabilità (nominalmente amministrativa ma, sostanzialmente, di carattere penale: la c.d. responsabilità amministrativa da reato) a carico di società, associazioni ed enti in genere, con conseguente abbandono della concezione rigorosamente personalistica della responsabilità penale e, quindi, dell'antico broccardo secondo cui *societas delinquere non potest*. Molti episodi criminali, infatti, (ad es. reati ambientali, finanziari, tributari...) traggono origine da attività imprenditoriali svolte attraverso lo strumento di persone giuridiche, specialmente società commerciali**: poiché il tratto comune di questa forma di criminalità è rappresentato proprio dal fatto che **soggetto attivo del reato è l'ente**, è evidente come, in una simile realtà, la concezione personalistica della pena si sia rivelata sempre più inadeguata ed insufficiente e la conseguenza necessitata di tale condizione delle cose è stata appunto la responsabilità (amministrativa da reato/*ex crimine*/parapenale) degli enti *ex* d. lgs. 231 del 2001.

La responsabilità dell'ente quale si delinea per mezzo del d. lgs. n. 231 del 2001 non sostituisce bensì si aggiunge a quella della persona fisica che ha materialmente posto in essere la condotta costituente reato, sicché sorgerà un duplice profilo di responsabilità: alle conseguenze penali ascrivibili all'autore dell'illecito si aggiungerà una sanzione, gravante sull'ente, di tipo pecuniario o interdittivo. Il procedimento di accertamento ed irrogazione delle sanzioni rispecchia nei suoi tratti essenziali il processo penale vigente, anche in forza del rinvio al Codice di Procedura Penale contenuto all'articolo 34 del Decreto.

1.2. I presupposti della responsabilità dell'Ente

I presupposti applicativi della responsabilità dell'Ente – che verranno di seguito analizzati – possono essere così sintetizzati.

a. L'Ente deve rientrare nel novero di quelli rispetto ai quali il Decreto trova applicazione (art. 1).
b. Per il principio di legalità, la responsabilità dell'Ente sussiste solo per l'avvenuta commissione di un reato compreso tra quelli elencati dallo stesso Decreto (art. 2).
c. La responsabilità sussite solo se il reato è stato commesso da un soggetto funzionalmente legato all'Ente e nell'interesse e/o a vantaggio dell'Ente medesimo (art. 5).

d. Mancata adozione o attuazione da parte dell'Ente di un Modello di Organizzazione e Gestione (di seguito "Modello") idoneo a prevenire la commissione di reati del tipo di quello verificatosi.
e. Mancato affidamento di autonomi poteri di iniziativa e controllo ad un apposito organismo dell'Ente detto Organismo di Vigilanza (o l'insufficiente vigilanza da parte di quest'ultimo) e l'elusione fraudolenta da parte del soggetto del Modello.

1.2.1. I destinatari del Decreto

Primo presupposto per la responsabilità dell'Ente è, dunque, che lo stesso rientri nel novero dei possibili destinatari indicati dal Decreto. A tal proposito, l'art. 1 indica come soggetti destinatari dell'applicazione del d. lgs. n. 231 del 2001 "*gli enti forniti di personalità giuridica, le società e le associazioni anche prive di personalità giuridica*" e precisa che lo stesso non si applica "allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici, nonché agli Enti che svolgono funzioni di rilievo costituzionale".

1.2.2. Le fattispecie di reato

In applicazione del principio di legalità di cui all'art. 2 del Decreto, l'Ente può essere ritenuto responsabile per un fatto costituente reato solo se la sua responsabilità amministrativa per quel reato e le relative sanzioni sono previste da una legge entrata in vigore prima della commissione del fatto.
A far data dall'entrata in vigore del Decreto, il novero dei reati-presupposto della responsabilità dell'Ente è stato notevolmente ampliato da interventi legislativi che hanno esteso la responsabilità amministrativa degli Enti ad una maggiore gamma di reati.
L'ambito applicativo delle nuove disposizioni, originariamente limitato agli artt. 24, 25 e 26 della legge, è stato successivamente esteso mediante modifica dello stesso Decreto come di seguito indicato:

26/09/2001
Il DECRETO-LEGGE 25 settembre 2001, n. 350 (in G.U. 26/09/2001, n.224) , convertito con modificazioni dalla L. 23 novembre 2001, n. 409 (in G.U. 24/11/2001, n. 274) ha disposto (con l'art. 6, comma 1) l'introduzione dell'art. 25-bis.

15/04/2002
Il DECRETO LEGISLATIVO 11 aprile 2002, n. 61 (in G.U. 15/04/2002, n.88) ha disposto (con l'art. 3, comma 2) l'introduzione dell'art. 25-ter.

15/06/2002
Il DECRETO DEL PRESIDENTE DELLA REPUBBLICA 30 maggio 2002, n. 115 (in SO n.126, relativo alla G.U. 15/06/2002, n.139) ha disposto (con l'art. 299) l'abrogazione dell'art. 75.

27/01/2003
La LEGGE 14 gennaio 2003, n. 7 (in G.U. 27/01/2003, n.21) ha disposto (con l'art. 3, comma 1) l'introduzione dell'art. 25-quater.

13/02/2003
Il DECRETO DEL PRESIDENTE DELLA REPUBBLICA 14 novembre 2002, n. 313 (in SO n.22, relativo alla G.U. 13/02/2003, n.36) ha disposto (con l'art. 52) l'abrogazione dell'art. 80.

13/02/2003
Il DECRETO DEL PRESIDENTE DELLA REPUBBLICA 14 novembre 2002, n. 313 (in SO n.22, relativo alla G.U. 13/02/2003, n.36) ha disposto (con l'art. 52) l'abrogazione dell'art. 81.

13/02/2003
Il DECRETO DEL PRESIDENTE DELLA REPUBBLICA 14 novembre 2002, n. 313 (in SO n.22, relativo alla G.U. 13/02/2003, n.36) ha disposto (con l'art. 52) l'abrogazione della lettera b) del comma 1 dell'art. 85.

04/08/2003
Il DECRETO 26 giugno 2003, n. 201 (in G.U. 04/08/2003, n.179) ha disposto (con l'art. 8, comma 1) la modifica dell'art. 6, comma 3.

23/08/2003
La LEGGE 11 agosto 2003, n. 228 (in G.U. 23/08/2003, n.195) ha disposto (con l'art. 5) l'introduzione dell'art. 25-quinquies.

27/04/2005
La LEGGE 18 aprile 2005, n. 62 (in SO n.76, relativo alla G.U. 27/04/2005, n.96) ha disposto (con l'art. 9, comma 3) l'introduzione dell'art. 25-sexies.

28/12/2005
La LEGGE 28 dicembre 2005, n. 262 (in SO n.208, relativo alla G.U. 28/12/2005, n.301) ha disposto (con l' artt. 31) la modifica dell'art. 25-ter, comma 1, lettera r).

28/12/2005
La LEGGE 28 dicembre 2005, n. 262 (in SO n.208, relativo alla G.U. 28/12/2005, n.301) ha disposto (con l'art. 39, comma 5) la modifica dell'art. 25-ter.

18/01/2006
La LEGGE 9 gennaio 2006, n. 7 (in G.U. 18/01/2006, n.14) ha disposto (con l'art. 8, comma 1)l'introduzione dell'art.25- quater.1.

15/02/2006
La LEGGE 6 febbraio 2006, n. 38 (in G.U. 15/02/2006, n.38) ha disposto (con l'art. 10, comma 1, lettera a) la modifica dell'art. 25-quinquies, comma 1, lettera b); (con l'art. 10, comma 1, lettera b) la modifica dell'art. 25-quinquies, comma 1, lettera c).

10/08/2007
La LEGGE 3 agosto 2007, n. 123 (in G.U. 10/08/2007, n.185) ha disposto (con l'art. 9, comma 1) l'introduzione dell'art. 25-septies.

14/12/2007
Il DECRETO LEGISLATIVO 21 novembre 2007, n. 231 (in SO n.268, relativo alla G.U. 14/12/2007, n.290) ha disposto (con l'art. 63, comma 3) l'introduzione dell'art. 25 - octies.

04/04/2008
La LEGGE 18 marzo 2008, n. 48 (in SO n.79, relativo alla G.U. 04/04/2008, n.80) ha disposto (con l'art. 7, comma 1) l'introduzione dell'art. 24-bis.

30/04/2008
Il DECRETO LEGISLATIVO 9 aprile 2008, n. 81 (in SO n.108, relativo alla G.U. 30/04/2008, n.101) ha disposto (con l'art. 300, comma 1) la modifica dell'art. 25-septies.

24/07/2009
La LEGGE 15 luglio 2009, n. 94 (in SO n.128, relativo alla G.U. 24/07/2009, n.170) ha disposto (con l'art. 2, comma 29) l'introduzione dell'art. 24-ter.

31/07/2009
La LEGGE 23 luglio 2009, n. 99 (in SO n.136, relativo alla G.U. 31/07/2009, n.176) ha disposto (con l'art. 15, comma 7, lettera a) la modifica dell'art. 25-bis, commi 1, 2, l'introduzione della lettera f-bis) e la modifica della rubrica.

31/07/2009
La LEGGE 23 luglio 2009, n. 99 (in SO n.136, relativo alla G.U. 31/07/2009, n.176) ha disposto (con l'art. 15, comma 7, lettera c) l'introduzione dell'art. 25-novies.

31/07/2009
La LEGGE 23 luglio 2009, n. 99 (in SO n.136, relativo alla G.U. 31/07/2009, n.176) ha disposto (con l'art. 15, comma 7, lettera b) l'introduzione dell'art. 25-bis.1.

14/08/2009
La LEGGE 3 agosto 2009, n. 116 (in G.U. 14/08/2009, n.188) ha disposto (con l'art. 4, comma 1) la modifica dell'art. 25-novies.

30/12/2009
La LEGGE 23 dicembre 2009, n. 191 (in SO n.243, relativo alla G.U. 30/12/2009, n.302) ha disposto (con l'art. 2, comma 218) la modifica dell'art. 18, comma 2.

01/08/2011
Il DECRETO LEGISLATIVO 7 luglio 2011, n. 121 (in G.U. 01/08/2011, n.177) ha disposto (con l'art. 2, comma 2) l'introduzione dell'art. 25-undecies.

01/08/2011
Il DECRETO LEGISLATIVO 7 luglio 2011, n. 121 (in G.U. 01/08/2011, n.177) , nel modificare l'art. 4 della L. 3 agosto 2009, n. 116 (in G.U. 14/8/2009, n.

188), ha conseguentemente disposto (con l'art. 2, comma 1) l'introduzione dell'art. 25-decies.

01/08/2011
Il DECRETO LEGISLATIVO 7 luglio 2011, n. 121 (in G.U. 01/08/2011, n.177) , nel modificare l'art. 4 della L. 3 agosto 2009, n. 116 (in G.U. 14/8/2009, n. 188), ha conseguentemente disposto (con l'art. 2, comma 1) la modifica dell'art. 25-novies.

14/11/2011
La LEGGE 12 novembre 2011, n. 183 (in SO n.234, relativo alla G.U. 14/11/2011, n.265) ha disposto (con l'art. 14, comma 12) l'introduzione del comma 4-bis all'art. 6.

25/07/2012
Il DECRETO LEGISLATIVO 16 luglio 2012, n. 109 (in G.U. 25/07/2012, n.172) ha disposto (con l'art. 2, comma 1) l'introduzione dell'art. 25-duodecies.

13/11/2012
La LEGGE 6 novembre 2012, n. 190 (in G.U. 13/11/2012, n.265) ha disposto (con l'art. 1, comma 77, lettera a)) la modifica dell'art. 25, comma 3 e rubrica.

13/11/2012
La LEGGE 6 novembre 2012, n. 190 (in G.U. 13/11/2012, n.265) ha disposto (con l'art. 1, comma 77, lettera b)) l'introduzione della lettera s-bis) all'art. 25-ter, comma 1.

31/08/2013
Il DECRETO-LEGGE 31 agosto 2013, n. 101 (in G.U. 31/08/2013, n.204) , convertito con modificazioni dalla L. 30 ottobre 2013, n. 125 (in G.U. 30/10/2013, n. 255), ha disposto (con l'art. 12, comma 5-bis) l'introduzione del comma 1-bis all'art. 53.

22/03/2014
Il DECRETO LEGISLATIVO 4 marzo 2014, n. 39 (in G.U. 22/03/2014, n.68) ha disposto (con l'art. 3, comma 1) la modifica dell'art. 25-quinquies, comma 1, lettera c).

17/12/2014
La LEGGE 15 dicembre 2014, n. 186 (in G.U. 17/12/2014, n.292) ha disposto (con l'art. 3, comma 5, lettera a)) la modifica dell'art. 25-octies, comma 1; (con l'art. 3, comma 5, lettera b)) la modifica della rubrica dell'art. 25-octies.
28/05/2015
La LEGGE 22 maggio 2015, n. 68 (in G.U. 28/05/2015, n.122) ha disposto (con l'art. 1, comma 8, lettera a)) la modifica dell'art. 25-undecies, comma 1, lettere a) e b), l'introduzione delle lettere da c) a g) all'art. 25-undecies, comma 1 e del comma 1-bis all'art. 25-undecies.

30/05/2015
La LEGGE 27 maggio 2015, n. 69 (in G.U. 30/05/2015, n.124) ha disposto (con l'art. 12, comma 1, lettera a)) la modifica dell'art. 25-ter, comma 1, alinea; (con l'art. 12, comma 1, lettera b)) la modifica dell'art. 25-ter, comma 1, lettera a); (con l'art. 12, comma 1, lettera c)) l'introduzione della lettera a-bis) all'art. 25-ter, comma 1; (con l'art. 12, comma 1, lettera d)) la modifica dell'art. 25-ter, comma 1, lettera b); (con l'art. 12, comma 1, lettera e)) l'abrogazione della lettera c) dell'art. 25-ter, comma 1.

03/11/2016
La LEGGE 29 ottobre 2016, n. 199 (in G.U. 03/11/2016, n.257) ha disposto (con l'art. 6, comma 1) la modifica dell'art. 25-quinquies, comma 1, lettera a).

30/03/2017
Il DECRETO LEGISLATIVO 15 marzo 2017, n. 38 (in G.U. 30/03/2017, n.75) ha disposto (con l'art. 6, comma 1) la modifica dell'art. 25-ter, comma 1, lettera s-bis).

04/11/2017
La LEGGE 17 ottobre 2017, n. 161 (in G.U. 04/11/2017, n.258) ha disposto (con l'art. 30, comma 4) l'introduzione dei commi 1-bis, 1-ter e 1-quater all'art. 25-duodecies.

27/11/2017
La LEGGE 20 novembre 2017, n. 167 (in G.U. 27/11/2017, n.277) ha disposto (con l'art. 5, comma 2) l'introduzione dell'art. 25-terdecies.

14/12/2017
La LEGGE 30 novembre 2017, n. 179 (in G.U. 14/12/2017, n. 291) ha disposto (con l'art. 2 comma 1) l'introduzione dei commi 2-bis, 2-ter, 2-quater all'art. 6.

16/01/2019
La LEGGE 9 gennaio 2019, n. 3 (in G.U. 16/01/2019, n.13) ha disposto (con l'art. 1, comma 9, lettera a)) la modifica dell'art. 13, comma 2, (con l'art. 1, comma 9, lettera b)) la modifica dell'art. 25, commi 1 e 5 e l'introduzione del comma 5-bis all'art. 25 e (con l'art. 1, comma 9, lettera c)) la modifica dell'art. 51, commi 1 e 2.

16/05/2019
La LEGGE 3 maggio 2019, n. 39 (in G.U. 16/05/2019, n.113) ha disposto (con l'art. 5, comma 1) l'introduzione dell'art. 25-quaterdecies.

25/12/2019
A partire dal 25 dicembre 2019 la legge di conversione del 19 dicembre 2019 n. 157 è entrata in vigore convertendo il D.l. 124/157 emanato il 26 ottobre 2019. Tale Legge interviene sulla disciplina del D.LGS 231/01 ampliando il novero dei reati presupposto introducendo l'art. 25 – quinquiesdecies "REATI TRIBUTARI". Inizialmente l'articolo in questione doveva riguardare solo la

fattispecie "Dichiarazione fraudolenta mediante l'utilizzo di fatture o altri documenti inesistenti ex art. 2 D. Lgs. 74/2000" mentre con il citato provvedimento sono inclusi tutti i delitti fiscali

16/07/2020
Contrabbando (Art. 25-sexiesdecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 75/2020]

29/11/2021

Il DECRETO LEGISLATIVO 8 novembre 2021, n. 184 (in G.U. 29/11/2021, n.284, S.O. n.40; entrato in vigore il 14/12/2021) ha disposto, con l'art. 3, l'introduzione dell'art. 25-octies.1, rubricato «Delitti in materia di strumenti di pagamento diversi dai contanti», includendo nel sistema 231, tra gli altri, i reati di cui agli artt. 493-ter, 493-quater e 640-ter c.p. nelle ipotesi previste dalla norma.

22/03/2022

La LEGGE 9 marzo 2022, n. 22 (in G.U. 22/03/2022, n.68; entrata in vigore il 23/03/2022) ha disposto, con l'art. 3, l'introduzione dell'art. 25-septiesdecies «Delitti contro il patrimonio culturale» e dell'art. 25-duodevicies «Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici».

22/10/2022

Il DECRETO LEGISLATIVO 4 ottobre 2022, n. 156 (in G.U. 22/10/2022, n.248; entrato in vigore il 06/11/2022) ha disposto, con l'art. 5, la modifica dell'art. 25-quinquiesdecies, comma 1-bis, precisando i presupposti di rilevanza dei reati tributari commessi al fine di evadere l'IVA nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea e con danno complessivo pari o superiore a 10 milioni di euro.

07/03/2023

Il DECRETO LEGISLATIVO 2 marzo 2023, n. 19 (in G.U. 07/03/2023, n.56; entrato in vigore il 22/03/2023), in materia di trasformazioni, fusioni e scissioni transfrontaliere, ha modificato l'art. 25-ter, estendendone il richiamo anche alle fattispecie previste da altre leggi speciali e introducendo la lettera s-ter relativa alle false o omesse dichiarazioni per il rilascio del certificato preliminare previsto dalla disciplina delle operazioni societarie transfrontaliere.

15/03/2023

Il DECRETO LEGISLATIVO 10 marzo 2023, n. 24 (in G.U. 15/03/2023, n.63; entrato in vigore il 30/03/2023), relativo alla protezione delle persone che segnalano violazioni (whistleblowing), ha coordinato la disciplina dell'art. 6 del D.Lgs. 231/2001 con il nuovo sistema di segnalazione interna, di tutela del segnalante e di divieto di ritorsione, sostituendo la previgente disciplina contenuta nel comma 2-bis e superando le precedenti disposizioni dei commi 2-ter e 2-quater.

09/10/2023

La LEGGE 9 ottobre 2023, n. 137 (in G.U. 09/10/2023, n.236; entrata in

vigore il 10/10/2023), di conversione del D.L. 10 agosto 2023, n. 105, ha ampliato l'art. 24 inserendo i delitti di turbata libertà degli incanti (art. 353 c.p.) e turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.). Ha inoltre modificato l'art. 25-octies.1, includendo il delitto di trasferimento fraudolento di valori di cui all'art. 512-bis c.p. e adeguando la rubrica dell'articolo.

02/07/2024

La LEGGE 28 giugno 2024, n. 90 (in G.U. 02/07/2024, n.153; entrata in vigore il 17/07/2024), recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, ha modificato l'art. 24-bis del D.Lgs. 231/2001, aggiornando il catalogo dei delitti informatici rilevanti e il relativo trattamento sanzionatorio in coordinamento con le modifiche apportate al codice penale.

09/08/2024

La LEGGE 8 agosto 2024, n. 112 (in G.U. 09/08/2024, n.186; entrata in vigore il 10/08/2024), di conversione del D.L. 4 luglio 2024, n. 92, ha modificato l'art. 25, comma 1, del D.Lgs. 231/2001 inserendo il nuovo delitto di «indebita destinazione di denaro o cose mobili» di cui all'art. 314-bis c.p.; contestualmente ha adeguato la rubrica dell'art. 25 ed eliminato dal relativo richiamo l'art. 323 c.p. (abuso d'ufficio).

03/10/2024

Il DECRETO LEGISLATIVO 26 settembre 2024, n. 141 (in G.U. 03/10/2024, n.232; entrato in vigore il 04/10/2024) ha modificato l'art. 25-sexiesdecies, aggiornando i riferimenti alla nuova disciplina doganale e includendo, nel perimetro della responsabilità dell'ente, anche i reati previsti dal testo unico delle disposizioni legislative concernenti le imposte sulla produzione e sui consumi (D.Lgs. 26 ottobre 1995, n. 504), con adeguamento del sistema sanzionatorio.

16/06/2025

La LEGGE 6 giugno 2025, n. 82 (in G.U. 16/06/2025, n.137; entrata in vigore il 01/07/2025) ha disposto, con l'art. 8, l'introduzione dell'art. 25-undevicies «Delitti contro gli animali». La disposizione richiama gli artt. 544-bis, 544-ter, 544-quater, 544-quinquies e 638 c.p., prevedendo sanzioni pecuniarie fino a 500 quote e, nei casi previsti, sanzioni interdittive fino a due anni.

08/08/2025 – 07/10/2025

Il DECRETO-LEGGE 8 agosto 2025, n. 116 (in G.U. 08/08/2025, n.183; entrato in vigore il 09/08/2025), convertito con modificazioni dalla LEGGE 3 ottobre 2025, n. 147 (in G.U. 07/10/2025, n.233; entrata in vigore il 08/10/2025), ha modificato l'art. 25-undecies del D.Lgs. 231/2001, ampliando e riordinando il sistema dei reati presupposto ambientali in materia di rifiuti e rafforzando le relative sanzioni a carico degli enti.

09/01/2026

Il DECRETO LEGISLATIVO 30 dicembre 2025, n. 211 (in G.U. 09/01/2026, n.6; entrato in vigore il 24/01/2026), in attuazione della direttiva (UE) 2024/1226, ha modificato gli artt. 10 e 13 e ha introdotto l'art. 25-octies.2 «Reati in materia di violazione di misure restrittive dell'Unione europea». Per

tali illeciti sono previste, nei casi indicati dalla norma, sanzioni pecuniarie determinate anche in percentuale sul fatturato globale dell'ente e specifiche sanzioni interdittive.

14/05/2026

La LEGGE 21 aprile 2026, n. 75 (in G.U. 14/05/2026, n.110; entrata in vigore il 29/05/2026), recante disposizioni sanzionatorie a tutela dei prodotti alimentari italiani, ha modificato l'art. 25-bis.1, comma 1, lettera a), inserendo tra i delitti contro l'industria e il commercio rilevanti ai fini 231 anche la fattispecie di cui all'art. 517-octies, quarto comma, c.p.

18/05/2026

Il DECRETO LEGISLATIVO 21 aprile 2026, n. 81 (in G.U. 18/05/2026, n.113; entrato in vigore il 02/06/2026), di attuazione della direttiva (UE) 2024/1203 sulla tutela penale dell'ambiente, ha ulteriormente modificato l'art. 25-undecies del D.Lgs. 231/2001, aggiornando e ampliando il catalogo dei reati presupposto ambientali e il relativo trattamento sanzionatorio in coordinamento con le nuove fattispecie e circostanze introdotte nel codice penale.

01/07/2026

Il DECRETO LEGISLATIVO 12 giugno 2026, n. 115 (in G.U. 01/07/2026, n.150; entrato in vigore il 16/07/2026), in attuazione della direttiva (UE) 2024/1712 sulla prevenzione e repressione della tratta di esseri umani, ha modificato l'art. 25-quinquies. In particolare ha introdotto, al comma 1, la lettera c-bis), riferita al delitto di cui all'art. 601.1 c.p., con sanzione pecuniaria da 100 a 600 quote, e ha previsto per tale fattispecie sanzioni interdittive per una durata non inferiore a sei mesi.

30/09/2026

Il DECRETO LEGISLATIVO 9 settembre 2026, n. 160 (pubblicato nella G.U. 15/09/2026, n. 214, ed entrato in vigore il 30/09/2026), recante disposizioni di adeguamento della normativa nazionale al Regolamento (UE) 2024/1689 sull'intelligenza artificiale, ha disposto, con l'art. 15, comma 1, l'introduzione nel D.Lgs. 231/2001 dell'art. 25-vicies, rubricato «Reati commessi con l'uso di sistemi di intelligenza artificiale».

La nuova disposizione estende la responsabilità amministrativa degli enti ai delitti di cui agli articoli 437-bis e 612-quater del Codice penale, prevedendo specifiche sanzioni pecuniarie e interdittive.

L'introduzione di tali reati-presupposto rende necessario valutare i rischi connessi all'utilizzo dei sistemi di intelligenza artificiale nell'ambito delle attività aziendali e verificare l'adeguatezza dei relativi presidi organizzativi, delle procedure di controllo e delle attività di vigilanza.

INTERVENTI CON EFFETTI INDIRETTI SUL CATALOGO DEI REATI PRESUPPOSTO

30/11/2021

Il DECRETO LEGISLATIVO 8 novembre 2021, n. 195 ha modificato le fattispecie codicistiche di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza

illecita e autoriciclaggio, incidendo conseguentemente sull'ambito delle condotte richiamate dall'art. 25-octies del D.Lgs. 231/2001.

10/08/2024

La LEGGE 9 agosto 2024, n. 114 (c.d. riforma Nordio), pubblicata in G.U. 10/08/2024, n.187 ed entrata in vigore il 25/08/2024, ha abrogato l'art. 323 c.p. (abuso d'ufficio) e modificato l'art. 346-bis c.p. (traffico di influenze illecite), con conseguenti effetti sul perimetro delle fattispecie rilevanti ai fini della responsabilità degli enti.

NUOVI ARTICOLI DEL D.LGS. 231/2001 INTRODOTTI DAL 2020

- **Art. 25-sexiesdecies** – Contrabbando (D.Lgs. 75/2020; successivamente modificato dal D.Lgs. 141/2024).
- **Art. 25-octies.1** – Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (D.Lgs. 184/2021; successivamente modificato dalla L. 137/2023).
- **Art. 25-septiesdecies** – Delitti contro il patrimonio culturale (L. 22/2022).
- **Art. 25-duodevicies** – Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (L. 22/2022).
- **Art. 25-undevicies** – Delitti contro gli animali (L. 82/2025).
- **Art. 25-octies.2** – Reati in materia di violazione di misure restrittive dell'Unione europea (D.Lgs. 211/2025).
- **Art. 25-vicies** – Reati commessi con l'uso di sistemi di intelligenza artificiale (D.Lgs. 160/2026, art. 15, in vigore dal 30/09/2026). Comprende i delitti di cui agli artt. 437-bis e 612-quater del Codice penale.

Per effetto dei progressivi ampliamenti normativi, il sistema di responsabilità amministrativa degli enti di cui al D.Lgs. 8 giugno 2001, n. 231 si applica oggi alle seguenti categorie di reati presupposto (in forma consumata o, limitatamente ai delitti, anche semplicemente tentata):

1. Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (art. 24), comprendente anche le fattispecie di cui agli artt. 353 e 353-bis c.p.
2. Delitti informatici e trattamento illecito di dati (art. 24-bis), comprendenti le fattispecie richiamate dagli artt. 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater, 635-quinquies, 629, terzo comma, 615-quater, 635-quater.1, 491-bis e 640-quinquies c.p., nonché le ulteriori fattispecie previste dall'art. 1, comma 11, D.L. n. 105/2019, come modificato dalla L. n. 90/2024.
3. Delitti di criminalità organizzata (art. 24-ter), comprendenti, tra gli altri, associazione per delinquere, associazione di tipo mafioso, scambio elettorale politico-mafioso, sequestro di persona a scopo di estorsione e associazione finalizzata al traffico illecito di sostanze stupefacenti.

4. Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità e corruzione (art. 25). La fattispecie di abuso d'ufficio non è più richiamata dall'art. 25; è stato invece inserito l'art. 314-bis c.p. in materia di indebita destinazione di denaro o cose mobili.
5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis).
6. Delitti contro l'industria e il commercio (art. 25-bis.1), come da ultimo modificato dalla L. n. 75/2026 in materia di tutela dei prodotti alimentari, con inclusione anche dell'art. 517-octies, quarto comma, c.p.
7. Reati societari (art. 25-ter).
8. Delitti con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-quater).
9. Pratiche di mutilazione degli organi genitali femminili, art. 583-bis c.p. (art. 25-quater.1).
10. Delitti contro la personalità individuale (art. 25-quinquies), comprendenti anche il delitto di cui all'art. 601.1 c.p., inserito nel catalogo dei reati presupposto dal D.Lgs. n. 115/2026.
11. Abusi di mercato, con particolare riferimento all'abuso di informazioni privilegiate e alla manipolazione del mercato (art. 25-sexies).
12. Omicidio colposo o lesioni gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-septies).
13. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio, artt. 648, 648-bis, 648-ter e 648-ter.1 c.p. (art. 25-octies).
14. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1), comprendenti, tra le principali fattispecie, gli artt. 493-ter, 493-quater, 640-ter e 512-bis c.p.
15. Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25-octies.2), introdotti dal D.Lgs. n. 211/2025 e riferiti, in particolare, agli artt. 275-bis, 275-ter e 275-quater c.p. e all'art. 12, comma 1-bis, D.Lgs. n. 286/1998.
16. Delitti in materia di violazione del diritto d'autore (art. 25-novies).
17. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, art. 377-bis c.p. (art. 25-decies).
18. Reati ambientali (art. 25-undecies), comprendenti i delitti ambientali previsti dal codice penale e le ulteriori fattispecie ambientali richiamate dalla normativa speciale, come da ultimo modificate e ampliate dal D.Lgs. n. 81/2026.
19. Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25-duodecies).

20. Razzismo e xenofobia (art. 25-terdecies).
21. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies).
22. Reati tributari (art. 25-quinquiesdecies).
23. Contrabbando (art. 25-sexiesdecies), con riferimento ai reati previsti dalle disposizioni nazionali complementari al Codice doganale dell'Unione e, a seguito delle modifiche introdotte nel 2024, anche alle fattispecie rilevanti previste dal testo unico delle accise di cui al D.Lgs. n. 504/1995.
24. Delitti contro il patrimonio culturale (art. 25-septiesdecies), comprendenti le fattispecie richiamate dagli artt. 518-bis, 518-ter, 518-quater, 518-octies, 518-novies, 518-decies, 518-undecies, 518-duodecies e 518-quaterdecies c.p.
25. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25-duodevicies), con riferimento agli artt. 518-sexies e 518-terdecies c.p.
26. Delitti contro gli animali (art. 25-undevicies), introdotti dalla L. n. 82/2025, con riferimento agli artt. 544-bis, 544-ter, 544-quater, 544-quinquies e 638 c.p.
27. Reati transnazionali di cui all'art. 10 della L. n. 146/2006, quando ricorrono i presupposti di transnazionalità previsti dalla medesima legge.
28. Reati commessi con l'uso di sistemi di intelligenza artificiale (art. 25-vicies del D.Lgs. 231/2001).
    La fattispecie comprende i seguenti delitti:
    Art. 437-bis c.p. – Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi;
    Art. 612-quater c.p. – Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale.
    La responsabilità amministrativa dell'ente può configurarsi qualora tali delitti siano commessi, nell'interesse o a vantaggio dell'ente, da soggetti apicali o da persone sottoposte alla loro direzione o vigilanza, secondo i presupposti stabiliti dal D.Lgs. 231/2001.
    L'utilizzo di sistemi di intelligenza artificiale può inoltre costituire una modalità di commissione di ulteriori reati-presupposto già contemplati dal Decreto, che continuano a essere disciplinati dalle rispettive disposizioni.

1.2.3. Responsabilità dell'Ente e funzione esimente del Modello

Secondo quanto previsto dall'art. 5, la responsabilità prevista dal Decreto a carico dell'Ente scatta qualora il reato commesso:
a. sia stato realizzato anche o esclusivamente nell'interesse o a vantaggio dell'Ente. Ne deriva che non vi è responsabilità dell'Ente se il reato è stato commesso nell'interesse esclusivo del reo o di terzi;
b. sia stato realizzato da una persona fisica legata, a vario titolo, da un rapporto funzionale con l'Ente. Esattamente, il reato può essere commesso da una

persona:
- in posizione apicale, ossia da una persona fisica che esercita funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, o che esercita, anche di fatto, la gestione e il controllo dello stesso ("Soggetto Apicale");
- sottoposta alla direzione o alla vigilanza di un Soggetto Apicale ("Soggetto Subordinato").

Tuttavia, pur in presenza dei presupposti di cui sopra (e cioè: reato rientrante tra i reati-presupposto di cui al Decreto; persona fisica funzionalmente legata all'Ente; sussistenza di un vantaggio o di un interesse per l'Ente), come stabilisce il primo comma dell'art. 6 del Decreto, ove il reato venga commesso da un Soggetto Apicale la società non risponde se prova che (inversione dell'onere della prova che viene a gravare sull'Ente anziché, come di regola, sul Pubblico Ministero):
- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione e di Gestione idoneo a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento è stato affidato ad un organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo, vale a dire all'Organismo di Vigilanza (negli enti di piccole dimensioni tale compito può essere svolto direttamente dall'organo dirigente);
- l'autore ha commesso il reato eludendo fraudolentemente il Modello;
- non vi è stata omessa o insufficiente vigilanza da parte dell'OdV.

Qualora quindi un soggetto in posizione di vertice commetta un reato tra quelli contemplati dal Decreto – derivandone un interesse o un vantaggio per l'Ente stesso – l'Ente incorrerà in responsabilità *ex* d.lgs. n. 231 del 2001 a meno che non provi la sussistenza di una serie di requisiti, tra loro concorrenti, descritti dal primo comma dell'art. 6 del Decreto tra cui, in primo luogo, l'adozione e l'efficace attuazione, prima della commissione del fatto, di un Modello di Organizzazione e Gestione idoneo a prevenire reati della specie di quello verificatosi.

Un ruolo essenziale è, inoltre, svolto dall'Organismo di Vigilanza: infatti, nel caso in cui il reato-presupposto sia stato commesso da un Soggetto Apicale, l'esenzione dell'Ente da responsabilità amministrativa *ex crimine* dipenderà dall'aver tale organo garantito l'efficienza e l'operatività del Modello, attraverso lo svolgimento di un'attività di controllo sull'idoneità del Modello a prevenire la commissione del reato-presupposto, sulla sua effettività all'interno dell'Ente e sul suo aggiornamento.

Se il fatto è stato, invece, commesso da un Soggetto Subordinato la società risulterà responsabile solo qualora il Pubblico Ministero provi (non c'è, in questo caso, inversione dell'onere della prova) che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o di vigilanza, e in ogni caso, come stabilisce il secondo comma dell'art. 7 del Decreto, detta inosservanza è esclusa se l'Ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello di Organizzazione,

Gestione e Controllo idoneo – secondo una valutazione che deve essere fatta a priori – a prevenire reati del tipo di quello verificatosi.

L'efficace attuazione del Modello richiede, inoltre, una verifica periodica dello stesso e l'eventuale sua modifica quando vengano scoperte significative violazioni delle prescrizioni, o quando intervengono mutamenti nell'organizzazione o nell'attività, o quando nel Decreto vengono ad aggiungersi nuove fattispecie di reati.

L'efficace attuazione del Modello richiede, infine, la previsione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

1.3. Le sanzioni

Il D.lgs. n. 231 del 2001 disegna un modello sanzionatorio pensato per rivolgersi all'Ente, non alla persona fisica, ed individua un sistema fondato essenzialmente su due tipi di sanzioni:
a. pecuniaria
b. interdittiva
alle quali si aggiungono:
c. la pubblicazione della sentenza di condanna
d. la confisca.

1.3.1. La sanzione pecuniaria

Come chiarisce il primo comma dell'art. 10 del Decreto, la sanzione pecuniaria è indefettibile: per l'illecito amministrativo dipendente da reato si applica sempre. Essa consiste nel pagamento di una somma di denaro determinata sulla base di un sistema bifasico c.d. per quote: sulla base di quanto previsto dall'art. 11 del Decreto, in prima battuta il giudice determinerà il numero delle quote (in numero non inferiore a 100 e non superiore a 1000) tenendo conto della gravità del fatto, del grado della responsabilità dell'Ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti; l'importo della quota sarà poi fissato (tra un valore minimo di euro 258,23 ed un massimo di euro 1.549,37) sulla base delle condizioni economiche e patrimoniali dell'Ente allo scopo di assicurare l'efficacia della sanzione, in modo tale che la sanzione pecuniaria non rischi di essere indifferente o, al contrario, insostenibile per l'Ente.
Con riferimento ai reati commessi con l'uso di sistemi di intelligenza artificiale, l'art. 25-vicies del D.Lgs. 231/2001, introdotto dal D.Lgs. 160/2026, prevede specifiche sanzioni pecuniarie a carico dell'ente.

In particolare:

per il delitto di cui all'art. 437-bis c.p. (omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi), si applica la sanzione pecuniaria da 600 a 1.000 quote;

per il delitto di cui all'art. 612-quater c.p. (illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale), si applica la sanzione pecuniaria da 200 a 700 quote.

L'importo complessivo della sanzione pecuniaria è determinato secondo i criteri previsti dagli articoli 10 e 11 del D.Lgs. 231/2001, tenendo conto della gravità del fatto, del grado di responsabilità dell'ente, delle iniziative adottate per prevenire ulteriori illeciti e delle condizioni economiche e patrimoniali della Società.

Le nuove previsioni rendono particolarmente importante l'adozione e l'efficace attuazione di misure organizzative e di controllo idonee a prevenire la commissione dei reati-presupposto connessi all'utilizzo dell'intelligenza artificiale.

1.3.2. Le sanzioni interdittive

Le sanzioni interdittive, di cui all'art. 13 del Decreto, consistono:

a. nell'interdizione dall'esercizio dell'attività;
b. nella sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
c. nel divieto, temporaneo o definitivo, di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
d. nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli già concessi;
e. nel divieto, temporaneo o definitivo, di pubblicizzare beni o servizi.

Le sanzioni interdittive si applicano, anche congiuntamente tra loro, esclusivamente in relazione ai reati per i quali sono espressamente previste dal Decreto e a condizione che ricorra almeno uno di tali presupposti:

- che l'Ente abbia tratto dal reato un profitto di rilevante entità e il reato sia stato commesso da un Soggetto Apicale ovvero da un Soggetto Subordinato quando, in quest'ultimo caso, la commissione del reato sia stata determinata o agevolata da gravi carenze organizzative;
- la reiterazione degli illeciti.

Pur in presenza di una o entrambe le condizioni di cui sopra, secondo quanto previsto dall'art. 17 del Decreto, le sanzioni interdittive non si applicano se, prima della dichiarazione di apertura del dibattimento di primo grado, si realizzino tutte le seguenti condizioni, considerate ostative all'applicazione di una sanzione interdittiva:

- l'Ente abbia risarcito integralmente il danno ed eliminato le conseguenze dannose o pericolose del reato ovvero si sia comunque efficacemente adoperato in tal senso;
- l'Ente abbia eliminato le carenze organizzative che hanno determinato il reato, mediante l'adozione e l'attuazione di un Modello;
- l'Ente abbia messo a disposizione il profitto conseguito ai fini della confisca.

Le sanzioni interdittive possono essere applicate anche in via cautelare, benché mai congiuntamente tra loro (su richiesta al Giudice da parte del Pubblico Ministero) quando ricorrono le seguenti condizioni:

- vi sono gravi indizi che portano a ritenere la sussistenza della responsabilità dell'Ente;
- vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi altri illeciti della stessa indole di quello per cui si procede.

Nel disporre le misure cautelari, il Giudice tiene conto della specifica idoneità

di ciascuna in relazione alla natura e al grado delle esigenze cautelari da soddisfare nel caso concreto, della necessaria proporzione tra la misura applicata, l'entità del fatto e la sanzione che si ritiene possa essere applicata all'Ente in via definitiva.

Con specifico riferimento ai reati commessi con l'uso di sistemi di intelligenza artificiale, l'art. 25-vicies, comma 3, del D.Lgs. 231/2001 dispone l'applicazione delle sanzioni interdittive previste dall'art. 9, comma 2, lettere b), c), d) ed e), del medesimo Decreto.

Le sanzioni interdittive richiamate sono:

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 ottenere le prestazioni di un pubblico servizio;

l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

il divieto di pubblicizzare beni o servizi.

L'applicazione delle sanzioni interdittive avviene secondo i presupposti e le condizioni stabiliti dal D.Lgs. 231/2001.

In considerazione delle possibili conseguenze sull'operatività aziendale, MI.ZAR. SRL considera la prevenzione dei reati connessi all'intelligenza artificiale parte integrante del proprio sistema di organizzazione, gestione e controllo.

1.3.3. La pubblicazione della sentenza di condanna

La pubblicazione della sentenza di condanna consiste nella pubblicazione di quest'ultima una sola volta, per estratto o per intero, a cura della Cancelleria e a spese dell'Ente, in uno o più giornali indicati nella sentenza, nonché nell'affissione della stessa nel Comune ove l'Ente ha la sede principale. La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'Ente viene applicata una sanzione interdittiva.

1.3.4. La confisca

La confisca è prevista quale sanzione all'art. 19 del Decreto e consiste nell'acquisizione coattiva da parte dello Stato del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato e fatti salvi, in ogni caso, i diritti acquisiti dai terzi in buona fede. Quando non è possibile eseguire la confisca in natura, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

2. Adozione del Modello da parte di MI.ZAR. SRL

2.1. Struttura della società

2.1.1. MI.ZAR. SRL e la sua *mission*

MI.ZAR. SRL è una società di servizi e consulenza alle aziende. Forniamo soluzioni, anche informatiche, per la gestione di temi quali la qualità, la produzione, la gestione dell'area commerciale, acquisti e ufficio tecnico, la gestione della marcatura CE di prodotto, l'analisi della sicurezza macchine ed

attrezzature di lavoro, le certificazioni forestali secondo i pertinenti schemi internazionali, l'Industria 4.0, Privacy e Modelli 231.
La Società si compone un team di professionisti con esperienza pluriennale nel campo delle certificazioni, strettamente coordinati per soddisfare pienamente e rapidamente le esigenze dei clienti e realizzare servizi improntati alla semplicità ed alla concretezza.

2.1.2. Oggetto sociale

Al momento dell'introduzione del presente Modello di Organizzazione e Gestione, le attività principali ricomprese nell'oggetto sociale di MI.ZAR. SRL sono date dalla prestazione di servizi di assistenza necessari alla gestione di imprese e/o industrie di piccole e medie dimensioni ed artigiane.

A titolo esemplificativo, la Società fornisce assistenza, sia direttamente che attraverso persone, enti e organismi terzi, nei settori:

- dell'informatica aziendale;
- della sicurezza e salute nei luoghi di lavoro;
- dell'ambiente;
- della certificazione, gestione e sistemi di qualità.

È contemplata nell'oggetto sociale qualsiasi ulteriore attività affine, complementare e/o accessoria a quelle su elencate, occorrenti per l'attuazione dell'oggetto sociale medesimo.
A novembre 2021 è stato aggiornato lo statuto dell'azienda ed è stato aggiunto un nuovo codice ateco 33.12.10 RIPARAZIONE E MANUTENZIONE DI MACCHINE DI IMPIEGO GENERALE.

2.1.3. Organigramma aziendale

Alla data di approvazione del presente Modello, l'attività di MI.ZAR. SRL è articolata secondo quanto descritto nell'allegato 01_01_Organigramma.
L'Organigramma aziendale, al pari di altri documenti aziendali previsti dal sistema qualità presente in azienda (attualmente non certificato), sono stati integrati con altri documenti presenti nel sistema salute e sicurezza del lavoro, ambiente per rendere più efficiente la gestione complessiva.
L'organigramma aggiornata è presente nel sito internet dell'azienda.

2.1.4. Governo societario: organo amministrativo

Al momento dell'adozione del presente Modello, l'amministrazione di MI.ZAR. SRL figura attribuita all'amministratore unico Dott. Enzo Stefani, investito dei più ampi poteri per la gestione, ordinaria e straordinaria, della Società, ad eccezione soltanto di quanto in forza della legge, dell'atto costitutivo o dello statuto sia riservato alla decisione dei soci. Compete, inoltre, all'amministratore unico di MI.ZAR. SRL la rappresentanza della Società innanzi ai terzi ed in giudizio.

Nello svolgimento delle proprie attività l'organo amministrativo si conforma alle prescrizioni contenute nei protocolli di condotta di cui alla Parte Speciale.

2.1.5. Certificazione ISO9001

Da agosto 2020 la MI.ZAR. SRL è certificata ISO9001, ed ha una politica integrata qualità, sicurezza, ambiente, privacy, 231 che viene verificata in sede di riesame della Direzione, e in caso di aggiornamento, la nuova revisione viene riportata nella sezione documenti del sito internet MIZAR.

L'attestato aggiornato della certificazione ISO9001 è pubblicato sul sito internet di MIZAR.

2.1.6. Certificazione ISO45001

Da dicembre 2020 la MI.ZAR. SRL è certificata ISO45001, e l'attestato aggiornato di questa certificazione è pubblicato sul proprio sito internet.

2.2. Struttura e scopo del Modello

Scopo del presente Modello è quello della realizzazione di un assetto organizzativo con un sistema di controllo interno finalizzato a prevenire la commissione, nell'interesse o a vantaggio della Società, di tutti i reati previsti dal D. Lgs. n. 231 del 2001, i quali reati costituiscono presupposto della responsabilità amministrativa da reato dell'Ente.

Il Modello si suddivide in due parti:
- la Parte generale, ove sono contenute le norme applicabili a tutte le attività societarie ed in relazione a tutti i reati da prevenire;
- la Parte speciale, ove vengono descritte le procedure specificamente rivolte alla prevenzione di alcuni reati, procedure adottate dalla Società a seguito di una approfondita mappatura delle sue attività a rischio e delle attività sensibili, in relazione alle tipologie dei reati presupposto.

Il presente Modello di Organizzazione e Gestione risponde alle seguenti esigenze:

- individuare le attività a rischio ossia quelle nel cui ambito possono essere commessi i reati previsti dal Decreto (le c.d. attività sensibili);
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire;
- individuare le modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- determinare, in tutti coloro che operano in nome e per conto di MI.ZAR. SRL nelle aree di attività a rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni non solo nei propri confronti ma anche nei confronti della Società e la cui commissione è fortemente censurata dalla stessa, in quanto contraria ai suoi interessi, anche laddove, apparentemente, potrebbe trarne immediato vantaggio;
- sensibilizzare e diffondere a tutti i livelli aziendali delle regole comportamentali e delle procedure aziendali;

- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- istituire un apposito Organismo di Vigilanza deputato al controllo sul funzionamento e sull'osservanza del Modello, e prevedere specifici obblighi di informazione nei confronti dello stesso;
- attribuire all'Organismo di Vigilanza specifici poteri di controllo sull'efficace e corretto funzionamento del Modello;
- consentire alla Società, grazie a un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi;
- verificare *ex post* i comportamenti aziendali e il funzionamento del Modello, con conseguente aggiornamento periodico dello stesso.

Prevenzione dei rischi connessi all'utilizzo dell'intelligenza artificiale

Nell'ambito delle finalità del presente Modello, MI.ZAR. SRL considera anche la prevenzione dei reati-presupposto connessi all'utilizzo di sistemi di intelligenza artificiale, con particolare riferimento alle fattispecie introdotte dall'art. 25-vicies del D.Lgs. 231/2001.

A tale scopo, il sistema di organizzazione, gestione e controllo aziendale è finalizzato anche a:

- individuare i sistemi di intelligenza artificiale utilizzati nell'ambito dei processi e delle attività aziendali;
- identificare le attività sensibili nelle quali l'utilizzo dell'intelligenza artificiale potrebbe contribuire alla commissione di reati-presupposto;
- valutare i rischi associati alle modalità di utilizzo dei sistemi di intelligenza artificiale, tenendo conto delle caratteristiche dei sistemi, delle attività svolte e dei soggetti coinvolti;
- definire le responsabilità e le autorizzazioni relative all'utilizzo dei sistemi di intelligenza artificiale;
- stabilire regole di comportamento e misure organizzative finalizzate a prevenire utilizzi illeciti o non autorizzati;
- prevedere, ove applicabili, controlli sulla sicurezza dei sistemi di intelligenza artificiale e sull'effettività della sorveglianza umana;
- assicurare la verifica e la validazione dei risultati generati dall'intelligenza artificiale quando utilizzati nell'erogazione dei servizi di consulenza;
- disciplinare la creazione, la modifica e la diffusione di immagini, video e contenuti audio generati o alterati mediante sistemi di intelligenza artificiale;

- garantire adeguata informazione e formazione al personale e agli altri soggetti autorizzati all'utilizzo dei sistemi;
- assicurare la tracciabilità delle attività di controllo, delle anomalie significative e delle eventuali azioni correttive;
- prevedere adeguati flussi informativi verso l'Organismo di Vigilanza in relazione ai rischi di commissione dei reati-presupposto;
- aggiornare periodicamente la valutazione dei rischi e le misure di prevenzione adottate, anche in conseguenza di modifiche normative, organizzative o tecnologiche.

L'attuazione delle suddette misure avviene mediante procedure e istruzioni operative aziendali, strumenti di valutazione dei rischi, registrazioni dei controlli e attività di vigilanza, in coordinamento con il sistema di gestione per la qualità adottato da MI.ZAR. SRL.

Il Modello deve pertanto essere considerato uno strumento dinamico, soggetto ad aggiornamento anche in relazione all'evoluzione delle tecnologie di intelligenza artificiale e delle modalità del loro utilizzo nei processi aziendali.

2.3. Approccio metodologico al modello

La redazione e l'aggiornamento del presente Modello si sviluppano attraverso un processo strutturato di identificazione, valutazione, prevenzione e controllo dei rischi di commissione dei reati-presupposto previsti dal D.Lgs. 231/2001.

Tale processo si articola nelle seguenti fasi:

1. Mappatura delle aree aziendali a rischio

Individuazione dei processi, delle attività e delle funzioni aziendali nell'ambito dei quali potrebbero essere commessi i reati-presupposto.

La mappatura considera anche l'utilizzo di sistemi di intelligenza artificiale, identificando le attività nelle quali tali sistemi vengono impiegati, le finalità del loro utilizzo, i soggetti coinvolti e le eventuali interazioni con informazioni, dati e documenti aziendali o dei clienti.

2. Valutazione dei rischi (Risk Assessment)

Per ciascuna fattispecie di reato-presupposto viene valutata l'esposizione della Società al rischio di commissione, considerando le caratteristiche delle attività svolte, le possibili modalità di realizzazione del reato e i controlli già adottati.

Con riferimento all'art. 25-vicies del D.Lgs. 231/2001, la valutazione comprende, in particolare:

- il censimento dei sistemi di intelligenza artificiale utilizzati dalla Società;
- l'identificazione dei relativi processi e delle attività sensibili;

- la verifica dell'eventuale impiego di sistemi di intelligenza artificiale ad alto rischio;
- la valutazione delle misure di sicurezza e di sorveglianza umana applicabili;
- l'analisi delle modalità di generazione, modifica e diffusione di immagini, video e contenuti audio mediante sistemi di intelligenza artificiale;
- l'individuazione delle possibili condotte illecite riconducibili ai reati-presupposto;
- la valutazione dei controlli esistenti e delle eventuali carenze organizzative;
- la determinazione del livello di rischio residuo, tenendo conto dell'efficacia delle misure di prevenzione adottate.

La valutazione dei rischi viene documentata e aggiornata in occasione di modifiche significative delle attività, dei sistemi utilizzati o della normativa applicabile.

3. Individuazione dei controlli e delle misure di prevenzione

Sulla base dei risultati del Risk Assessment vengono individuati i controlli già presenti e le eventuali misure integrative necessarie per prevenire la commissione dei reati.

I controlli possono comprendere:

- autorizzazioni e limitazioni nell'utilizzo dei sistemi di intelligenza artificiale;
- definizione di responsabilità e compiti di verifica;
- misure di sicurezza informatica e protezione delle informazioni;
- verifica umana dei risultati generati dai sistemi;
- controllo delle modalità di produzione e diffusione dei contenuti generati artificialmente;
- formazione e sensibilizzazione del personale;
- registrazione delle anomalie, delle violazioni e delle azioni correttive;
- attività di monitoraggio e flussi informativi verso l'Organismo di Vigilanza.

Le misure sono definite in modo proporzionato ai rischi effettivamente individuati e alle caratteristiche organizzative della Società.

4. Definizione delle procedure organizzative e delle regole di comportamento

Predisposizione e aggiornamento di procedure, istruzioni operative e disposizioni vincolanti finalizzate a prevenire la commissione dei reati-presupposto.

In particolare, per l'utilizzo dei sistemi di intelligenza artificiale, MI.ZAR. SRL definisce specifiche regole aziendali riguardanti l'autorizzazione all'utilizzo, la sicurezza delle informazioni, il controllo dei risultati, la responsabilità

professionale, la gestione dei contenuti generati artificialmente e la segnalazione delle anomalie.

5. Monitoraggio e aggiornamento del Modello

L'efficacia delle misure adottate viene verificata periodicamente, anche attraverso le attività dell'Organismo di Vigilanza e il monitoraggio delle attività sensibili.

La valutazione dei rischi e le misure organizzative sono riesaminate quando si verificano:

- modifiche normative che introducono nuovi reati-presupposto o modificano quelli esistenti;
- modifiche significative dei processi e dell'organizzazione aziendale;
- introduzione di nuovi sistemi di intelligenza artificiale o modifiche rilevanti alle loro modalità di utilizzo;
- anomalie, incidenti, violazioni delle procedure o carenze dei controlli;
- altre circostanze che possono incidere sull'adeguatezza e sull'efficacia del Modello.

La documentazione relativa alle attività di Risk Assessment costituisce allegato al presente Modello (Risk Assessment per singolo reato, 01_02).

Per i rischi connessi all'utilizzo dell'intelligenza artificiale, la Società può avvalersi anche di strumenti di registrazione e controllo integrati nel proprio sistema di gestione aziendale, garantendo la disponibilità delle evidenze necessarie alle attività di verifica e vigilanza.

2.4. Destinatari del Modello

Le regole contenute nel presente Modello si applicano a tutti coloro (interni e/o esterni) che operano per il conseguimento dello scopo e degli obiettivi di MI.ZAR. SRL. Ne sono quindi destinatari: coloro che svolgono funzioni di rappresentanza, amministrazione o direzione, nonché coloro che esercitano, anche di fatto, funzioni di gestione e controllo della stessa; i dipendenti, i collaboratori e coloro i quali, pur non appartenendo alla Società, operano su mandato della medesima.

MI.ZAR. SRL condanna qualsiasi comportamento difforme dalla legge, dalle previsioni del presente Modello e del Codice Etico, anche laddove detto comportamento sia posto in essere nell'interesse dell'Ente e/o con l'obiettivo di arrecare ad esso un vantaggio.

2.5. Approvazione, modifiche ed integrazioni del Modello

Il Modello, redatto anche con l'eventuale ausilio di professionisti, è approvato dall'Organo Amministrativo.

Le successive modifiche, che dovessero rendersi necessarie per migliorarne l'idoneità a prevenire i reati, ovvero in ragione di novità legislative, restano di competenza dell'Organo Amministrativo.
E' attribuito all'Organismo di Vigilanza il potere di proporre modifiche per migliorare gli assetti organizzativi e per adeguare il Modello alle novità legislative.

2.6. Il sistema di whistleblowing e il Dlgs n° 24/2023

MI.ZAR. SRL, al fine di garantire una gestione responsabile ed in linea con le prescrizioni legislative introdotte dal Dlgs n° 24/2023, ha adottato le linee guida ANAC "Linee Guida whistleblowing approvate con Delibera n. 311 del 12 luglio 2023" (successivamente aggiornate con delibera n. 478 del 26 novembre 2025) e la "GUIDA OPERATIVA PER GLI ENTI PRIVATI" di ottobre 2023 predisposta da Confindustria per la "NUOVA DISCIPLINA WHISTLEBLOWING".

A fronte di quanto sopra e per rispettare i vari adempimenti previsti dal Dlgs n° 24/2023 ha implementato un sistema di gestione whistleblowing che prevede:

- Comunicazione alle rappresentanze sindacali più rappresentative presenti nel territorio;
- Comunicazione ai dipendenti sull'attivazione del sistema whistleblowing;
- Predisposizione di apposita procedura (Policy Whistleblowing) resa disponibile sul sito aziendale, per descrivere dettagliatamente le fasi operative delle comunicazioni;
- Predisposizione di apposita informativa sul Whistleblowing resa disponibile sul sito aziendale;
- Individuazione e nomina del gestore delle segnalazioni;
- Attivazione di un canale informatico per le segnalazioni scritte;
- Valutazione di impatto sulla privacy del Whistleblowing;
- Aggiornamento della privacy per gli elementi di interazione (es. informative, registro trattamenti, nomine responsabile esterni del trattamento, valutazioni impatto, tempi di conservazione delle comunicazioni).

Nella Policy whistleblowing sono riportati:

- Le modalità operative per la corretta gestione delle comunicazioni e delle fasi delle stesse;
- i canali interni di segnalazione disponibili (scritto e verbale);
- i canali esterni di segnalazione (ANAC);
- i soggetti abilitati alle segnalazioni;
- i riferimenti del gestore delle segnalazioni;
- i reati che possono essere segnalati;
- le conseguenze di segnalazioni false o calunniose.

Con il sistema Whistleblowing implementato, MI.ZAR. SRL:

a) consente ai soggetti indicati nel Dlgs n° 24/2023, di presentare, a tutela dell'integrità dell'ente, segnalazioni di condotte illecite rilevanti ai sensi del presente Decreto o violazioni del presente Modello, di cui siano venuti a conoscenza in ragione delle funzioni svolte, e comunicazioni relative agli altri reati elencati nella Policy Whistleblowing;
b) garantisce la riservatezza dell'identità del segnalante;
c) vieta ogni atto di ritorsione o discriminatorio, diretto o indiretto, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
d) tutela, tramite misure *ad hoc*, il segnalato;
e) prevede, nel sistema disciplinare adottato, sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché' di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate o calunniose.

Rinviandosi all'apposita procedura per la gestione delle segnalazioni (POLICY WHISTLEBLOWING) si ricorda sin da ora che la violazione degli obblighi di riservatezza dei dati del segnalante è ritenuta alla stregua di una violazione del Modello 231 e sarà, dunque, sanzionata ai sensi del sistema sanzionatorio e disciplinare di cui al presente Modello 231 aziendale.
Il licenziamento ritorsivo o discriminatorio del soggetto segnalante sarà ritenuto nullo ed altresì nulli saranno ritenuti il mutamento di mansioni ai sensi dell'art. 2103 del Codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante.
Sarà onere dell'Amministratore Unico, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.
L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.
È altresì sanzionato il comportamento di chi effettua, con dolo o colpa grave, segnalazioni che si rivelano infondate: tale comportamento sarà ritenuto alla stregua di una grave violazione del Modello 231 e del Codice Etico.

2.7. Intelligenza artificiale: legge 132/2025

La legge 132/2025 stabilisce principi generali e ambiti applicativi che riguardano direttamente le imprese responsabili della gestione dei rischi aziendali.
In particolare, gli articoli 3, 4 e 5 della Legge 132/2025 fanno riferimento a:

- Diritti e libertà fondamentali: trasparenza, proporzionalità, accuratezza, sostenibilità, parità di genere
- Protezione dei dati personali: trattamento lecito, corretto e trasparente dei dati, in linea con il GDPR
- Sviluppo economico: promozione dell'IA per sostenere la competitività e la sovranità tecnologica del Paese.

I tre articoli della legge 132/2025 collegati ai reati contemplati nel Dlgs 231/2001 sono:

- Art. 185 TUF – Manipolazione del mercato
  → collegato all' Art. 25-sexies D.Lgs. 231/01 (Abusi di mercato)
  → rischio: utilizzo di algoritmi per influenzare i mercati
- Art. 171 L. 633/1941 comma 1, lett. a-bis – Messa a disposizione del pubblico di un'opera dell'ingegno protetta o parte di essa
  → collegato all' Art. 25-novies D.Lgs. 231/01 (Violazione del diritto d' autore)
  → rischio: uso di IA generative che riproducono contenuti protetti
- Art. 2637 c.c. – Aggiotaggio
  → collegato all' Art. 25-ter D.Lgs. 231/01 (Reati societari)
  → rischio: diffusione automatizzata di informazioni false o fuorvianti

Il rischio di commissione di questi reati nella nostra azienda è considerato molto basso. L'azienda monitorerà l'evolversi della situazione.
MI.ZAR. SRL riconosce le opportunità offerte dall'impiego dei sistemi di intelligenza artificiale per il miglioramento delle attività di consulenza, gestione documentale, ricerca normativa, formazione, analisi dei dati e supporto ai processi aziendali.

L'utilizzo di tali sistemi deve avvenire nel rispetto del Regolamento (UE) 2024/1689, della Legge 23 settembre 2025, n. 132, del D.Lgs. 9 settembre 2026, n. 160, della disciplina relativa alla protezione dei dati personali e delle altre disposizioni applicabili.

2.7.1. Nuovi reati-presupposto

Il D.Lgs. 160/2026 ha introdotto nel D.Lgs. 231/2001 l'art. 25-vicies, relativo ai reati commessi con l'uso di sistemi di intelligenza artificiale.

Le fattispecie considerate sono:

a) Art. 437-bis c.p. – Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi;

b) Art. 612-quater c.p. – Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale.

Restano inoltre rilevanti le ulteriori fattispecie già richiamate dal Modello aziendale, qualora l'intelligenza artificiale venga utilizzata come strumento per commetterle.

2.7.2. Valutazione dei rischi

MI.ZAR. SRL provvede a individuare i sistemi di intelligenza artificiale utilizzati, le finalità del loro impiego, i processi interessati, i soggetti autorizzati e gli eventuali rischi di commissione dei reati-presupposto.

La valutazione tiene conto, in particolare:

- della classificazione dei sistemi ai sensi del Regolamento (UE) 2024/1689;

- dell'eventuale utilizzo di sistemi IA ad alto rischio;
- della presenza di misure tecniche e organizzative di sicurezza;
- dell'effettività della sorveglianza umana, ove applicabile;
- dell'eventuale generazione e diffusione di contenuti audiovisivi artificiali;
- delle modalità di verifica dei risultati prodotti dai sistemi IA;
- delle attività affidate a fornitori esterni.

Gli esiti della valutazione sono documentati nell'allegato aziendale di risk assessment e riesaminati in caso di modifiche significative.

2.7.3. Regole di comportamento e controlli

I destinatari del Modello devono utilizzare esclusivamente i sistemi IA autorizzati dalla Società e rispettare le relative istruzioni operative.

È vietato:

- alterare illecitamente sistemi IA o eludere le misure di sicurezza e sorveglianza umana previste;
- utilizzare sistemi IA per finalità illecite;
- diffondere senza consenso contenuti audiovisivi artificialmente generati o alterati quando ricorrono le condizioni di illiceità previste dalla legge;
- utilizzare risultati generati dall'IA senza le verifiche professionali prescritte;
- inserire informazioni riservate, dati personali o documenti dei clienti in sistemi IA in violazione delle istruzioni aziendali.

I documenti, le valutazioni tecniche e i pareri professionali predisposti con il supporto dell'intelligenza artificiale rimangono soggetti alla responsabilità e alla verifica dei professionisti incaricati.

2.7.4. Responsabilità e vigilanza

L'Organo Amministrativo assicura l'individuazione delle responsabilità per l'autorizzazione, la gestione e il controllo dei sistemi IA.

L'Organismo di Vigilanza, nell'ambito delle proprie competenze, verifica l'adeguatezza e l'effettiva applicazione delle misure organizzative adottate per prevenire i reati-presupposto.

Eventuali violazioni, anomalie significative o situazioni potenzialmente riconducibili all'art. 25-vicies devono essere comunicate secondo i flussi informativi previsti dal Modello.

2.7.5. Formazione e aggiornamento

MI.ZAR. SRL assicura ai soggetti coinvolti una formazione proporzionata alle modalità di utilizzo dei sistemi IA e ai rischi associati.

La valutazione dei rischi, i protocolli di controllo e le istruzioni operative vengono riesaminati periodicamente e in occasione di modifiche normative, organizzative o tecnologiche significative.

Il testo proposto costituisce una base di revisione organizzativa: non equivale, da solo, a dimostrare l'efficace attuazione delle misure preventive.

3. Organismo di Vigilanza

3.1. Composizione e requisiti

Tra le condizioni di esonero dalla responsabilità amministrativa delle persone giuridiche, l'art. 6, comma 1, lettera *b* del D.lgs. n. 231 del 2001, individua la nomina di "*un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo*" cui è affidato il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento.
La legge non fornisce puntuali indicazioni circa la composizione dell'Organismo di Vigilanza (di seguito OdV): ciò consente di optare per una composizione monosoggettiva oppure per una composizione plurisoggettiva. In quest'ultimo caso, possono essere chiamati a comporre l'OdV soggetti interni o esterni all'Ente purché dotati dei requisiti di seguito precisati.
Il D.lgs. n. 231 del 2001 non individua l'organo competente alla designazione dell'OdV (organo amministrativo o assemblea dei soci): si ritiene, tuttavia, che la nomina spetti all'Organo amministrativo cui l'art. 6 del Decreto attribuisce il potere di adottare il Modello di Organizzazione e Gestione.

La prima nomina dell'OdV avviene con la stessa delibera di approvazione e adozione del Modello. Successivamente, è rinnovato con apposita decisione dell'Organo amministrativo e resta in carica per il numero di esercizi sociali da quest'ultimo stabilita nell'atto di nomina.
La nomina dei membri dell'OdV (in ipotesi di OdV plurisoggettivo) o dell'unico componente (in ipotesi di OdV monosoggettivo) deve essere resa nota a ciascun componente nominato e da questi formalmente accettata per iscritto con apposita dichiarazione che attesti il possesso dei requisiti richiesti dalla norma.
Quanto ai contenuti dell'incarico, nel silenzio della legge, si ritiene necessaria, ai fini del corretto inquadramento giuridico-funzionale dell'Organismo, l'esplicitazione dei seguenti elementi: funzioni, durata, cause di decadenza, compenso, obblighi e responsabilità.

L'OdV plurisoggettivo nominerà tra i suoi componenti il Presidente cui sarà affidato, tra gli altri, il compito di espletare le formalità relative alla convocazione, alla fissazione degli argomenti da trattare di volta in volta e allo svolgimento delle riunioni collegiali.
L'Organo amministrativo approva altresì lo Statuto dell'Organismo di Vigilanza il quale disciplina, tra le altre cose, nomina e composizione, durata in carica, cessazione, riporto gerarchico, riporto informativo, requisiti di professionalità e onorabilità, cause di ineleggibilità e incompatibilità e risorse finanziarie da attribuire.

L'Organismo di Vigilanza è dotato di autonomi poteri di iniziativa e controllo, intesi questi come libertà d'azione e di autodeterminazione.
L'OdV ha diritto di accesso, senza necessità di autorizzazione, a tutti gli atti della Società.
In considerazione della peculiarità delle proprie attribuzioni e dei propri requisiti professionali, l'Organismo di Vigilanza, nello svolgimento dell'attività di sua competenza, si avvarrà del supporto di quelle funzioni aziendali dell'Ente che si rendessero utili per il perseguimento dello scopo.
L'OdV nominato, in conformità alle disposizioni del d. lgs. n. 231 del 2001, deve avere i seguenti requisiti: autonomia, indipendenza, professionalità, onorabilità e continuità d'azione.
Tali requisiti sembrano assicurati dall'inserimento dell'Organismo in esame quale unità di staff in una posizione gerarchica la più elevata possibile e prevedendo che lo stesso debba riferire unicamente al massimo vertice aziendale, Amministratore unico o Consiglio di Amministrazione che sia.
Per assicurare la necessaria autonomia è indispensabile che l'OdV non abbia all'interno dell'Ente alcuna mansione operativa che potrebbe comprometterne l'obbiettività di giudizio e che lo stesso possa svolgere la propria funzione in assenza di qualunque interferenza e condizionamento da parte dell'Ente ed in particolare del managment aziendale.
Il requisito dell'indipendenza, pur non espressamente richiamato dal Decreto, viene incluso tra quelli richiesti all'OdV, in quanto individua la necessaria assenza di conflitto d'interesse nei confronti dell'Ente e, quindi, del suo *management*.
Il requisito della professionalità si riferisce alle competenze tecnico-professionali richieste all'OdV, che devono essere adeguate alle funzioni che lo stesso è chiamato a svolgere.
Nonostante l'assenza nel testo normativo di qualsivoglia indicazione circa la professionalità richiesta all'OdV, stando agli orientamenti giurisprudenziali, si ritiene che debba essere in possesso di competenze di carattere aziendalistico, in quanto chiamato a vigilare sull'osservanza del Modello.
Quanto alle competenze giuridiche, atteso lo scopo di prevenire il compimento di reati, è essenziale la conoscenza della struttura e delle modalità di commissione degli illeciti penali.
Il requisito dell'onorabilità attiene alla persona investita della funzione di OdV: ciascun soggetto investito di tale funzione deve infatti avere un profilo etico di indiscutibile valore. Il requisito dell'onorabililtà è valutata in base a quanto già previsto per gli altri settori della normativa societaria (Collegio sindacale, Controllo interno, Casellario Giudiziario).
Quanto al requisito della continuità d'azione, l'OdV:
- svolge in modo continuativo le attività necessarie di vigilanza con adeguato impegno e con i necessari poteri di indagine;
- redige un verbale, trasmesso all'Amministratore Unico, in cui sono descritte le attività svolte nel corso della singola verifica e le indicazioni utili al miglioramento dell'assetto organizzativo;
- cura l'attuazione del Modello e ne assicura il costante aggiornamento.

3.2. Funzioni e poteri dell'Organismo di Vigilanza

L'OdV ha le seguenti competenze:

- vigilare costantemente affinché i Destinatari del Modello recepiscano ed osservino le prescrizioni in esso contenute (funzione ispettiva e repressiva dei reati);
- verificare i risultati raggiunti nell'applicazione del Modello in ordine alla prevenzione di reati e valutare la necessità di proporre modifiche dello stesso.

Qualora emerga che lo stato di attuazione degli standard operativi richiesti sia carente, spetta all'Organismo di Vigilanza adottare tutte le iniziative necessarie per correggere tale condizione:

- sollecitando i responsabili delle singole unità organizzative al rispetto dei modelli di comportamento;
- indicando direttamente quali correzioni e modifiche debbano essere apportate ai protocolli;
- segnalando i casi di mancata attuazione del Modello ai responsabili e agli addetti ai controlli all'interno delle singole funzioni.

Qualora, invece, dal monitoraggio dello stato di attuazione del Modello emerga la necessità del suo adeguamento, l'OdV deve assumere le iniziative necessarie affinché vengano apportati, in tempi brevi, i necessari aggiornamenti.

Nello svolgimento dell'attività di controllo, l'OdV deve:

- effettuare interventi periodici volti all'accertamento dell'applicazione del Modello ed in particolare vigilare affinché le procedure ed i controlli da esso contemplati siano posti in essere e documentati in maniera conforme ed i principi etici siano rispettati;
- segnalare eventuali carenze e/o inadeguatezze del Modello nella prevenzione dei reati di cui al D.lgs. n. 231 del 2001;
- suggerire procedure di verifica adeguate;
- avviare indagini interne straordinarie laddove sia evidenziata o sospettata la violazione del Modello ovvero la commissione di reati;
- verificare periodicamente gli atti societari più significativi ed i contratti di maggior rilievo conclusi dall' Ente nell'ambito delle aree a rischio;
- promuovere iniziative per diffondere la conoscenza e l'effettiva comprensione del Modello tra i dipendenti, i collaboratori e i terzi che, comunque, abbiano rapporti con l'Ente, predisponendo la documentazione interna (istruzioni, chiarimenti, aggiornamenti) ovvero specifici seminari di formazione, necessari affinché il Modello possa essere compreso ed applicato;
- coordinarsi con i responsabili delle varie funzioni aziendali per il controllo delle attività nelle aree a rischio e confrontarsi con essi su tutte le problematiche relative all'attuazione del Modello;
- coordinarsi con le altre funzioni aziendali;
- richiedere l'eventuale aggiornamento del Modello;

- richiedere l'aggiornamento periodico della mappa delle attività a rischio e verificarne l'effettivo aggiornamento attraverso il compimento di verifiche periodiche puntuali e mirate sulle attività a rischio. A tal fine, all'OdV devono essere segnalate da parte degli amministratori e degli addetti alle attività di controllo, nell'ambito delle singole funzioni, le eventuali situazioni che possono esporre l'Ente a rischio di illecito amministrativo dipendente da reato;
- raccogliere, elaborare e conservare tutte le informazioni rilevanti ricevute sul rispetto del Modello;
- verificare che le norme previste dalle singole Parti Speciali del presente Modello siano comunque adeguate e rispondenti alle esigenze di osservanza di quanto prescritto dal D.lgs. n. 231 del 2001; a tal fine, l'OdV deve avere libero accesso, senza la necessità di alcun consenso preventivo, a tutta la documentazione societaria, nonché la possibilità di acquisire dati ed informazioni rilevanti dai soggetti responsabili.

L'Organismo di Vigilanza ha altresì la facoltà di avvalersi di consulenti esterni qualora vi sia la necessità di avere un parere che presuppone un'adeguata conoscenza professionale della materia.

Infine, in relazione agli aspetti concernenti la calendarizzazione delle attività, le modalità di verbalizzazione delle riunioni, la disciplina dei flussi informativi, le deleghe interne sulle verifiche in ordine alla materia di competenza, l'Organismo di Vigilanza si dota di un regolamento interno che deve essere trasmesso all'Organo amministrativo.

3.3. Flussi informativi provenienti dall'Organismo di Vigilanza

L'OdV trasmette senza ritardo all'Organo amministrativo i verbali delle verifiche periodiche indicando le eventuali prescrizioni per l'effettiva applicazione del Modello e le ipotesi di violazione dello stesso.

Nei confronti dell'Organo amministrativo, l'OdV ha la responsabilità di:

- comunicare, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere per adempiere ai compiti assegnatigli;
- comunicare periodicamente lo stato di avanzamento del programma definito ed eventuali cambiamenti apportati al piano;
- comunicare immediatamente eventuali problematiche significative scaturite dalle attività;
- relazionare, almeno semestralmente, in merito all'attuazione del Modello;
- l'OdV potrà essere convocato, o chiedere di essere convocato, in qualsiasi momento dai suddetti organi, per riferire sul funzionamento del Modello o su altre situazioni specifiche che si dovessero verificare nello svolgimento della propria attività.

L'OdV potrà, inoltre, valutando le singole circostanze:

- comunicare i risultati dei propri accertamenti ai responsabili delle funzioni e/o dei processi, qualora dalle attività scaturissero aspetti suscettibili di miglioramento;
- segnalare eventuali comportamenti e/o azioni non in linea con il Modello e con le procedure aziendali al fine di:
  - acquisire, sulla base di specifiche segnalazioni ricevute o di dati oggettivi riscontrati, tutti gli elementi da eventualmente comunicare alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
  - evitare il ripetersi dell'accadimento, dando indicazioni per la rimozione delle carenze.

Le attività indicate al punto precedente dovranno, nel più breve tempo possibile, essere comunicate dall'OdV all'Organo amministrativo, richiedendo anche il supporto delle strutture aziendali in grado di collaborare nell'attività di accertamento e nell'individuazione delle azioni idonee ad impedire il ripetersi di tali circostanze.

3.4. Flussi informativi verso l'Organismo di Vigilanza

Al fine di agevolare l'attività di vigilanza sull'efficacia del Modello qualsiasi informazione, comunicazione e documentazione, anche se proveniente da terzi, riguardante o, comunque, connessa all'attuazione del Modello deve essere inoltrata all'OdV.
I dipendenti e gli organi societari devono segnalare all'OdV le notizie relative alla commissione o alla ragionevole convinzione di commissione, di reati, ovvero notizie in merito a comportamenti non in linea con il Modello.
Le segnalazioni devono essere effettuate in forma scritta e non anonima.
Le informazioni acquisite dall' OdV sono trattate, in aderenza al Codice Etico, in modo da garantire il rispetto della persona, della dignità umana e della riservatezza e da evitare per i segnalanti qualsiasi forma di ritorsione, penalizzazione o discriminazione.
L' OdV valuta le segnalazioni ricevute con discrezionalità e responsabilità. A tal fine, potrà ascoltare l'autore della segnalazione, le persone informate sui fatti ed il soggetto nei cui confronti è ipotizzabile la violazione del Modello.
I dipendenti e gli amministratori non possono rifiutare di essere sentiti dall'OdV.
Le dichiarazioni vengono verbalizzate nelle forme previste dal Regolamento dell'OdV.

3.5. Informazioni obbligatorie e deleghe

Sono considerate informazioni da trasmettere obbligatoriamente all' OdV, a prescindere da un'esplicita richiesta, quelle riguardanti:

- le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al d. lgs. n. 231 del 2001;
- provvedimenti e/o notizie, relative alla Società, provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo

svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al d. lgs. n. 231 del 2001;
- le richieste di assistenza legale inoltrate dagli Amministratori, dai Dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dal d. lgs. n. 231 del 2001;
- le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- le relazioni preparate da responsabili delle varie funzioni aziendali da cui emergano fatti, eventi o omissioni anche solo potenzialmente ricollegabili alle fattispecie di reato previste dal d. lgs. n. 231 del 2001;
- le informazioni sull'evoluzione delle attività attinenti alle aree a rischio individuate dal Modello e/o sulle modifiche dell'organizzazione aziendale;
- gli aggiornamenti della valutazione dei rischi aziendali come redatta ai sensi dell'art. 28 e 29 del d. lgs. n. 81/08;
- gli infortuni sul lavoro e le malattie professionali;
- i risultati della sorveglianza sanitaria che contemplino inidoneità parziali e totali a mansioni specifiche;
- gli aggiornamenti e modifiche dell'organizzazione del lavoro;
- l'organigramma aziendale, il sistema delle deleghe di funzioni e qualsiasi modifica ad esso riferita.

3.6. Il sistema di whistleblowing

In aggiunta a quanto riportato nel paragrafo 2.6, si stabilisce che è compito dell'ODV valutare la corretta applicazione del sistema WHISTLEBLOWING, essendo lo stesso previsto nell'art 6 del Dlgs 231/2001 come rivisto dal Dlgs 24/2023.
Le segnalazioni che il gestore delle comunicazioni rientranti nel sistema whistleblowing riceve, se accettate, devono essere comunicate all'ODV nel rispetto dei doveri di riservatezza.

4. Formazione ed informativa

4.1. Formazione ed informativa al personale

MI.ZAR. SRL ritiene che, ai fini dell'efficacia del Modello, sia necessario garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute, sia nei confronti dei dipendenti sia nei confronti dei c.d. Esterni. Tale obbiettivo riguarda tutte le risorse aziendali, sia che si tratti di risorse già presenti in Azienda che di risorse da inserire.
MI.ZAR. SRL effettua (destinando a tal fine risorse tanto finanziarie quanto umane) programmi di formazione ed informazione attuati con differente livello di approfondimento in relazione al diverso grado di coinvolgimento delle risorse medesime nelle c.d. attività sensibili.

La formazione del personale è considerata dalla Società condizione necessaria per l'attuazione del Modello, da effettuarsi periodicamente e con modalità che garantiscano l'obbligatorietà di partecipazione ai corsi, i controlli sulla frequenza, sulla qualità dei contenuti dei programmi e la verifica dell'apprendimento.
La formazione del personale ai fini dell'attuazione del Modello è gestita dall'amministrazione in stretta cooperazione con l'OdV e sarà articolata sui livelli qui di seguito indicati:
a. Personale direttivo e con funzioni di rappresentanza dell'ente:
- seminario iniziale esteso di volta in volta a tutti i neo assunti;
- seminario di aggiornamento annuale;
- occasionali e-mail di aggiornamento;
- informativa nella lettera di assunzione per i neoassunti;
b. altro Personale:
- nota informativa interna;
- informativa nella lettera di assunzione per i neo assunti;
- e-mail di aggiornamento.
Le modalità operative per l'attuazione e la verbalizzazione della formazione sono state integrate nel processo di gestione del personale presente nel sistema qualità.

4.2. Informativa ai soggetti esterni ed ai consulenti

L'attività di comunicazione dei contenuti del Modello è indirizzata anche nei confronti di soggetti terzi che intrattengono con MI.ZAR. SRL rapporti di collaborazione contrattualmente regolati o che rappresentano la Società senza vincoli di dipendenza (partner commerciali, agenti, consulenti, distributori, procacciatori d'affari e altri collaboratori autonomi).
A tal fine, ai soggetti terzi più significativi la Società fornirà un estratto descrittivo del Modello, del Codice Etico (allegato 01_03) e del Sistema Disciplinare (allegato 01_04).
Si provvederà, altresì, alla pubblicazione del Modello e del Codice Etico sul sito web della Società.

5. Sistema Disciplinare

5.1. Principi generali

Aspetto essenziale per l'effettività del Modello è la predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta imposte ai fini della prevenzione dei reati di cui al D. Lgs. n. 231 del 2001 e, in generale, delle procedure interne previste dal Modello stesso.
Ai sensi dell'art. 6 comma 2, lettera e) e dell'articolo 7, comma 4, lettera b), infatti, il Modello può ritenersi efficacemente attuato e, quindi, può avere valore scriminante, solo qualora preveda un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure in esso indicate.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale in quanto le regole di condotta, i protocolli e le procedure interne sono vincolanti per i destinatari, indipendentemente dall'effettiva realizzazione di un reato quale conseguenza del comportamento commesso.

5.2. Misure per i lavoratori dipendenti

Il mancato rispetto e/o la violazione delle regole di comportamento ad opera di lavoratori dipendenti della Società costituisce inadempimento alle obbligazioni derivanti dal rapporto di lavoro *ex* art. 2104 del Codice civile e dà luogo all'applicazione delle sanzioni disciplinari. Le sanzioni irrogabili saranno applicate nel rispetto di quanto previsto dalla Legge e dal Contratto Collettivo Nazionale di Lavoro applicato (CONTRATTO COLLETTIVO NAZIONALE DI LAVORO PER I DIPENDENTI DA AZIENDE DEL COMMERCIO, DEI SERVIZI E DEL TERZIARIO).

5.3. Misure nei confronti di dirigenti e di amministratori

In caso di violazione, da parte di dirigenti, delle regole di comportamento, la Società valuterà i fatti ed i comportamenti ed assumerà le opportune iniziative nei confronti dei responsabili, ai sensi delle disposizioni di legge e di Contratto Collettivo Nazionale applicabile, tenuto presente che tali violazioni costituiscono inadempimento delle obbligazioni derivanti dal rapporto di lavoro.

5.4. Misure nei confronti di collaboratori, consulenti e altri terzi

Ogni comportamento posto in essere dai fornitori, collaboratori, dai consulenti o da altri terzi collegati a MI.ZAR. SRL da un rapporto contrattuale non di lavoro dipendente in violazione delle previsioni del Modello potrà determinare, nelle ipotesi di maggiore gravità, anche la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla Società, e ciò anche indipendentemente dalla risoluzione del rapporto contrattuale.

5.5. Sistema disciplinare

Il Sistema Disciplinare adottato da MI.ZAR. SRL. è allegato al presente Modello di Organizzazione e Gestione, 01_04 Sistema Disciplinare.

6. Modello e Codice Etico

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice Etico, pur avendo il Modello, per le finalità che esso intende perseguire in attuazione alla disciplina di cui al D.Lgs. n. 231 del 2001, una diversa natura giuridica. Sotto tale profilo, infatti:

- il Codice Etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale da parte dell'Ente allo scopo di esprimere dei principi di "deontologia aziendale" che la stessa riconosce come propri e sui quali richiama l'osservanza da parte di tutti i dipendenti, dirigenti, amministratori, collaboratori esterni;
- il Modello risponde, invece, a specifiche prescrizioni contenute nel D.lgs. n. 231 del 2001, finalizzate a prevenire la commissione di particolari tipologie di reati commessi nell'interesse o a vantaggio dell'Ente.

Il Codice Etico adottato da MI.ZAR. SRL è allegato al presente Modello di Organizzazione e Gestione, 01_03 Codice Etico.

7. Allegati richiamati in questo documento

Costituiscono allegati al presente Modello:

- 01_01_ORGANIGRAMMA
- 01_02_RISK ASSESSMENT PER SINGOLO REATO
- 01_03_CODICE ETICO
- 01_04_SISTEMA DISCIPLINARE
- 01_05_WHISTLEBLOWING

PARTE SPECIALE

1. I Reati contro la Pubblica Amministrazione (artt. 24 e 25 del Decreto)

1.1. I reati

La presente Parte Speciale è aggiornata tenendo conto delle modifiche intervenute sul catalogo dei reati presupposto di cui agli artt. 24 e 25 del D. Lgs. n. 231/2001. Per MI.ZAR. SRL assumono particolare rilievo i rapporti con Pubbliche Amministrazioni, enti pubblici, organismi dell'Unione europea, autorità di vigilanza e soggetti incaricati di pubbliche funzioni o pubblici servizi.

Rientrano nell'art. 24 del Decreto, tra gli altri, i seguenti reati:

- malversazione di erogazioni pubbliche (art. 316-bis c.p.);
- indebita percezione di erogazioni pubbliche (art. 316-ter c.p.);
- turbata libertà degli incanti (art. 353 c.p.) e turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.);
- truffa in danno dello Stato o di altro ente pubblico o dell'Unione europea (art. 640, comma 2, n. 1, c.p.) e truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
- frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.);
- frode nelle pubbliche forniture (art. 356 c.p.) e frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale, nei casi previsti dall'art. 2 della L. 23 dicembre 1986, n. 898.

Rientrano nell'art. 25 del Decreto, tra gli altri, i reati di concussione, corruzione e traffico di influenze illecite, nonché - nei casi e alle condizioni previste dalla norma - peculato e indebita destinazione di denaro o cose mobili:

- peculato (art. 314, primo comma, c.p.), indebita destinazione di denaro o cose mobili (art. 314-bis c.p.) e peculato mediante profitto dell'errore altrui (art. 316 c.p.), nelle ipotesi rilevanti ai sensi dell'art. 25;
- concussione (art. 317 c.p.); corruzione per l'esercizio della funzione (art. 318 c.p.); corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.); circostanze aggravanti (art. 319-bis c.p.); corruzione in atti giudiziari (art. 319-ter c.p.);
- induzione indebita a dare o promettere utilità (art. 319-quater c.p.); corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.); pene per il corruttore (art. 321 c.p.); istigazione alla corruzione (art. 322 c.p.);
- fattispecie relative a membri e funzionari dell'Unione europea, di Stati esteri e di organizzazioni internazionali richiamate dall'art. 322-bis c.p.; traffico di influenze illecite (art. 346-bis c.p.).

L'abuso d'ufficio (art. 323 c.p.) è stato abrogato dalla L. 9 agosto 2024, n. 114 e non costituisce più reato presupposto; il D.L. 4 luglio 2024, n. 92, convertito dalla L. 8 agosto 2024, n. 112, ha invece inserito nel perimetro dell'art. 25 l'art. 314-bis c.p.

1.2. Aree a rischio

- Gestione dei rapporti con soggetti pubblici per l'ottenimento di permessi, autorizzazioni e licenze per l'esercizio delle attività aziendali.

- Partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti agevolati da parte di organismi pubblici italiani o comunitari ed il loro concreto impiego.
- Rapporti istituzionali con la Pubblica Amministrazione.
- Gestione dei controlli/ispezioni esterni e rapporti con le pubbliche autorità preposte a controlli/ispezioni sulla sicurezza nei luoghi di lavoro.
- Gestione di adempimenti, verifiche, ispezioni a fronte della produzione di rifiuti solidi, liquidi o gassosi, ovvero dell'emissione di fumi o della produzione di inquinamento acustico/elettromagnetico soggetti a controlli da parte di soggetti pubblici.
- Rappresentanza in giudizio della società e partecipazione di soggetti appartenenti alla società a procedimenti giudiziali.
- Processo di selezione e assunzione del personale.
- Gestione della liquidità e contabilità.
- Gestione di omaggi/pubblicità.
- Partecipazione a gare, procedure negoziate, affidamenti, concessioni e altri procedimenti di scelta del contraente pubblico, comprese le attività di predisposizione della documentazione, presentazione dell'offerta ed esecuzione del contratto.
- Gestione di contributi, sovvenzioni, incentivi, crediti d'imposta, finanziamenti o altre risorse di provenienza pubblica o europea, inclusa la verifica della destinazione delle somme.

1.3. Divieti

Divieti generali

È fatto espresso divieto ai Destinatari di porre in essere:

- comportamenti tali da integrare le fattispecie di reato previste dagli artt. 24 e 25 del D. Lgs. n. 231/2001;
- comportamenti che, sebbene non siano tali da costituire di per sé fattispecie di reato rientranti tra quelle previste dagli artt. 24 e 25 del D. Lgs. n. 231/2001, possano considerarsi propedeutiche alla commissione degli stessi;
- comportamenti da cui derivino situazioni di conflitto di interessi nei confronti della Pubblica Amministrazione, in relazione a quanto previsto dalle suddette ipotesi di reato.

Divieti specifici

È fatto divieto, in particolare, di:

- effettuare elargizioni in denaro o accordare vantaggi di qualsiasi natura (ad esempio, la promessa di assunzione) a funzionari pubblici;
- distribuire e/o ricevere omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire, ogni forma di regalo offerto o, ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque, finalizzato ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa) o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per la Società. Gli omaggi consentiti si caratterizzano sempre

per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere artistico (ad esempio, la distribuzione di libri d'arte) o la brand image della Società. I regali offerti - salvo quelli di modico valore - devono essere documentati in modo idoneo per consentire all'OdV di effettuare le verifiche al riguardo;

- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti a scopi diversi da quelli cui erano destinati.
- alterare, condizionare o turbare, direttamente o indirettamente, lo svolgimento di gare, procedure di affidamento o procedimenti di scelta del contraente, anche mediante accordi collusivi, scambio di informazioni riservate, rinunce concordate o altri artifici;
- destinare erogazioni, contributi, finanziamenti o altre risorse pubbliche a finalità diverse da quelle previste dal provvedimento di concessione, dalla legge o dagli atti vincolanti applicabili;
- utilizzare relazioni, intermediazioni o promesse di utilità per influenzare illecitamente l'operato di pubblici ufficiali o incaricati di pubblico servizio.

1.4. Procedure specifiche per aree sensibili

È fatto espresso obbligo di:

- osservare rigorosamente tutte le leggi e i regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione e alle attività relative allo svolgimento di una pubblica funzione o di un pubblico servizio;
- gestire qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza.

Al fine di prevenire l'attuazione dei comportamenti vietati:

- nessun tipo di pagamento può essere effettuato in contanti o in natura;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento di attività quali pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitari etc., devono porre particolare attenzione all'attuazione degli adempimenti stessi e riferire immediatamente al proprio superiore o all'OdV eventuali situazioni di irregolarità;
- su ogni singola attività sensibile è opportuno predisporre e formalizzare evidenza dei controlli in essere ed effettuare un monitoraggio periodico delle procedure al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù delle nuove esigenze normative;
- predisporre e formalizzare evidenze al fine di documentare la corretta applicazione della procedura di partecipazione prevista dal bando, della fase di ricezione della informazione circa la natura del bando cui si vorrà partecipare (ovvero il modo con cui si è venuti a conoscenza del bando), sia con riferimento alla valutazione del bando stesso, alla sua approvazione, che alla predisposizione e spedizione della documentazione all'Ente che indice il relativo bando;

- effettuare controlli sulla documentazione attestante l'esistenza di condizioni essenziali per partecipare ai bandi sia direttamente che tramite *outsourcer*, sugli enti contattati, sulle delibere autorizzative alla partecipazione alla gara, sull'integrità della busta accompagnatoria della documentazione necessaria per partecipare al bando;
- procedere alla tracciabilità e verificabilità ex post delle transazioni, fatte con la Pubblica Amministrazione tramite adeguati supporti documentali/informativi;
- è necessario che durante eventuali ispezioni giudiziarie, tributarie e amministrative poste in essere dalle Autorità di Vigilanza di settore (quali ad esempio quelle preposte al rispetto della normativa sulla sicurezza, alle verifiche tributarie, INPS) nonché in ogni atto propedeutico alla richiesta di autorizzazioni, licenze o altro, partecipino i soggetti a ciò espressamente delegati. Di tutto il procedimento relativo all'ispezione devono essere redatte e conservate apposite evidenze. Nel caso in cui il verbale conclusivo evidenziasse criticità, l'OdV deve essere informato con nota scritta da parte del responsabile della funzione coinvolta.

1.5. Presidi adottati

PGM-A PROCEDURA GENERALE DI PREVENZIONE
PGM–B PROCEDURA GENERALE DI CONTROLLO
PGM–G PAGAMENTI
CODICE ETICO LETT. C - CRITERI DI CONDOTTA NEI CONFRONTI DELLA PA

2. I Delitti informatici e trattamento illecito di dati (art. 24 bis)

2.1. I reati

L'art. 24-bis del D. Lgs. n. 231/2001, introdotto dalla L. 18 marzo 2008, n. 48, è stato oggetto di successive modifiche, da ultimo con la L. 28 giugno 2024, n. 90. Il catalogo oggi comprende le seguenti principali fattispecie:

- accesso abusivo a un sistema informatico o telematico (art. 615-ter c.p.); detenzione, diffusione e utilizzo abusivo di codici di accesso (art. 615-quater c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche e condotte relative ad apparecchiature destinate a tali attività (artt. 617-quater e 617-quinquies c.p.);
- danneggiamento di informazioni, dati, programmi e sistemi informatici o telematici, anche di interesse pubblico o pubblica utilità (artt. 635-bis, 635-ter, 635-quater e 635-quinquies c.p.);
- estorsione realizzata mediante condotte informatiche nelle ipotesi previste dall'art. 629, terzo comma, c.p.;
- detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi diretti a danneggiare o interrompere sistemi informatici o telematici (art. 635-quater.1 c.p.);
- falsità in documenti informatici (art. 491-bis c.p.) e frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.);
- violazioni previste dall'art. 1, comma 11, del D.L. 21 settembre 2019, n. 105 in materia di perimetro di sicurezza nazionale cibernetica.

Le fattispecie relative agli strumenti di pagamento diversi dai contanti sono disciplinate separatamente dall'art. 25-octies.1 e non sono ricomprese, in quanto tali, nel presente art. 24-bis.

2.2. Aree a rischio

- Gestione dei sistemi informatici aziendali al fine di assicurarne il funzionamento e la manutenzione, l'evoluzione della piattaforma tecnologica e applicativa IT nonché la Sicurezza Informatica.
- Tutte le attività aziendali svolte dai Destinatari tramite l'utilizzo dei sistemi informatici aziendali, del servizio di posta elettronica e dell'accesso ad Internet.
- Gestione di account privilegiati, credenziali, accessi da remoto, servizi cloud, backup e configurazioni di sicurezza.
- Gestione di incidenti cyber, ransomware, tentativi di estorsione informatica e rapporti con fornitori IT o amministratori di sistema esterni.

2.3. Divieti

Divieti generali
È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, promuovere, collaborare o dare causa a comportamenti tali da integrare le fattispecie rientranti tra i reati informatici come richiamati dall'art 24 bis del D. Lgs. n. 231/2001;
- porre in essere comportamenti che, sebbene non risultino tali da costituire di per sé ipotesi di reato rientranti tra quelle sopra descritte, possano potenzialmente diventarle;
- utilizzare anche occasionalmente la Società o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei reati di cui all'art. 24 bis del D. Lgs. n. 231/2001.

Divieti specifici
È fatto divieto, in particolare, di:

- acquisire, possedere o utilizzare strumenti software e/o hardware - se non per casi debitamente autorizzati ovvero in ipotesi in cui tali software e/o hardware siano utilizzati per il monitoraggio della sicurezza dei sistemi informatici aziendali - che potrebbero essere adoperati abusivamente per compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le Credenziali, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.);
- accedere abusivamente ad un sistema informatico altrui - ovvero nella disponibilità di altri dipendenti o terzi - nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;
- manomettere, sottrarre o distruggere il patrimonio informatico aziendale di clienti o di terze parti, comprensivo di archivi, dati e programmi;
- sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi.

2.4. Procedure specifiche per aree sensibili

È fatto espresso obbligo di:

- informare adeguatamente i Destinatari autorizzati all'utilizzo dei sistemi informatici, dell'importanza di mantenere le proprie credenziali di accesso confidenziali e di non divulgare le stesse a soggetti terzi;
- prevedere attività di formazione e addestramento periodico in favore dei dipendenti, diversificate in ragione delle rispettive mansioni al fine di diffondere una chiara consapevolezza sui rischi derivanti da un utilizzo improprio delle risorse informatiche aziendali;
- impostare le postazioni di lavoro in modo tale che, qualora non vengano utilizzate per un determinato periodo di tempo, si blocchino automaticamente;
- limitare gli accessi ai server unicamente al personale autorizzato;
- proteggere, per quanto possibile, ogni sistema informatico al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;

- dotare i sistemi informatici di adeguato software firewall e antivirus prevenendone, ove possibile, la disattivazione;
- impedire l'installazione e l'utilizzo di software non approvati dallo MI.ZAR. SRL e non correlati con l'attività professionale espletata per la stessa;
- prevedere un procedimento di autenticazione mediante l'utilizzo di credenziali al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ciascuno dei dipendenti, degli stagisti e degli altri soggetti - come ad esempio i collaboratori esterni - eventualmente autorizzati all'utilizzo dei sistemi informatici;
- limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei dipendenti, degli stagisti e degli altri soggetti (come, ad esempio, i collaboratori esterni) eventualmente autorizzati all'utilizzo dei Sistemi Informatici;
- provvedere senza indugio alla cancellazione degli account attribuiti agli amministratori di sistema una volta concluso il relativo rapporto contrattuale;
- nei rapporti con parti terze, richiedere l'impegno al rispetto degli obblighi di legge in tema di reati Informatici e prevedere apposita clausola contrattuale che richieda l'impegno al rispetto degli obblighi di legge in tema di reati informatici, delle norme di cui al D. Lgs. n. 231/2001 nonché del presente Modello e regoli le conseguenze della loro violazione.
- adottare, ove tecnicamente applicabile, autenticazione a più fattori per accessi privilegiati, remoti e ai servizi critici;
- gestire aggiornamenti, patch e vulnerabilità con criteri di priorità e con evidenza delle attività svolte;
- mantenere sistemi di registrazione degli accessi e degli eventi rilevanti, coerentemente con la normativa privacy e con le esigenze di sicurezza;
- predisporre backup protetti e periodicamente verificati, nonché procedure per la gestione e l'escalation degli incidenti informatici;
- sottoporre i fornitori IT che accedono ai sistemi o ai dati aziendali a regole contrattuali di sicurezza, riservatezza, gestione delle credenziali e segnalazione degli incidenti.

2.5. Presidi adottati

SISTEMA PRIVACY
REGOLAMENTO INTERNO PER L'USO DI STRUMENTI INFORMATICI
CODICE ETICO
PGM-E PROCEDURA CONTRATTUALE GENERALE

3. Delitti di criminalità organizzata (art. 24 ter)

3.1. I reati

La Legge 15 luglio 2009 n. 94, recante "Disposizioni in materia di sicurezza pubblica" ha previsto, tra l'altro, l'inserimento nel D. Lgs. n. 231/01 dell'articolo 24 ter relativo ai "Delitti di Criminalità Organizzata".
Il suddetto articolo ha, pertanto, ampliato la lista dei cd. reati presupposto, aggiungendovi:

- l'art 416 c.p. ("associazione per delinquere");
- l'art. 416 bis c.p. ("associazione di stampo mafiosoanche straniere");
- l'art. 416 ter c.p. ("scambio elettorale politico-mafioso");
- l'art. 630 c.p. ("sequestro di persona a scopo di estorsione");
- l'art. 74 del D.P.R. n. 309/1990 ("associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope");
- l'art. 407 comma 2, lett. a) n. 5 c.p.p. (delitti di 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 oparti di esse, di esplosivi, di armi clandestine nonché di armi comuni da sparo escluse quelle previste dall'art. 2, comma terzo, L. 110/1975).

Con riferimento alle fattispecie di associazioni per delinquere sopra considerate, la sanzione penale è ricollegata al solo fatto della promozione, costituzione, partecipazione ad una associazione criminosa formata da tre o più persone, indipendentemente dall'effettiva commissione (e distinta punizione) dei reati che costituiscono il fine dell'associazione. Ciò significa che la sola cosciente partecipazione ad una associazione criminosa da parte di un esponente o di un dipendente dell'ente potrebbe determinare la responsabilità amministrativa dell'ente stesso qualora detta partecipazione, o il concorso all'associazione, risultasse strumentale al perseguimento anche dell'interesse o del vantaggio dell'ente medesimo. E', inoltre, richiesto che il vincolo associativo si esplichi attraverso un'organizzazione a carattere stabile nel tempo con condivisione di un programma di realizzazione di una serie indeterminata di delitti, non essendo sufficiente l'occasionale accordo per la commissione di uno o più delitti determinati.

3.2. Aree a rischio

Il rischio di verificazione dei suddetti delitti è considerato minimo alla luce delle considerazioni metodologiche della parte generale.
Si ritiene che in relazione alla modestia del rischio rilevato, possa essere individuata quale efficace e sufficiente misura di prevenzione l'osservanza dei principi e delle disposizioni adottate dal Codice Etico, la stretta osservanza delle regole dettate dalla policy aziendale unitamente alla rigorosa applicazione da parte dello MI.ZAR. SRL **del** sistema disciplinare e dei seguenti divieti generali.

3.3. Divieti

Divieti generali
È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall' art. 24 ter del D. Lgs. n. 231/2001;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene non risultino tali integrare di per sé le fattispecie di reato rientranti tra quelle considerate dall' art. 24 ter del D.Lgs. 231/2001, possano considerarsi propedeutiche alla commissione degli stessi.

3.4. Procedure specifiche per aree sensibili

E' fatto espresso obbligo di:

- prevedere, nei rapporti con parti terze, apposita clausola contrattuale che richieda l'impegno al rispetto delle norme di cui al D. Lgs.n. 231/2001 nonché del presente Modello e regoli le conseguenze della loro violazione.

3.5. Presidi adottati

PGM-E PROCEDURA CONTRATTUALE GENERALE
CODICE ETICO

4. Delitti contro l'industria e il commercio (art. 25 bis 1)

4.1. I reati

L'art. 25-bis.1 del D. Lgs. n. 231/2001 disciplina i delitti contro l'industria e il commercio. La L. 21 aprile 2026, n. 75, in vigore dal 29 maggio 2026, ha modificato il catalogo con riferimento ai reati a tutela dei prodotti alimentari e ha abrogato l'art. 516 c.p.

Alla data di aggiornamento, l'art. 25-bis.1 richiama:

- art. 513 c.p. - turbata libertà dell'industria o del commercio;
- art. 515 c.p. - frode nell'esercizio del commercio;
- art. 517 c.p. - vendita di prodotti industriali con segni mendaci;
- art. 517-ter c.p. - fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale;
- art. 517-quater c.p. - contraffazione dei segni di indicazione geografica e di denominazione protetta dei prodotti agroalimentari;
- art. 517-octies, quarto comma, c.p., nelle ipotesi richiamate dall'art. 25-bis.1;
- art. 513-bis c.p. - illecita concorrenza con minaccia o violenza; art. 514 c.p. - frodi contro le industrie nazionali.

Per MI.ZAR. SRL il rischio deve essere valutato in relazione alle concrete attività svolte, alle dichiarazioni commerciali rese ai clienti e, ove applicabile, alla gestione di prodotti, materiali, segni distintivi, certificazioni e informazioni di provenienza.

4.2. Aree a rischio

- Attività di certificazione della Società.

4.3. Divieti

Divieti generali
È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall' art.25 bis 1 del D. Lgs. n. 231/2001;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate dall' art.25 - bis 1 del D. Lgs. n. 231/2001, possano considerarsi propedeutiche alla commissione degli stessi.

Divieti specifici
E' fatto divieto, in particolare, di:

- rivelare a terzi informazioni riguardanti le conoscenze tecniche, tecnologiche e commerciali della società, se non nei casi in cui tale

rivelazione sia richiesta dall'Autorità giudiziaria, da leggi o da altre disposizioni regolamentari o laddove sia espressamente prevista da specifici accordi contrattuali con cui le controparti si siano impegnate a utilizzarle esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenerne la confidenzialità;
- violare le procedure aziendali in vigore (ISO9001);

4.4. Procedure specifiche per aree sensibili

È fatto espresso obbligo di
- accertare la legittima provenienza dei prodotti acquistati/conferiti, con particolare riferimento a quelli che, per la loro qualità o per l'entità del prezzo, inducano a ritenere che siano state violate le norme in materia di proprietà intellettuale, di origine o provenienza;
- prima dell'immissione di prodotti sul mercato, accertare la regolarità e la completezza dell'etichettatura e delle informazioni poste sugli stessi, con particolare attenzione alla presenza delle informazioni relative alla denominazione del prodotto, al nome o marchio e alla sede di produzione o di importazione in base alle disposizioni legislative dedicate attualmente in vigore;
- astenersi dal porre in essere pratiche che turbino l'esercizio di un'industria o di un commercio;
- astenersi dal porre in essere comportamenti atti a perpetrare il delitto di frode nell'esercizio del commercio.
- improntare a onestà, correttezza professionale e trasparenza ogni rapporto e contatto con la clientela;
- nei contratti con i fornitori, prevedere apposite clausole con cui i medesimi si impegnano a garantire che la qualità dei prodotti oggetto del contratto sia conforme a:
    - quanto previsto dalle norme tecniche in vigore presso la società, da ogni disposizione di legge, regolamentare, amministrativa o provvedimento giurisdizionale od amministrativo applicabile o di prevista applicazione nei paesi nei quali il prodotto dovrà essere commercializzato;
    - standard, capitolati, norme, circolari, procedure ed altra simile regolamentazione, di volta in volta comunicata o resa conoscibile al fornitore;
- prevedere, nei rapporti con parti terze, apposita clausola contrattuale che richieda l'impegno al rispetto delle norme di cui al D. Lgs.n. 231/2001 nonché del presente Modello e regoli le conseguenze della loro violazione.

4.5. Presidi adottati

ISO 9001
CODICE ETICO
PGM-E Procedura contrattuale generale

5. Reati societari (art. 25 ter)

5.1. I reati

Le norme penali previste dal Codice Civile - riformate con il D. Lgs. 11 aprile 2002, n. 61, in attuazione della delega espressa dall'art. 11 della Legge 3 ottobre 2001 in tema di disciplina degli illeciti penali e amministrativi riguardanti le società commerciali - hanno trovato accoglimento nell'ambito del D. Lgs. n. 231/2001, attraverso l'introduzione, in quest'ultimo, dell'articolo 25-ter (Reati societari) che ha ulteriormente esteso l'ambito operativo della responsabilità amministrativa da reato dell'Ente.
Per i reati in materia societaria il testo normativo non ha previsto l'applicazione di sanzioni interdittive o accessorie, ma solo di sanzioni pecuniarie, che possono aumentare fino a un terzo qualora a seguito della commissione dei reati l'Ente abbia conseguito un profitto di rilevante entità. In ogni caso, ai sensi di quanto disposto dall'art. 19 del D. Lgs. n. 231/2001, si applicherà sempre la confisca del prezzo o del profitto del reato.
Tutti i reati previsti dalla riforma del Codice Civile sono perseguibili d'ufficio salvo che non sia espressamente previsto che contro di essi si proceda solo a querela di parte e si prescrivono nei tempi e con le modalità ordinarie dei singoli reati in relazione alle pene per essi previste.
È opportuno, infine, ricordare che, per espressa previsione dell'art. 25 ter del D. Lgs. n. 231/2001, si applicano le sanzioni amministrative a carico dell'Ente solo alle precise condizioni che i reati siano commessi nell'interesse dell'Ente stesso e che, quindi, essi siano finalizzati a realizzarne gli scopi - anche illeciti - e siano commessi, salvo specifiche previsioni, da amministratori, direttori generali o liquidatori (soggetti in posizione apicale), ovvero da persone sottoposte alla loro vigilanza (soggetti sottoposti). In altri termini, l'Ente risponde anche quando manchi un vantaggio per esso, ma il reato sia stato commesso nel suo interesse, anche concorrente e non esclusivo.
La "Legge Anticorruzione" (L. n. 190/2012), in vigore dal 28 novembre 2012 ha riscritto la rubrica e il contenuto l'art. 2635 del Codice Civile, definendo così il nuovo reato di "Corruzione tra Privati". Recependo le misure previste dagli articoli 7 e 8 della *Convenzione Penale sulla Corruzione* (firmata dall'Italia il 27 gennaio 1999 e ratificata con Legge n. 110/2012), la nuova norma punisce:

- i soggetti apicali, nonché i soggetti sottoposti al loro controllo e vigilanza che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, causando un danno alla propria società (commi 1 e 2);
- chiunque dà o promette denaro o altre utilità ai soggetti apicali, ai dirigenti, ai sindaci, nonché ai soggetti sottoposti al loro controllo e vigilanza (comma 3).

La legge 190/2012 ha infine introdotto nel comma 1 dell'art. 25 ter del D.Lgs. 231/2001, la lettera s-bis, che estende la responsabilità amministrativa degli Enti alle condotte illecite di cui al terzo comma dell'art. 2635 del Codice Civile

(vale a dire alle condotte dei soggetti corruttori), qualora messe in atto nell'interesse del proprio Ente.
Da ultimo, si segnala che, con la Legge 27 maggio 2015 n. 69 recante 'Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio', pubblicata in Gazzetta Ufficiale il 30 maggio 2015 ed entrata in vigore il 14 giugno 2015, sono state introdotte alcune disposizioni di particolare rilevanza in materia di reati societari.
Ai fini che rilevano in questa sede, giova precisare che detta legge ha operato una significativa modifica degli artt. 2621 - 2622 del Codice Civile, in materia di falso in bilancio, ed introdotto l'art. 2621 bis del Codice Civile.
È stato, inoltre, modificato l'art. 25-ter D. Lgs. 231/01, che ha recepito le modifiche relative, appunto, al cosiddetto falso in bilancio.
Si riporta il testo del comma I dell'art. 25 ter D. Lgs. n. 231/01, come modificato dalla L. 69/2015:
"In relazione ai reati in materia societaria previsti dal codice civile, si applicano all'ente le seguenti sanzioni pecuniarie:
a) per il delitto di false comunicazioni sociali previsto dall'articolo 2621 del codice civile, la sanzione pecuniaria da duecento a quattrocento quote;
a-bis) per il delitto di false comunicazioni sociali previsto dall'articolo 2621-bis del codice civile, la sanzione pecuniaria da cento a duecento quote;
b) per il delitto di false comunicazioni sociali previsto dall'articolo 2622 del codice civile, la sanzione pecuniaria da quattrocento a seicento quote".
Aggiornamenti successivi: il D.Lgs. 15 marzo 2017, n. 38 ha riformato le fattispecie di corruzione tra privati e istigazione alla corruzione tra privati richiamate dall'art. 25-ter. Inoltre, il D.Lgs. 2 marzo 2023, n. 19 ha inserito, alla lettera s-ter dell'art. 25-ter, il delitto di false o omesse dichiarazioni per il rilascio del certificato preliminare previsto dall'art. 54 dello stesso decreto, nell'ambito delle trasformazioni, fusioni e scissioni transfrontaliere.

La presente Parte Speciale deve pertanto essere applicata anche alla predisposizione, verifica e trasmissione della documentazione societaria eventualmente necessaria per operazioni transfrontaliere e al procedimento per il rilascio del certificato preliminare.

5.2. Aree a rischio

- Predisposizione di comunicazioni dirette ai soci ovvero al pubblico in generale riguardo la situazione economica, patrimoniale e finanziaria della Società, anche nel caso in cui si tratti di comunicazioni diverse dalla documentazione contabile periodica (bilancio d'esercizio, bilancio consolidato, relazione trimestrale e semestrale, ecc.).
- Predisposizione e divulgazione verso l'esterno di dati o notizie relativi alla Società.
- Tenuta della contabilità.
- Gestione dei rapporti con l'incaricato del controllo contabile e con la società di revisione, con il collegio sindacale e gli altri organi societari.
- Predisposizione di comunicazioni alle Autorità Pubbliche di Vigilanza e gestione dei rapporti con le stesse (Consob, Borsa Italiana, Isvap,

Autorità per l'energia elettrica e il gas, Autorità Garante della Concorrenza e del Mercato, Autorità per le garanzie nelle telecomunicazioni, ecc.).
- Attività relative alle riunioni assembleari.
- Operazioni societarie che possano incidere sull'integrità del capitale sociale.
- Compimento di operazioni di significativo rilievo concluse sia con soggetti terzi che con parti correlate (fusioni, scissioni ecc.).
- Attività commerciali che prevedono la vendita di beni o servizi a società.
- Stipula e gestione di accordi di partnership con altre società.
- Attività dell'ufficio acquisti.
- Gestione di eventuali trasformazioni, fusioni e scissioni transfrontaliere, inclusa la predisposizione dei dati e dei documenti per il rilascio del certificato preliminare.

5.3. Divieti

Divieti generali

È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall' art.25 ter del D.Lgs. 231/2001;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate dall'art. 25 ter del D. Lgs. n. 231/2001, possano considerarsi propedeutiche alla commissione degli stessi.

Divieti specifici

E' fatto divieto, in particolare, di:

- predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria dell'Ente;
- non attenersi ai principi e alle prescrizioni contenute nelle istruzioni per la redazione dei bilanci, della relazione semestrale e trimestrale, nelle procedure amministrativo-contabili, nel piano dei conti di Contabilità Generale;
- presentare i dati e le informazioni utilizzati in modo tale da fornire una rappresentazione non corretta e veritiera sulla situazione patrimoniale, economica e finanziaria dell'Ente e sull'evoluzione delle relative attività, nonché sugli strumenti finanziari dell'Ente e relativi diritti;
- tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o della società di revisione o dei soci;

- porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità di Vigilanza tutte le comunicazioni, periodiche e non, previste dalla legge e dalla ulteriore normativa di settore; nonché la trasmissione dei dati e documenti previsti dalle norme in vigore e/o specificamente richiesti dalle predette Autorità;
- esporre nelle comunicazioni alle Autorità di Vigilanza e nella documentazione trasmessa alle stesse, fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della Società;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità pubbliche di Vigilanza, anche in sede di ispezione (espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti);
- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;
- effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
- procedere in ogni modo a formazione o aumenti fittizi del capitale sociale;
- ripartire i beni sociali tra i soci - in fase di liquidazione - prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli;
- effettuare elargizioni in denaro o accordare vantaggi di qualsiasi natura ad amministratori, direttori generali, dirigenti, sindaci, liquidatori di altre società;
- offrire denaro o altre utilità ai vertici aziendali, ai dirigenti, ai sindaci, ai liquidatori o ai dipendenti di altre società;
- effettuare pagamenti in contanti o in natura;
- affidare ad un soggetto aziendale la gestione in completa autonomia dei rapporti con società terze;
- formare o utilizzare documenti falsi, alterare documenti veri, rendere dichiarazioni false o omettere informazioni rilevanti al fine di ottenere il rilascio del certificato preliminare previsto per operazioni societarie transfrontaliere.

5.4. Procedure specifiche per aree sensibili

È fatto espresso obbligo di:

- conoscere e rispettare i principi di Corporate Governance approvati dagli Organi Sociali dello MI.ZAR. SRL che rispecchiano le normative applicabili;
- conoscere e rispettare il sistema di controllo interno, e quindi le procedure aziendali, la documentazione e le disposizioni inerenti la struttura

gerarchico-funzionale aziendale ed organizzativa dello MI.ZAR. SRL ed il sistema di controllo di gestione;

- conoscere e rispettare le norme interne inerenti il sistema amministrativo, contabile, finanziario, di reporting;
- conoscere e rispettare le norme interne inerenti l'uso e il funzionamento del sistema informativo dello MI.ZAR. SRL;
- tenere un comportamento corretto, trasparente e collaborativo, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci ed al pubblico in generale una informazione veritiera appropriata sulla situazione economica, patrimoniale e finanziaria dello MI.ZAR. SRL;
- assicurare il regolare funzionamento dello MI.ZAR. SRL e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione della Società stessa;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità e dell'effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in generale;
- effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate;
- astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee a provocare una sensibile distorsione dei risultati economici/patrimoniali e finanziari conseguiti dallo MI.ZAR. SRL;
- assicurare, nel compimento di operazioni di significativo rilievo concluse sia con soggetti terzi che con parti correlate, la trasparenza ed il rispetto dei criteri di correttezza sostanziale e procedurale nonché i termini e le modalità di approvazione previsti dalla normativa interna;
- osservare rigorosamente tutte le leggi e regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con società terze;
- gestire qualsiasi rapporto con società terze in conformità a criteri di massima correttezza e trasparenza;
- gestire in modo unitario i rapporti con società terze, individuando il responsabile per ogni operazione o pluralità di operazioni (in caso di particolare ripetitività delle stesse) svolte nelle aree di attività a rischio;
- definire per iscritto gli accordi di associazione con i Partner, evidenziando tutte le condizioni dell'accordo stesso, con particolare riguardo alle condizioni economiche concordate.
- redigere per iscritto gli incarichi conferiti ai Collaboratori esterni, a qualunque titolo questi siano fatti, con l'indicazione del compenso pattuito;
- garantire che tutte le transazioni economiche a favore di società terze siano documentate e verificabili, tramite adeguati supporti informativi.
- in caso di operazioni societarie transfrontaliere, sottoporre la documentazione destinata al notaio, al Registro delle imprese o ad altre

autorità a verifica preventiva di completezza, veridicità e coerenza, assicurando la tracciabilità delle approvazioni.

5.5. Presidi adottati

PGM-G PAGAMENTI
PGM-F ACQUISTO DI BENI E SERVIZI
CODICE ETICO

6. Reati in materia di sicurezza e salute sul lavoro (art. 25 septies)

6.1. I reati

La Legge 3 agosto 2007, n. 123, ha introdotto l'art. 25 septies del D. Lgs. n. 231/2001, articolo in seguito sostituito dall'art. 300 del D. Lgs. 9 aprile 2008 n. 81, che prevede l'applicazione di sanzioni pecuniarie ed interdittive agli Enti i cui esponenti commettano i reati di cui agli artt. **589 (omicidio colposo)** e **590 terzo comma (lesioni personali colpose gravi o gravissime) del codice penale, in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.**

Le fattispecie delittuose inserite all'art. 25 septies riguardano unicamente le ipotesi in cui l'evento sia stato determinato non già da colpa di tipo generico (e dunque per imperizia, imprudenza o negligenza) bensì da "colpa specifica" che richiede che l'evento si verifichi a causa dell'inosservanza delle norme per la prevenzione degli infortuni sul lavoro.

Perché si venga a configurare la responsabilità amministrativa dello MI.ZAR. SRL ai sensi del D. Lgs. n.231/2001, l'art. 5 del Decreto medesimo esige però che i reati siano stati commessi nel suo interesse o a suo vantaggio (ad esempio in termini di risparmi di costi per la salute e sicurezza sul lavoro).

6.2. Aree a rischio

In relazione ai reati di cui agli artt. 589 e 590 del Codice Penale, le aree ritenute più a rischio, ai fini del presente Modello, risultano essere quelle aree aziendali di attività dove possono concretamente svilupparsi i fattori di rischio generali, validi per tutti i dipendenti, apprendisti, terzi e visitatori.

Sono considerate maggiormente a rischio le seguenti aree:

- Valutazione dei rischi e predisposizione di procedure di sicurezza.
- Formazione ed informazione del personale.
- Gestione delle emergenze.
- Manutenzione delle attrezzature antincendio.
- Formazione del personale sulla Sicurezza.
- Manutenzione attrezzature.

6.3. Divieti

Divieti generali

È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall'art. 25 septies del D.Lgs. n. 231/2001;
- porre in essere, collaborare o creare i presupposti per la realizzazione di comportamenti che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato e di illecito amministrativo rientranti tra quelle considerate nel presente Modello.

Divieti specifici
E' fatto divieto, in particolare, di:

- aggirare le limitazioni di sicurezza imposte nell'utilizzo degli strumenti di lavoro e quelle descritte nell'opportuna segnaletica interna ed esterna apposta nei luoghi di lavoro;
- tacere eventuali non conformità, rischi non valutati o comportamenti scorretti;
- sottrarsi alle visite mediche periodiche, mentire sul proprio stato di salute e di idoneità al lavoro assegnato;
- sottrarsi alla formazione promossa dall'azienda per la sicurezza e la salute sui luoghi di lavoro ovvero all'assunzione dei compiti specifici assegnati in conformità alla normativa in materia;
- mettere in atto qualsivoglia forma di attività che abbia come scopo la attenuazione o la violazione delle regole e delle procedure previste per assicurare, mantenere e controllare la salute e la sicurezza dei lavoratori dello MI.ZAR. SRL e di tutti i soggetti che si trovano sui luoghi di lavoro della stessa.

6.4. Procedure specifiche per aree sensibili

È previsto l'espresso obbligo, a carico degli Esponenti Aziendali in via diretta e, tramite apposite clausole contrattuali, a carico dei collaboratori esterni e Partner, di:

- mantenere aggiornato il Documento di valutazione dei rischi e di seguirne le indicazioni per la mitigazione dei rischi;
- verificare l'adempimento delle misure indicate nel Documento di valutazione dei rischi e la loro efficacia;
- verificare periodicamente lo stato di conformità aziendale a leggi e regolamenti applicabili;
- verificare la corretta manutenzione programmata delle macchine/attrezzature;
- verificare il mantenimento in efficienza delle attrezzature antincendio;
- verificare l'avvenuta informazione, formazione ed addestramento dei lavoratori.

È previsto l'espresso obbligo a carico del personale aziendale coinvolto nel processo di gestione delle risorse umane di:

- verificare che il personale, prima di essere destinato alla mansione, sia stato adeguatamente formato;
- verificare che il personale neoassunto, all'atto dell'assunzione, venga informato e formato sui rischi di sicurezza nei luoghi di lavoro;
- verificare che il personale addetto alle squadre di emergenza sia adeguatamente formato secondo le scadenze previste;
- verificare che tutto il personale aziendale partecipi alle prove di emergenza secondo le scadenze previste;
- verificare che il piano di formazione per la sicurezza predisposto dal RSPP e approvato dalla Direzione sia attuato.

È previsto l'espresso obbligo per tutto il personale aziendale

- di conoscere e rispettare per le parti di proprio interesse, oltre alle regole definite nel Modello e nei suoi protocolli, i principi contenuti nei

seguenti documenti: Codice Etico, Documento di valutazione dei rischi, procedure, istruzioni o disposizioni aziendali poste in essere dal datore di lavoro e dal Servizio di Prevenzione e Protezione in materia di sicurezza e igiene sul lavoro, compresa la documentazione in materia di appalti.

È previsto, inoltre, l'espresso obbligo di:

- dotare i responsabili del SPP di poteri di spesa adeguati e, oltre questi, del potere di impulso nei confronti del datore di lavoro;
- prevedere, nei rapporti con parti terze, apposita clausola contrattuale che richieda l'impegno al rispetto delle norme di cui al D. Lgs.n. 231/2001 nonché del presente Modello e regoli le conseguenze della loro violazione.

6.5. Presidi adottati

PROTOCOLLI SICUREZZA
CODICE ETICO
Certificazione ISO45001

7. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita ed autoriciclaggio (art. 25 octies)

7.1. I reati

L'articolo 25 octies è stato introdotto nel corpus del D. Lgs. n. 231 del 2001, dal D. Lgs. n. 231/2007 (di seguito "Decreto Antiriciclaggio").
I reati di riciclaggio contemplati dall'articolo in commento (di seguito "reati di riciclaggio") sono: Ricettazione (art. 648 Codice Penale); Riciclaggio (art. 648 bis Codice Penale); Impiego di denaro, beni o utilità di provenienza illecita (art.648 ter Codice Penale); Autoriciclaggio (art. 648 ter. 1 codice penale).
La normativa italiana in tema di prevenzione dei reati di riciclaggio prevede norme tese ad ostacolare le pratiche di riciclaggio, vietando tra l'altro l'effettuazione di operazioni di trasferimento di importi rilevanti con strumenti anonimi ed assicurando la ricostruzione delle operazioni attraverso l'identificazione della clientela e la registrazione dei dati in appositi archivi.
Nello specifico, il corpo normativo in materia di riciclaggio è costituito anzitutto dal Decreto Antiriciclaggio che ha in parte abrogato e sostituito la Legge del 5 luglio 1991 n. 197.
Il Decreto Antiriciclaggio, come modificato dalla Legge n. 208 del 28.12.2015 prevede i seguenti strumenti di contrasto al fenomeno del riciclaggio di proventi illeciti:

1. la previsione di un divieto di trasferimento di denaro contante o di libretti di deposito bancari o postali al portatore o di titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) in Euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi quando il valore dell'operazione è pari o superiori a euro 3.000,00. Il trasferimento può, tuttavia, essere eseguito per il tramite di banche, istituti di moneta elettronica e Poste Italiane S.p.A.;
2. l'obbligo di adeguata verifica della clientela da parte di alcuni soggetti destinatari del Decreto Antiriciclaggio (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) in relazione ai rapporti e alle operazioni inerenti allo svolgimento dell'attività istituzionale o professionale degli stessi;
3. l'obbligo da parte di alcuni soggetti (elencati agli artt. 11, 12, 13 e 14 del Decreto Antiriciclaggio) di conservare, nei limiti previsti dall'art. 36 del Decreto Antiriciclaggio, i documenti o le copie degli stessi e registrare le informazioni che hanno acquisito per assolvere gli obblighi di adeguata verifica della clientela affinché possano essere utilizzati per qualsiasi indagine su eventuali operazioni di riciclaggio o di finanziamento del terrorismo o per corrispondenti analisi effettuate dall'UIF o da qualsiasi altra autorità competente;
4. l'obbligo di segnalazione da parte di alcuni soggetti (elencati agli artt. 10, comma 2, 11, 12, 13 e 14 del Decreto Antiriciclaggio) all'UIF, di tutte quelle operazioni, poste in essere dalla clientela, ritenute "sospette" o quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo.

I soggetti sottoposti agli obblighi di cui ai n. 2., 3., 4., sono:

1) gli intermediari finanziari e gli altri soggetti esercenti attività finanziaria. Tra tali soggetti figurano, ad esempio:

• banche;
• poste italiane;
• società di intermediazione mobiliare (SIM);
• società di gestione del risparmio (SGR);
• società di investimento a capitale variabile (SICAV).
2) I professionisti, tra i quali si indicano:
• i soggetti iscritti nell'albo dei ragionieri e periti commerciali;
• i notai e gli avvocati quando, in nome e per conto dei loro clienti, compiono qualsiasi operazione di natura finanziaria o immobiliare e quando assistono i loro clienti in determinate operazioni.
3) I revisori contabili.
4) Altri soggetti, intesi quali operatori che svolgono alcune attività il cui esercizio resta subordinato al possesso delle licenze, autorizzazioni, iscrizioni in albi o registri, ovvero alla preventiva dichiarazione di inizio di attività richieste dalle norme. Tra le attività si indicano:
• recupero di crediti per conto terzi;
• trasporto di denaro contante;
• gestione di case da gioco;
• offerta, attraverso internet, di giochi, scommesse o concorsi pronostici con vincite in denaro.
Da ultimo, si segnala che la Legge n. 186 del 15 dicembre 2014 (Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonche' per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio) ha introdotto nell'ordinamento giuridico italiano il delitto di autoriciclaggio (art. 648 ter.1). Trattasi di una rilevantissima innovazione, destinata ad incidere sullo stesso catalogo dei reati disciplinato dal D. Lgs. n. 231/01, il cui articolo 25 octies è stato, infatti, modificato.
Il D.Lgs. 8 novembre 2021, n. 195 ha inoltre modificato le fattispecie codicistiche di ricettazione, riciclaggio, impiego e autoriciclaggio, ampliandone in più punti il perimetro. I controlli previsti dalla presente Parte Speciale devono quindi essere applicati con riferimento alla provenienza illecita dei beni o delle utilità secondo la disciplina penale pro tempore vigente.

7.2. Aree a rischio

- Rapporti con fornitori e partner;
- Rapporti con soggetti terzi relativi a:
  - Contratti di acquisto e/o di vendita con controparti
  - Transazioni finanziarie con controparti
  - Investimenti con controparti
  - Sponsorizzazioni
- Acquisto di beni e servizi;
- Pagamenti ed incassi;
- Gestione fatturazione;
- Marketing e commerciale;
- Processo di erogazione del credito;

7.3. Divieti

Divieti generali
E' fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere condotte tali da integrare le fattispecie di reato previste dall'art. 25 octies del Decreto;
- porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- porre in essere o agevolare operazioni o attività che non siano rispettose delle norme del Codice Etico;
- intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o, comunque, operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
- utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- porre in essere attività che siano in contrasto con le procedure e i principi di controllo in esse previste ai fini della prevenzione dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

7.4. Procedure specifiche per aree sensibili

Nell'espletamento di tutte le operazioni attinenti alla gestione, oltre alle regole di cui al presente Modello, gli Esponenti aziendali, sono tenuti in generale a conoscere e rispettare tutte le regole ed i principi contenuti nei seguenti documenti:
- Codice Etico;
- Procedura ISO9001 per la gestione degli acquisti, vendite, delle forniture, dei contratti e di qualsivoglia operazione o transazione con terzi.
Ai Consulenti, Partner e Fornitori e parti terze deve essere resa nota l'adozione del Modello e del Codice etico da parte dell'Ente.
I Destinatari sono in particolare tenuti a provvedere - prima di compiere un'operazione ritenuta sospetta a trasmettere la segnalazione all'OdV per ricevere indicazioni in merito.
Al fine di prevenire l'attuazione dei comportamenti vietati, gli Esponenti Aziendali, in via diretta, e i Consulenti e i Partner, tramite apposite clausole contrattuali, in relazione al tipo di rapporto in essere con la Società, dovranno:

- verificare l'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari;
- verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- effettuare controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni infragruppo. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte

nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;

- effettuare controlli formali e sostanziali dei flussi finanziari aziendali in entrata; tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, paesi a rischio terrorismo ecc.), degli Istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie;
- determinare dei criteri di selezione, stipulazione ed esecuzione di accordi/joint-venture con altre imprese per la realizzazione di investimenti;
- adottare adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio;
- mantenere evidenza, in apposite registrazioni su archivi informatici, delle transazioni effettuate su conti correnti aperti presso stati in cui permangono regole di trasparenza meno restrittive per importi superiori, complessivamente, a euro 3.000,00;
- effettuare controlli specifici sui soggetti che gestiscono le operazioni di finanziamento.

7.5. Presidi adottati

PGM-F ACQUISTO BENI E SERVIZI
PGM–G PAGAMENTI
CODICE ETICO

8. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (art. 25-octies.1)

8.1. I reati

Il D.Lgs. 8 novembre 2021, n. 184 ha introdotto l'art. 25-octies.1 del D. Lgs. n. 231/2001 in materia di strumenti di pagamento diversi dai contanti. Il D.L. 10 agosto 2023, n. 105, convertito con modificazioni dalla L. 9 ottobre 2023, n. 137, ha successivamente aggiunto il delitto di trasferimento fraudolento di valori e ha modificato la rubrica dell'articolo.

Le fattispecie espressamente richiamate comprendono:

- indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (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 (art. 640-ter c.p.) nelle ipotesi concernenti trasferimenti di denaro, valore monetario o valuta virtuale;
- altri delitti contro la fede pubblica, contro il patrimonio o che comunque offendono il patrimonio, quando hanno ad oggetto strumenti di pagamento diversi dai contanti, nei casi previsti dal comma 2 dell'art. 25-octies.1;
- trasferimento fraudolento di valori (art. 512-bis c.p.), compresa la fittizia attribuzione a terzi della titolarità o disponibilità di denaro, beni, utilità, imprese, quote, azioni o cariche sociali nelle ipotesi previste dalla norma.

8.2. Aree a rischio

- Rapporti con fornitori e partner;
- Rapporti con soggetti terzi relativi a:
  - Contratti di acquisto e/o di vendita con controparti
  - Transazioni finanziarie con controparti
  - Investimenti con controparti
  - Sponsorizzazioni
- Acquisto di beni e servizi;
- Pagamenti ed incassi;
- Gestione fatturazione;
- Marketing e commerciale;
- Processo di erogazione del credito;
- Gestione di carte aziendali, credenziali bancarie, home banking, dispositivi di autenticazione e altri strumenti di pagamento.
- Modifica di IBAN o coordinate di pagamento di clienti, fornitori, collaboratori e altri beneficiari.
- Operazioni che comportino intestazioni, attribuzioni o trasferimenti di beni, quote o disponibilità a soggetti diversi dagli effettivi titolari o beneficiari.

8.3. Divieti

Divieti generali
È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere condotte tali da integrare le fattispecie di reato previste dall'art. 25 octies-1 del Decreto;
- porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra delineate, possa in astratto diventarlo;
- porre in essere o agevolare operazioni o attività che non siano rispettose delle norme del Codice Etico;
- intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o, comunque, operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
- utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
- porre in essere attività che siano in contrasto con le procedure e i principi di controllo in esse previste ai fini della prevenzione dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

8.4. Procedure specifiche per aree sensibili

Nell'espletamento di tutte le operazioni attinenti alla gestione, oltre alle regole di cui al presente Modello, gli Esponenti aziendali, sono tenuti in generale a conoscere e rispettare tutte le regole ed i principi contenuti nei seguenti documenti:
- Codice Etico;
- Procedura ISO9001 per la gestione degli acquisti, vendite, delle forniture, dei contratti e di qualsivoglia operazione o transazione con terzi.
Ai Consulenti, Partner e Fornitori e parti terze deve essere resa nota l'adozione del Modello e del Codice etico da parte dell'Ente.
I Destinatari sono in particolare tenuti a provvedere - prima di compiere un'operazione ritenuta sospetta a trasmettere la segnalazione all'OdV per ricevere indicazioni in merito.
Al fine di prevenire l'attuazione dei comportamenti vietati, gli Esponenti Aziendali, in via diretta, e i Consulenti e i Partner, tramite apposite clausole contrattuali, in relazione al tipo di rapporto in essere con la Società, dovranno:

- verificare l'attendibilità commerciale e professionale dei fornitori e partner commerciali/finanziari;
- verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- effettuare controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi e ai pagamenti/operazioni infragruppo. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte

nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie;
- effettuare controlli formali e sostanziali dei flussi finanziari aziendali in entrata; tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, paesi a rischio terrorismo ecc.), degli Istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie;
- determinare dei criteri di selezione, stipulazione ed esecuzione di accordi/joint-venture con altre imprese per la realizzazione di investimenti;
- adottare adeguati programmi di formazione del personale ritenuto esposto al rischio di riciclaggio;
- mantenere evidenza, in apposite registrazioni su archivi informatici, delle transazioni effettuate su conti correnti aperti presso stati in cui permangono regole di trasparenza meno restrittive per importi superiori, complessivamente, a euro 3.000,00;
- effettuare controlli specifici sui soggetti che gestiscono le operazioni di finanziamento.
- prevedere verifica indipendente delle richieste di variazione di IBAN o coordinate di pagamento, utilizzando canali di contatto già noti e diversi dal messaggio che richiede la modifica;
- assicurare, ove compatibile con le dimensioni aziendali, separazione tra predisposizione e autorizzazione dei pagamenti e tracciabilità delle operazioni;
- vietare l'utilizzo di intestazioni fittizie o di interposizioni finalizzate a occultare il titolare effettivo, eludere misure di prevenzione patrimoniali, documentazione antimafia o agevolare altri reati.

8.5. Presidi adottati

PGM-F ACQUISTO BENI E SERVIZI
PGM–G PAGAMENTI
CODICE ETICO

9. Delitti in materia di violazione del diritto d'autore (art. 25 novies)

9.1. I reati

Il 31 luglio 2009 è stata pubblicata sulla Gazzetta Ufficiale n. 176 la legge n. 94/09 del 23 luglio 2009 il cui art. 15, comma 7 introduce definitivamente nel D. Lgs. n. 231/2001 il nuovo articolo 25 novies "Delitti in materia di violazione del diritto d'autore".
Tale articolo contempla alcuni reati previsti dalla Legge sul diritto d'autore quali, ad esempio, l'importazione, la distribuzione, la vendita o la detenzione a scopo

commerciale o imprenditoriale di programmi contenuti in supporti non contrassegnati dalla SIAE; la riproduzione o il reimpiego del contenuto di banche dati; l'abusiva duplicazione, la riproduzione, la trasmissione o la diffusione in pubblico, di opere dell'ingegno destinate al circuito televisivo o cinematografico; l'immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa.
Le sanzioni applicabili alla Società nell'ipotesi di commissione dei delitti in materia di violazione del diritto d'autore sono di natura pecuniaria (fino a 500 quote) e di natura interdittiva (quali l'interdizione dall'esercizio dell'attività o la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, per una durata non superiore ad un anno).
La disciplina del diritto d'autore è stata oggetto di ulteriori interventi, tra cui il D.L. 16 settembre 2024, n. 131, convertito dalla L. 14 novembre 2024, n. 166, con modifiche agli artt. 171-bis e 171-ter della L. n. 633/1941. I Destinatari devono pertanto fare riferimento alla disciplina sul diritto d'autore e sul contrassegno applicabile pro tempore.

9.2. Aree a rischio

- Si considerano a rischio tutte le aree di attività dell'Ente in cui lo svolgimento delle funzioni potrebbe determinare, anche potenzialmente, la violazione del diritto d'autore di un altro soggetto, legalmente tutelato. In particolare, possiamo individuare un maggior rischio in quelle aree che utilizzano sistemi informatici i quali, generalmente, sono protetti da un copyright.
- Tutte le attività aziendali svolte dai Destinatari del Modello tramite l'utilizzo dei sistemi informatici aziendali, del servizio di posta elettronica e dell'accesso ad Internet.
- Utilizzo di software e banche dati.

9.3. Divieti

Divieti specifici
È fatto divieto, in particolare, di:

- connettere ai sistemi informatici dello MI.ZAR. SRL personal computer, periferiche e altre apparecchiature o installare software, senza preventiva autorizzazione del soggetto aziendale responsabile individuato;
- procedere ad installazioni di prodotti software in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano il diritto d'autore;
- modificare la configurazione software e/o hardware di postazioni di lavoro fisse o mobili se non previsto da una regola aziendale ovvero, in diversa ipotesi, se non previa espressa autorizzazione;
- divulgare, cedere o condividere con personale interno o esterno allo MI.ZAR. SRL le proprie credenziali d'accesso ai sistemi e alla rete aziendale, di clienti o terze parti;
- accedere abusivamente ad un sistema informatico altrui - ovvero nella disponibilità di altri dipendenti o terzi - nonché accedervi al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto;

- acquisire e/o utilizzare prodotti tutelati dal diritto d'autore in violazione delle tutele contrattuali previste per i diritti di proprietà intellettuale altrui;
- accedere abusivamente al sito Internet dell'Ente al fine di manomettere o alterare abusivamente qualsiasi dato ivi contenuto ovvero allo scopo di immettervi dati o contenuti multimediali (immagini, video, ecc.) in violazione della normativa sul diritto d'autore e delle procedure aziendali applicabili;
- comunicare a persone non autorizzate, interne o esterne allo MI.ZAR. SRL, i controlli sui sistemi informatici e le modalità con cui sono utilizzati;
- inviare attraverso un sistema informatico aziendale qualsiasi informazione o dato, previa alterazione o falsificazione dei medesimi.

9.4. Procedure specifiche per aree sensibili

È fatto espresso obbligo di:

- informare gli utilizzatori dei sistemi informatici che il software loro assegnato è protetto dalle leggi sul diritto d'autore e che, pertanto, ne è vietata la duplicazione, la distribuzione, la vendita o la detenzione a scopo commerciale/imprenditoriale;
- fornire ai destinatari un'adeguata informazione relativamente alle opere protette dal diritto d'autore e al rischio della commissione di tale reato;
- tutelare il copyright su dati, immagini e/o software sviluppati dall'azienda e di valore strategico per la stessa attraverso segreto industriale, qualora legalmente possibile e/o registrazioni SIAE (per l'Italia);
- vietare l'impiego/l'uso/l'installazione sugli strumenti informatici concessi in dotazione dall'Ente di materiale copiato/non contrassegnato/non autorizzato;
- vietare il download di software coperti da copyright;
- nell'ambito delle attività di promozione/pubblicizzazione di marchi/prodotti ed in particolare, nella gestione degli eventi, l'utilizzo, la messa a disposizione del pubblico anche attraverso un sistema di reti telematiche, di opere dell'ingegno protette, deve avvenire nel rispetto della normativa in materia di diritto d'autore;
- prevedere, nei rapporti contrattuali con partner/terzi, clausole di manleva volte a tenere indenne l'Ente da eventuali responsabilità in caso di condotte, poste in essere dagli stessi, che possano determinare violazione di qualsiasi diritto di proprietà intellettuale.

Al fine di prevenire l'attuazione dei comportamenti vietati, lo MI.ZAR. SRL si impegna a porre in essere i seguenti adempimenti:

- far sottoscrivere ai dipendenti, nonché agli stagisti e agli altri soggetti eventualmente autorizzati all'utilizzo dei sistemi informatici, uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo e tutela delle risorse informatiche aziendali;
- dotare i sistemi informatici di adeguato software firewall e antivirus e far sì che, ove possibile, questi non possano venir disattivati;
- impedire l'installazione e l'utilizzo di software non approvati da MI.ZAR. SRL e non correlati con l'attività professionale dalla stessa esercitata.

9.5. Presidi adottati

CODICE ETICO
PRIVACY

10. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies)

10.1. I reati

La Legge 3 agosto 2009, n. 116 ha introdotto il delitto di "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" all'art. 25 decies del D.Lgs. 231/2001.
Tale ipotesi delittuosa - già contemplata dal D.Lgs. n. 231/2001 fra i reati transazionali (art.10, comma 9, L. 146/2006) - assume ora rilevanza anche in ambito nazionale.
L'art. 377 bis del Codice Penale intende sanzionare ogni comportamento diretto ad influenzare la persona chiamata dinanzi all'Autorità Giudiziaria a rendere dichiarazioni utilizzabili in un procedimento penale o in altri procedimenti connessi. Tale influenza può avere ad oggetto l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci, al fine di celare elementi "compromettenti" a carico di un determinato Ente, con evidente interesse del medesimo.
La norma mira a tutelare il corretto svolgimento dell'attività processuale contro ogni forma di indebita interferenza.
Per quanto riguarda invece le sanzioni applicabili all'Ente nell'ipotesi di commissione del reato in parola, esse possono consistere in sanzioni di natura pecuniaria, fino a 500 quote (e dunque fino ad un massimo di circa Euro 780.000).

10.2. Aree a rischio

- In relazione al delitto di cui sopra, si considerano "aree a rischio" tutte le aree aziendali le quali potrebbero essere chiamate a rendere dichiarazioni all'Autorità Giudiziaria.

10.3. Divieti

Divieti generali
È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall' art.25 terdecies del D. Lgs. n. 231/2001;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate dall' art. 25 decies del D. Lgs. n. 231/2001, possano potenzialmente diventarlo.

10.4. Procedure specifiche per aree sensibili

- La fattispecie criminosa è ipotizzabile nel caso di pressioni o induzioni poste in essere da un dipendente/consulente della Società nei confronti del soggetto indagato o imputato.

Il rischio di verificazione del reato (delitto) è considerato minimo alla luce delle considerazioni metodologiche della parte generale.
Si ritiene che in relazione alla modestia del rischio rilevato, possa essere individuata quale efficace e sufficiente misura di prevenzione l'osservanza dei principi e delle disposizioni adottate dal Codice Etico, unitamente alla rigorosa applicazione da parte dello MI.ZAR. SRL del sistema disciplinare.

10.5. Presidi adottati

CODICE ETICO

11. REATI AMBIENTALI (art. 25 undecies)

11.1. I reati

L'art. 25-undecies del D. Lgs. n. 231/2001 disciplina i reati ambientali. Il catalogo, introdotto nel 2011 e ampliato dalla L. 22 maggio 2015, n. 68, è stato ulteriormente modificato dalla normativa più recente in materia di rifiuti e, da ultimo, dal D.Lgs. 21 aprile 2026, n. 81, in vigore dal 2 giugno 2026, di attuazione della direttiva (UE) 2024/1203 sulla tutela penale dell'ambiente.

Alla data di aggiornamento, l'art. 25-undecies comprende, tra l'altro:

- i delitti ambientali del codice penale richiamati dall'art. 25-undecies, tra cui gli artt. 452-bis, 452-bis.1, 452-quater, 452-quinquies, 452-octies, 452-sexies, 452-septies, 452-terdecies e 452-quaterdecies, nonché gli artt. 727-bis e 733-bis c.p.;
- i reati in materia di scarichi idrici di cui all'art. 137 del D.Lgs. n. 152/2006 nelle ipotesi richiamate;
- i reati in materia di abbandono, gestione non autorizzata, combustione, traffico e altre condotte illecite relative ai rifiuti, comprese le fattispecie degli artt. 255-bis, 255-ter, 256, 256-bis, 257, 258, 259, 260 e 260-bis del D.Lgs. n. 152/2006 nelle ipotesi previste dall'art. 25-undecies;
- le violazioni relative alle emissioni in atmosfera di cui all'art. 279, comma 5, del D.Lgs. n. 152/2006;
- le fattispecie relative alle specie protette di cui alla L. n. 150/1992, le violazioni in materia di sostanze lesive dell'ozono e i reati di inquinamento provocato da navi di cui al D.Lgs. n. 202/2007;

i reati previsti dal decreto legislativo attuativo dell'art. 9 della L. 13 giugno 2025, n. 91, per le violazioni degli artt. 4 e 5, nei termini richiamati dal comma 1-ter dell'art. 25-undecies.

La valutazione del rischio ambientale di MI.ZAR. SRL deve essere mantenuta coerente con la natura di società di servizi, ma non può essere esclusa in via assoluta, in particolare per la gestione dei rifiuti prodotti dalle attività d'ufficio e dalle apparecchiature.

11.2. Aree a rischio

Nello svolgimento delle attività di mappatura del rischio propedeutica alla costruzione del Modello sono state individuate nell'ambito della struttura organizzativa di MI.ZAR. SRL le seguenti Attività sensibili che possono astrattamente comportare il rischio di commissione da parte dell'Ente dei reati ambientali.

a. Gestione dei rifiuti

I rifiuti prodotti dalla MIZAR e che possono rappresentare una qualche criticità sono rappresentati da quelli relativi alle attrezzature utilizzate: computer e loro accessori, stampanti, cartucce per stampanti, cellulari, pile non ricaricabili, prodotti scaduti presenti nella cassetta di pronto soccorso.

- Gestione del deposito temporaneo, classificazione e conferimento dei rifiuti prodotti, con particolare attenzione a RAEE, apparecchiature informatiche, telefoni, pile/batterie, cartucce/toner e prodotti scaduti presenti nelle dotazioni di primo soccorso, ove qualificabili come rifiuti.
- Selezione e controllo di trasportatori, intermediari e impianti di destinazione dei rifiuti, ove utilizzati.
- Gestione della documentazione ambientale e delle registrazioni previste dalla normativa, compresi gli adempimenti RENTRI, registri, formulari e MUD ove applicabili alla concreta posizione di MI.ZAR. SRL.

11.3. Divieti

Divieti generali

È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall' art.25 undecies del D. Lgs. n. 231/2001;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate dall' art. 25 undecies del D. Lgs. n. 231/2001, possano potenzialmente diventarlo.

11.4. Procedure specifiche per aree sensibili

MI.ZAR. SRL deve verificare periodicamente gli obblighi ambientali effettivamente applicabili in funzione della tipologia e quantità dei rifiuti prodotti, delle modalità di deposito e conferimento e delle eventuali modifiche normative. Non devono pertanto essere assunte in modo permanente esenzioni da registri, formulari, RENTRI o MUD senza preventiva verifica della normativa pro tempore vigente.

Al fine di prevenire i reati ambientali è fatto obbligo di:

- classificare correttamente i rifiuti e mantenerli separati secondo le relative caratteristiche, evitando abbandono, miscelazione o combustione illecita;
- conferire i rifiuti esclusivamente a soggetti autorizzati, verificando, ove necessario, validità e coerenza delle autorizzazioni del trasportatore e dell'impianto di destinazione;
- conservare le evidenze dei conferimenti e della corretta gestione dei rifiuti e adempiere agli obblighi documentali e di tracciabilità applicabili;
- gestire RAEE, pile/batterie, toner/cartucce e altri rifiuti particolari attraverso canali conformi alla normativa applicabile;
- segnalare all'OdV anomalie, contestazioni, ispezioni, sanzioni, abbandoni, smarrimenti di documentazione o altri eventi che possano assumere rilievo ai fini del D. Lgs. n. 231/2001.

11.5. Presidi adottati

CODICE ETICO

SISTEMA DI GESTIONE AMBIENTALE / PROCEDURE AMBIENTALI, ove adottate

ISTRUZIONI PER LA GESTIONE DEI RIFIUTI E VERIFICA PERIODICA DEGLI ADEMPIMENTI APPLICABILI

12. Reato di impiego di lavoratori irregolari (art. 25-duodecies)

12.1. I reati

La presente Parte Speciale si riferisce al reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare richiamato dalla disposizione di cui all'art. 25-duodecies del D. Lgs. 231/2001.
Per effetto dell'entrata in vigore del D.Lgs. n. 109/2012, avvenuto il 9 Agosto 2012, il novero dei reati che possono generare una responsabilità amministrativa degli enti si è arricchito con la fattispecie criminosa di cui sopra. L'articolo aggiunto dal D.Lgs. n. 109/2012 è stato modificato da ultimo dalla Legge 17 ottobre 2017 n. 161 (recante "Modifiche al codice delle leggi antimafia e delle misure di prevenzione, di cui al decreto legislativo 6 settembre 2011, n.159, al codice penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale e altre disposizioni. Delega al Governo per la tutela del lavoro nelle aziende sequestrate e confiscate"), che ha disposto (con l'art. 30, comma 4) l'introduzione dei commi 1-bis, 1-ter e 1-quater all'art. 25-duodecies in materia di Impiego di cittadini di paesi terzi il cui soggiorno è irregolare.

12.2. Aree a rischio

In relazione al reato della presente sezione della Parte Speciale del Modello, le aree ritenute più specificatamente a rischio risultano le seguenti:
- assunzione del personale, con particolare riferimento ai cittadini extracomunitari.

Tale situazione ad oggi non si è mai presentata, e questa parte del modello è stata inserita solo per essere pronti nel saper gestire correttamente questa possibilità.

12.3. Divieti

Divieti generali
È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall' art.25 duodecies del D. Lgs. n. 231/2001;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate dall' art. 25 duodecies del D. Lgs. n. 231/2001, possano potenzialmente diventarlo.

12.4. Procedure specifiche per aree sensibili

L'Amministratore Unico e le funzioni aziendali che intervengono nelle aree sensibili (es. Amministrazione) non possono impiegare lavoratori stranieri del tutto privi di permesso di soggiorno o con un permesso revocato o scaduto, del

quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale.

12.5. Presidi adottati

CODICE ETICO

13. Reato di razzismo e xenofobia (art. 25 terdecies)

13.1. I reati

In data 27 novembre 2017 è stata pubblicata in Gazzetta Ufficiale la Legge 20 novembre 2017 n. 167 "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2017". Il provvedimento amplia il catalogo dei reati presupposto del d.lgs. 231/2001, inserendo l'art. 25 terdecies rubricato come "razzismo e xenofobia".

I delitti di cui si fa dunque rimando puniscono i partecipanti di organizzazioni, associazioni, movimenti o gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici, nazionali, religiosi, nonché la propaganda ovvero l'istigazione e l'incitamento, commessi in modo che derivi concausa pericolo di diffusione, fondati in tutto o in parte sulla negazione, sulla minimizzazione in modo grave sull'apologia (inciso aggiunto dalla stessa legge Europea) della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra.

13.2. Aree a rischio

Si tratta di una tipologia di reato che riguarda la discriminazione razziale e xenofoba nei confronti di lavoratori stranieri o italiani presso qualsiasi sede della società, anche se in prova o impiegati a svolgere attività temporanee. In particolare l'area interessata è quella delle Risorse Umane perché ad essa è stata attribuita la responsabilità della gestione del personale.

13.3. Divieti

Divieti generali
E' fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall' art.25 terdecies del D. Lgs. n. 231/2001;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate dall' art. 25 terdecies del D. Lgs. n. 231/2001, possano potenzialmente diventarlo.

13.4. Procedure specifiche per aree sensibili

Chi ha la responsabilità della gestione/conduzione del personale deve prestare la massima attenzione per prevenire e nel caso sopprimere episodidi razzismo o xenofobia che potrebbero essere consumati sia da figure apicali che sottoposti, denunciando i fatti ai superiori interessati e all'Organismo di Vigilanza

Principi organizzativi e di controllo

Devono essere raccolte tutte le informazioni che potrebbero indicare la potenziale presenza di fatti di razzismo o xenofobia.

Procedure, prassi, regolamenti interni, circolari, linee guida in essere

A mitigazione del potenziale rischio riteniamo sufficienti le attuali regole presenti nel sistema qualità, nonché il Codice Etico.

13.5. Presidi adottati

CODICE ETICO

14. FRODE IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O DI SCOMMESSA E GIOCHI D'AZZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI" (art. 25 quaterdecies)

14.1. I reati

La legge n. 39 del 3.5.2019 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla manipolazione di competizioni sportive" ha introdotto l'art. 25 quaterdecies, che prevede pene per gli enti in relazione alla commissione dei reati di frode in competizioni sportive (art. 1) e di esercizio abusivo di attività di giuoco o di scommessa (art. 4), previsti dalla legge n. 401 del 13.12.1989.

14.2. Aree a rischio

Si tratta di una tipologia di reato che data la tipologia di attività svolte dalla MIZAR si ritiene molto improbabile.

14.3. Divieti

Divieti generali.
E' fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall' art.25 quatedecies del D. Lgs. n. 231/2001;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate dall' art. 25 quatedecies del D. Lgs. n. 231/2001, possano potenzialmente diventarlo.

14.4. Procedure specifiche per aree sensibili

A mitigazione del potenziale rischio riteniamo sufficienti i principi riportato nel Codice Etico.

14.5. Presidi adottati

CODICE ETICO

15. REATI TRIBUTARI (art. 25 quinquiesdecies)

15.1. I reati

L'art. 25-quinquiesdecies del D. Lgs. n. 231/2001, introdotto nel 2019 e ampliato dal D.Lgs. 14 luglio 2020, n. 75, disciplina la responsabilità dell'ente per specifici reati tributari previsti dal D.Lgs. 10 marzo 2000, n. 74.

Rientrano nel comma 1:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, commi 1 e 2-bis);
- dichiarazione fraudolenta mediante altri artifici (art. 3);
- emissione di fatture o altri documenti per operazioni inesistenti (art. 8, commi 1 e 2-bis);
- occultamento o distruzione di documenti contabili (art. 10);
- sottrazione fraudolenta al pagamento di imposte (art. 11).

Il comma 1-bis estende inoltre la responsabilità ai delitti di dichiarazione infedele (art. 4), omessa dichiarazione (art. 5) e indebita compensazione (art. 10-quater) quando sono commessi al fine di evadere l'IVA nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'Unione europea, dai quali consegua o possa conseguire un danno complessivo pari o superiore a 10 milioni di euro.

Le funzioni amministrative e contabili devono tenere conto anche delle modifiche intervenute sulla disciplina sostanziale dei reati tributari, applicando sempre la normativa fiscale e penale vigente al momento dei fatti.

15.2. Aree a rischio

Le aree di attività ritenute più specificamente a rischio ai fini della presente Parte Speciale sono:

- GESTIONE FATTURAZIONE/RENDICONTAZIONE
  – Gestione del controllo incrociato fattura/ordine acquisto;
  - Emissione o ricezione di fatture o documenti contabili
- GESTIONE RAPPORTI CON FORNITORI E SETTORE ACQUISTI
  - Gestione del processo di valutazione del fornitore;
  - Monitoraggio del servizio in conformità con l'ordine di acquisto contratto, sia in termini qualitativi che quantitativi.
- GESTIONE DEGLI ADEMPIMENTI TRIBUTARI: PREDISPOSIZIONE ED INVIO DEI DATI TELEMATICI ALL'ANAGRAFE TRIBUTARIA E PAGAMENTO DI IMPOSTE
  - predisposizione delle dichiarazioni relativa alle imposte sui redditi e sul valore aggiunto;
  - conservazione documentazione contabile;
  - gestione contenzioso con Amministrazione Finanziaria
- Operazioni transfrontaliere rilevanti ai fini IVA, gestione di operazioni intracomunitarie e rapporti con controparti estere.
- Gestione di crediti fiscali e compensazioni, incluse le verifiche sull'esistenza, spettanza e utilizzabilità dei crediti.

15.3. Divieti

Divieti generali
È fatto espresso divieto a carico dei Destinatari del Modello, di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate dall' art.25 quinquiesdecies del D. Lgs. n. 231/2001;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle considerate dall' art. 25 quinquiesdecies del D. Lgs. n. 231/2001, possano potenzialmente diventarlo.
- Porre in essere qualsiasi situazione di conflitto di interessi in relazione a quanto previsto dalle suddette ipotesi di reato

15.4. Procedure specifiche per aree sensibili

in merito alle competenze e responsabilità si evidenzia che la società nell'ambito del sistema qualità si è dotata di una regolamentazione dettagliata, nominativa per funzione dove sono evidenziati i compiti e le attività svolte da ciascuna persona.
Si evidenzia che i fornitori sono operatori economici in possesso di requisiti di onorabilità, di idoneità morale nonché capacità tecnica ed economico-finanziaria. Gli elenchi sono soggetti a revisione ed aggiornamento almeno manuale e l'ufficio è tenuto a verificare eventuali variazioni chiedendo carichi pendenti della società fornitore.
È necessario sensibilizzare le figure dell'area contabile soprattutto con riferimento a eventuali "distrazioni" contabili e gestionali.

- assicurare riconciliazioni periodiche tra fatture, contratti/ordini, prestazioni effettivamente rese o ricevute, pagamenti e registrazioni contabili;
- documentare le verifiche sui crediti utilizzati in compensazione e sulle operazioni IVA transfrontaliere di maggiore rilevanza o anomalia;
- conservare la documentazione fiscale e contabile secondo i termini di legge, impedendone alterazione, occultamento o distruzione;
- sottoporre a verifica qualificata le operazioni non ordinarie, con controparti estere o caratterizzate da elementi di anomalia fiscale.

15.5. Flussi informativi verso l'Organismo di Vigilanza

Le funzioni organizzative della MI.ZAR. SRL che nello svolgimento delle attività vengano a conoscenza di anomalie nelle procedure di fatturazione (attiva o passiva), provvedono a comunicare all'Organismo di Vigilanza, le anomalie o criticità riscontrate.

15.6. Presidi adottati

PGM-A Procedura generale di prevenzione
PGM-B Procedura generale di controllo

PGM-C Gestione Ciclo Attivo – Clienti
PGM-E Procedura contrattuale generale
PGM-F Procedura acquisto beni e servizi
PGM-G Procedura pagamenti
CODICE ETICO

16. REATI CONTRABBANDO (art. 25 sexiesdecies)

16.1. I reati

L'art. 25-sexiesdecies del D. Lgs. n. 231/2001 è stato introdotto dal D.Lgs. 14 luglio 2020, n. 75. A seguito della riforma doganale, dal 4 ottobre 2024 il rinvio non è più formulato con riferimento al previgente elenco del D.P.R. n. 43/1973.

La disposizione vigente prevede la responsabilità dell'ente in relazione ai reati previsti dalle disposizioni nazionali complementari al Codice doganale dell'Unione, adottate in attuazione degli artt. 11 e 20, commi 2 e 3, della L. 9 agosto 2023, n. 111, nonché dal D.Lgs. 26 ottobre 1995, n. 504 in materia di imposte sulla produzione e sui consumi e relative sanzioni.

La rilevanza concreta per MI.ZAR. SRL dipende dall'eventuale effettuazione, diretta o indiretta, di operazioni di importazione, esportazione, acquisto o movimentazione di beni con profili doganali o di accisa.

16.2. Aree a rischio

Il rischio è ordinariamente contenuto in ragione dell'attività di consulenza svolta da MI.ZAR. SRL, ma deve essere rivalutato qualora la Società effettui o organizzi operazioni con merci provenienti o destinate a Paesi extra-UE, importazioni temporanee, spedizioni, acquisti con formalità doganali o operazioni concernenti prodotti soggetti ad accisa.

Aree potenzialmente sensibili:

- acquisti e rapporti con fornitori esteri, spedizionieri, corrieri e rappresentanti doganali;
- documentazione commerciale, fatture, descrizione, origine, valore e classificazione delle merci eventualmente importate o esportate;
- pagamento di diritti doganali, imposte o accise, nonché gestione di eventuali agevolazioni o regimi speciali.

16.3. Divieti

È vietato porre in essere, collaborare o dare causa a condotte idonee a integrare i reati richiamati dall'art. 25-sexiesdecies del D. Lgs. n. 231/2001.

In particolare è vietato utilizzare documentazione falsa o incompleta, indicare origine, quantità, qualità, classificazione o valore delle merci non corrispondenti al vero, eludere il pagamento di diritti o imposte dovuti o utilizzare impropriamente regimi o agevolazioni doganali.

16.4. Procedure specifiche per aree sensibili

Qualora siano effettuate operazioni con rilevanza doganale o di accisa, MI.ZAR. SRL deve:

- utilizzare spedizionieri, intermediari e rappresentanti doganali qualificati, formalizzando ruoli e responsabilità;
- verificare la coerenza tra ordine/contratto, fattura, documenti di trasporto e documentazione doganale;
- conservare la documentazione relativa a origine, valore, classificazione, destinazione e adempimenti doganali delle merci;
- sottoporre a verifica le operazioni anomale, le richieste di sottovalutazione, falsa descrizione, triangolazione o utilizzo di documenti non coerenti.

16.5. Flussi informativi verso l'Organismo di Vigilanza

Devono essere segnalate all'OdV eventuali contestazioni doganali, sequestri, rettifiche di valore/origine/classificazione, anomalie documentali, richieste illecite da parte di controparti o intermediari e ogni altra circostanza potenzialmente rilevante ai fini dell'art. 25-sexiesdecies.

16.6. Presidi adottati

CODICE ETICO

PGM-E PROCEDURA CONTRATTUALE GENERALE

PGM-F ACQUISTO BENI E SERVIZI

PGM-G PAGAMENTI

17. DELITTI CONTRO IL PATRIMONIO CULTURALE (art. 25 septiesdecies.)

17.1. I reati

L'articolo 25 septiesdecies è stato inserito dall' art. 3, comma 1, L. 9 marzo 2022, n. 22, a decorrere dal 23 marzo 2022, ai sensi di quanto disposto dall' art. 7, comma 1, della medesima legge n. 22/2022.

In data 23 marzo 2022 è entrata in vigore la legge n.9/2022 recante "Disposizioni in materia di reati contro il patrimonio culturale" con la quale nel Codice penale s'inserisce il titolo VIII-bis, rubricato "Dei delitti contro il patrimonio culturale". La tutela dei bene culturali è centrale all'interno della nostra Costituzione ed attraverso questa legge il legislatore ha inteso razionalizzare il sistema penale inserendo all'interno del Codice penale norme contenute nel D.Lgs. n.42/2004 (Codice dei beni culturali e del paesaggio, c.d. Codice Urbani).

Per quanto attiene al Codice penale s'introducono i seguenti articoli che prevedono le nuove fattispecie di reato inserite nell'articolo 25 septiesdecies:

518-bis "Furto di beni culturali";

518-ter "Appropriazione indebita di beni culturali";

518-quater "Ricettazione di beni culturali";

518-quinquies "Impiego di beni culturali provenienti da delitto";

518-sexies "Riciclaggio di beni culturali";

518-septies "Autoriciclaggio di beni culturali";

518-octies "Falsificazione in scrittura privata relativa a beni culturali";

518-novies "Violazioni in materia di alienazione di beni culturali";

518-decies "Importazione illecita di beni culturali";

518-undecies "Uscita o esportazione illecite di beni culturali";

518-duodecies "Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici";

518-terdecies "Devastazione e saccheggio di beni culturali e paesaggistici";

518-quaterdecies "Contraffazione di opere d'arte"; art. 518-quinquiesdecies "Casi di non punibilità".

1. In relazione alla commissione del delitto previsto dall'articolo 518-novies del codice penale, si applica all'ente la sanzione pecuniaria da cento a quattrocento quote.

2. In relazione alla commissione dei delitti previsti dagli articoli 518-ter, 518-decies e 518-undecies del codice penale, si applica all'ente la sanzione pecuniaria da duecento a cinquecento quote.

3. In relazione alla commissione dei delitti previsti dagli articoli 518-duodecies e 518-quaterdecies del codice penale, si applica all'ente la sanzione pecuniaria da trecento a settecento quote.

4. In relazione alla commissione dei delitti previsti dagli articoli 518-bis, 518-quater e 518-octies del codice penale, si applica all'ente la sanzione pecuniaria da quattrocento a novecento quote.

5. Nel caso di condanna per i delitti di cui ai commi da 1 a 4, si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non superiore a due anni.

17.2. Aree a rischio

Considerata l'attività svolta dalla MI.ZAR. SRL non ci sono aree e attività a rischio per i DELITTI CONTRO IL PATRIMONIO CULTURALE.

17.3. Divieti

Non ci sono attività e aree a rischio.

17.4. Procedure specifiche per aree sensibili

Non ci sono attività e aree a rischio.

17.5. Flussi informativi verso l'Organismo di Vigilanza

Non ci sono attività e aree a rischio.

17.6. Presidi adottati

CODICE ETICO

18. RICICLAGGIO DI BENI CULTURALI E DEVASTAZIONE E SACCHEGGIO DI BENI CULTURALI E PAESAGGISTICI (art. 25 duodevicies)

18.1. I reati

L'articolo 25 duodevicies è stato inserito dall' art. 3, comma 1, L. 9 marzo 2022, n. 22, a decorrere dal 23 marzo 2022, ai sensi di quanto disposto dall' art. 7, comma 1, della medesima legge n. 22/2022.

1. In relazione alla commissione dei delitti previsti dagli articoli 518-sexies e 518-terdecies del codice penale, si applica all'ente la sanzione pecuniaria da cinquecento a mille quote.

2. Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti indicati al comma 1, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'articolo 16, comma 3.

18.2. Aree a rischio

Considerata l'attività svolta dalla MI.ZAR. SRL non ci sono aree e attività a rischio per RICICLAGGIO DI BENI CULTURALI E DEVASTAZIONE E SACCHEGGIO DI BENI CULTURALI E PAESAGGISTICI.

18.3. Divieti

Non ci sono attività e aree a rischio.

18.4. Procedure specifiche per aree sensibili

Non ci sono attività e aree a rischio.

18.5. Flussi informativi verso l'Organismo di Vigilanza

Non ci sono attività e aree a rischio.

18.6. Presidi adottati

CODICE ETICO

19. Reati in materia di violazione di misure restrittive dell'Unione europea (art. 25-octies.2)

19.1. I reati

Il D.Lgs. 30 dicembre 2025, n. 211, in vigore dal 24 gennaio 2026, ha introdotto nel D. Lgs. n. 231/2001 l'art. 25-octies.2, relativo alla violazione delle misure restrittive dell'Unione europea.

L'articolo richiama, in particolare:

- violazione delle misure restrittive dell'Unione europea nelle ipotesi previste dall'art. 275-bis, primo, secondo e quinto comma, c.p.;
- violazione degli obblighi informativi imposti da misure restrittive dell'Unione europea (art. 275-ter, primo e secondo comma, c.p.);
- violazione delle condizioni dell'autorizzazione allo svolgimento di attività soggette a misure restrittive (art. 275-quater, primo comma, c.p.);
- agevolazione dell'ingresso nel territorio dello Stato di persone fisiche designate, nei casi di cui all'art. 12, comma 1-bis, del D.Lgs. n. 286/1998.

Le condotte possono riguardare, tra l'altro, messa a disposizione di fondi o risorse economiche a soggetti designati, mancato congelamento, operazioni economiche/commerciali/finanziarie vietate, importazione o esportazione di beni, servizi e assistenza tecnica, elusione delle misure, omesse informazioni e inosservanza delle condizioni di autorizzazioni.

19.2. Aree a rischio

- rapporti commerciali e contrattuali con clienti, fornitori, consulenti, partner e altri soggetti esteri o con assetti proprietari/beneficiari effettivi esteri;
- incassi, pagamenti e altre operazioni finanziarie transfrontaliere;
- prestazione di servizi professionali, tecnici o informativi a soggetti operanti in Paesi interessati da misure restrittive UE;
- eventuali acquisti, vendite, importazioni, esportazioni, trasferimenti o assistenza riguardanti beni o tecnologie soggetti a restrizioni.

Per MI.ZAR. SRL il rischio assume particolare rilievo quando un incarico, una controparte, il relativo titolare effettivo, il Paese di destinazione o il servizio richiesto presentino collegamenti con misure restrittive dell'Unione europea.

19.3. Divieti

È fatto divieto di eseguire o agevolare operazioni vietate da misure restrittive dell'Unione europea, di mettere direttamente o indirettamente fondi o risorse economiche a disposizione di soggetti designati, di eludere congelamenti o restrizioni, di utilizzare documenti o dichiarazioni false per occultare titolari effettivi o beneficiari e di prestare servizi vietati o in difformità dalle autorizzazioni previste.

19.4. Procedure specifiche per aree sensibili

- effettuare, quando il rapporto o l'operazione presenta profili internazionali o altri indicatori di rischio, controlli sulle liste UE delle persone, entità e organismi soggetti a misure restrittive;
- verificare, in misura proporzionata al rischio, titolare effettivo, proprietà e controllo della controparte, Paese di destinazione, natura del servizio e finalità dell'operazione;
- sospendere l'operazione e sottoporla a verifica prima dell'esecuzione in presenza di corrispondenze, dubbi o anomalie;

- conservare evidenza dei controlli svolti, delle eventuali autorizzazioni e della documentazione contrattuale e finanziaria pertinente;
- inserire nei contratti, ove appropriato, clausole sul rispetto delle sanzioni e delle misure restrittive UE e sul diritto della Società di sospendere o risolvere il rapporto in caso di violazione.

19.5. Flussi informativi verso l'Organismo di Vigilanza

Devono essere comunicati all'OdV i casi di potenziale corrispondenza con soggetti designati, operazioni sospese o rifiutate per ragioni sanzionatorie, richieste di elusione, utilizzo di intermediari non trasparenti, richieste di modifica anomala di beneficiari o destinazioni, nonché contestazioni o richieste delle autorità competenti.

19.6. Presidi adottati

CODICE ETICO

PGM-A PROCEDURA GENERALE DI PREVENZIONE

PGM-B PROCEDURA GENERALE DI CONTROLLO

PGM-E PROCEDURA CONTRATTUALE GENERALE

PGM-F ACQUISTO BENI E SERVIZI

PGM-G PAGAMENTI

20. Delitti contro gli animali (art. 25-undevicies)

20.1. I reati

La L. 6 giugno 2025, n. 82, in vigore dal 1° luglio 2025, ha introdotto nel D. Lgs. n. 231/2001 l'art. 25-undevicies, relativo ai delitti contro gli animali. Sono richiamati gli artt. 544-bis, 544-ter, 544-quater, 544-quinquies e 638 c.p., fermo quanto previsto dal comma 3 dell'art. 25-undevicies per i casi di cui all'art. 19-ter delle disposizioni di coordinamento e transitorie per il codice penale.

20.2. Aree a rischio

In base alle attività descritte nel presente Modello non risultano individuate attività tipiche di MI.ZAR. SRL che comportino ordinariamente la gestione, custodia, allevamento, impiego o commercio di animali. Il rischio è pertanto valutato come residuale, ferma la necessità di rivalutarlo qualora siano organizzati eventi, sponsorizzazioni, servizi o rapporti con terzi che possano coinvolgere animali.

20.3. Divieti

È vietato porre in essere, favorire, finanziare, commissionare o tollerare condotte che possano integrare i delitti richiamati dall'art. 25-undevicies, incluse uccisione o maltrattamento di animali, organizzazione di spettacoli o manifestazioni vietate e combattimenti tra animali.

20.4. Procedure specifiche per aree sensibili

- qualora un'attività aziendale o iniziativa promozionale coinvolga animali, verificarne preventivamente liceità, autorizzazioni e condizioni di svolgimento;
- nei rapporti con fornitori o partner che, per l'oggetto del servizio, possano coinvolgere animali, prevedere obblighi di rispetto della normativa e delle regole del Codice Etico;
- segnalare tempestivamente anomalie o sospetti di condotte illecite alle funzioni aziendali competenti e all'OdV.

20.5. Flussi informativi verso l'Organismo di Vigilanza

Devono essere segnalati all'OdV episodi, contestazioni, denunce o informazioni attendibili relative a condotte contro animali connesse, anche indirettamente, ad attività, fornitori, partner o iniziative della Società.

20.6. Presidi adottati

CODICE ETICO

PGM-A PROCEDURA GENERALE DI PREVENZIONE

PGM-B PROCEDURA GENERALE DI CONTROLLO

PGM-E PROCEDURA CONTRATTUALE GENERALE

21. REATI COMMESSI CON L'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE (art. 25-vicies del D.Lgs. 231/2001)

21.1. I reati

Il D.Lgs. 9 settembre 2026, n. 160, entrato in vigore il 30 settembre 2026, ha introdotto, mediante l'art. 15, l'art. 25-vicies nel D.Lgs. 231/2001, rubricato «Reati commessi con l'uso di sistemi di intelligenza artificiale».

La disposizione prevede la responsabilità amministrativa degli enti in relazione ai seguenti delitti:

a) Art. 437-bis c.p. – Omessa adozione di misure di sicurezza nei sistemi di intelligenza artificiale e alterazione illecita dei sistemi.

La fattispecie riguarda, nei casi e alle condizioni previste dalla norma:

- *l'omessa adozione delle misure tecniche di sicurezza previste per la progettazione, l'addestramento, la produzione e l'immissione sul mercato di sistemi di intelligenza artificiale ad alto rischio;*
- *l'omessa adozione di misure di sorveglianza umana;*
- *l'alterazione illecita di sistemi di intelligenza artificiale ad alto rischio;*
- *l'omissione intenzionale delle misure di sorveglianza umana da parte dell'utilizzatore professionale di sistemi ad alto rischio.*

La rilevanza penale di tali condotte è subordinata agli specifici presupposti previsti dall'articolo, tra cui il verificarsi di un pericolo per la vita o l'incolumità pubblica o individuale oppure per la sicurezza dello Stato.

La norma contempla anche specifiche ipotesi di responsabilità per colpa grave.

Per tale reato l'art. 25-vicies prevede, a carico dell'ente, una sanzione pecuniaria da 600 a 1.000 quote.

b) Art. 612-quater c.p. – Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale.

Il delitto riguarda la cessione, pubblicazione o diffusione, senza il consenso della persona interessata, di immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale, idonei a indurre in inganno sulla loro genuinità, quando dalla condotta derivi un danno ingiusto alla persona.

Per tale reato l'art. 25-vicies prevede, a carico dell'ente, una sanzione pecuniaria da 200 a 700 quote.

Per entrambe le fattispecie sono inoltre previste le sanzioni interdittive di cui all'art. 9, comma 2, lettere b), c), d) ed e), del D.Lgs. 231/2001, secondo le condizioni di applicabilità stabilite dal Decreto.

La responsabilità amministrativa di MI.ZAR. SRL può configurarsi esclusivamente in presenza dei presupposti stabiliti dal D.Lgs. 231/2001, compresa la commissione del reato nell'interesse o a vantaggio della Società.

21.2. Aree a rischio

In considerazione delle caratteristiche organizzative di MI.ZAR. SRL e delle attività di consulenza, assistenza tecnica, formazione e gestione documentale svolte dalla Società, vengono individuate le seguenti aree potenzialmente sensibili.

a) Utilizzo di sistemi di intelligenza artificiale nelle attività di consulenza

Impiego di strumenti di intelligenza artificiale per ricerche normative, elaborazione di documenti tecnici, valutazioni di conformità, predisposizione di procedure, analisi dei rischi, relazioni e documentazione destinata ai clienti.

Il rischio rilevante ai fini dell'art. 25-vicies deve essere valutato in relazione alle specifiche caratteristiche dei sistemi impiegati e alle condotte previste dalle fattispecie penali.

b) Utilizzo di sistemi di intelligenza artificiale ad alto rischio

Eventuale impiego, sviluppo, configurazione, modifica o utilizzo professionale di sistemi classificabili ad alto rischio ai sensi del Regolamento (UE) 2024/1689.

La valutazione riguarda le misure di sicurezza, le eventuali misure di sorveglianza umana e le possibili conseguenze derivanti dalla loro omissione o dall'alterazione illecita dei sistemi.

c) Produzione e diffusione di contenuti mediante intelligenza artificiale

Utilizzo di sistemi di intelligenza artificiale per la predisposizione di immagini, video, registrazioni vocali, presentazioni, contenuti formativi, comunicazioni pubblicitarie e materiali informativi.

Particolare attenzione viene riservata ai contenuti che riproducono o alterano immagini, voci o video riferibili a persone reali e che potrebbero essere erroneamente ritenuti autentici.

d) Gestione dei sistemi informatici e delle piattaforme di intelligenza artificiale

Attività di autorizzazione all'utilizzo dei sistemi, gestione degli accessi, configurazione delle piattaforme e controllo delle eventuali modifiche apportate alle impostazioni o alle misure di sicurezza.

e) Affidamento di attività a fornitori e collaboratori esterni

Eventuale ricorso a soggetti esterni che utilizzano sistemi di intelligenza artificiale per conto della Società, con particolare riferimento alla produzione di contenuti audiovisivi e all'utilizzo di sistemi ad alto rischio.

L'effettiva esposizione ai rischi individuati viene determinata mediante il Risk Assessment aziendale, tenendo conto delle attività concretamente svolte, dei sistemi utilizzati e dei controlli applicati.

21.3. Divieti

Ai destinatari del presente Modello è fatto divieto di porre in essere, direttamente o indirettamente, comportamenti che possano integrare le fattispecie previste dall'art. 25-vicies del D.Lgs. 231/2001.

In particolare, è vietato:

1. *Omettere le misure tecniche di sicurezza previste dalla normativa applicabile per i sistemi di intelligenza artificiale ad alto rischio, quando l'omissione possa determinare le situazioni di pericolo considerate dall'art. 437-bis c.p.*
2. *Omettere intenzionalmente le misure di sorveglianza umana previste per l'utilizzo professionale dei sistemi di intelligenza artificiale ad alto rischio, nei casi contemplati dalla normativa penale.*
3. *Alterare illecitamente sistemi di intelligenza artificiale ad alto rischio, anche mediante modifiche non autorizzate delle relative configurazioni, qualora ricorrano le condizioni previste dall'art. 437-bis c.p.*
4. *Cedere, pubblicare o diffondere senza il consenso della persona interessata immagini, video o voci falsificati o alterati mediante sistemi di intelligenza artificiale, idonei a ingannare sulla loro autenticità, con le conseguenze previste dall'art. 612-quater c.p.*
5. *Utilizzare sistemi di intelligenza artificiale per commettere, agevolare o occultare reati-presupposto previsti dal D.Lgs. 231/2001.*
6. *Eludere i controlli, le autorizzazioni e le limitazioni stabiliti dalle procedure aziendali per l'utilizzo dei sistemi di intelligenza artificiale.*
7. *Omettere la segnalazione di anomalie o situazioni di rischio rilevanti ai fini della prevenzione dei reati-presupposto.*
8. *Utilizzare contenuti generati mediante intelligenza artificiale in violazione delle istruzioni aziendali relative alla verifica, alla validazione e alla diffusione di documenti e comunicazioni.*

I divieti di cui ai punti 5, 6, 7 e 8 costituiscono ulteriori misure preventive organizzative, anche quando la singola inosservanza non integri autonomamente uno dei reati previsti dall'art. 25-vicies.

21.4. Procedure specifiche per aree sensibili

Per prevenire i rischi di commissione dei reati previsti dall'art. 25-vicies, MI.ZAR. SRL definisce e applica, in misura proporzionata alle attività svolte e ai sistemi utilizzati, le seguenti misure organizzative.

a) Identificazione dei sistemi di intelligenza artificiale

I sistemi utilizzati nell'ambito delle attività aziendali sono identificati mediante apposito inventario.

Per ciascun sistema sono registrati, ove pertinenti, la denominazione, il fornitore, la finalità di utilizzo, le funzioni aziendali interessate e la classificazione del rischio.

b) Valutazione dei rischi

L'utilizzo dei sistemi di intelligenza artificiale viene considerato nell'ambito della valutazione dei rischi di commissione dei reati-presupposto.

Con particolare riferimento all'art. 437-bis c.p., viene verificata l'eventuale presenza di sistemi ad alto rischio e l'applicabilità delle misure tecniche di sicurezza e sorveglianza umana.

Con riferimento all'art. 612-quater c.p., vengono valutate le attività di produzione e diffusione di contenuti audiovisivi generati o alterati artificialmente.

c) Autorizzazione all'utilizzo

La Direzione individua i sistemi di intelligenza artificiale utilizzabili per le attività aziendali, definendo eventuali limitazioni e responsabilità.

L'introduzione di nuovi sistemi, quando comporti rischi significativi, è sottoposta a preventiva valutazione.

d) Verifica umana dei risultati

I risultati prodotti mediante intelligenza artificiale e utilizzati nelle attività di consulenza sono sottoposti alle verifiche professionali previste dalle procedure aziendali.

Particolare attenzione viene riservata alla correttezza delle informazioni normative, tecniche e contrattuali riportate nei documenti destinati ai clienti.

e) Gestione dei sistemi ad alto rischio

Qualora MI.ZAR. SRL utilizzi sistemi classificabili ad alto rischio, sono individuati gli obblighi applicabili in funzione del ruolo effettivamente ricoperto dalla Società.

Vengono definite le responsabilità per l'applicazione delle misure di sicurezza e di sorveglianza umana, per la gestione delle anomalie e per la verifica delle condizioni di utilizzo.

f) Produzione e diffusione dei contenuti audiovisivi

La pubblicazione o diffusione di immagini, video e contenuti audio generati o alterati mediante intelligenza artificiale è soggetta alle verifiche e alle autorizzazioni aziendali previste.

Quando i contenuti riproducono o modificano l'immagine o la voce di persone identificabili, devono essere verificate la liceità del trattamento, la disponibilità dei consensi necessari e le condizioni per la pubblicazione.

g) Gestione delle anomalie

Eventuali anomalie, incidenti, utilizzi non autorizzati o violazioni delle procedure sono segnalati ai soggetti aziendali competenti.

Le situazioni rilevanti ai fini del D.Lgs. 231/2001 sono comunicate all'Organismo di Vigilanza secondo i flussi informativi previsti dal Modello.

h) Formazione

Il personale interessato riceve informazioni e formazione sulle regole aziendali relative all'utilizzo dell'intelligenza artificiale, sui principali rischi e sui comportamenti vietati.

La formazione è aggiornata in occasione di modifiche normative o dell'introduzione di sistemi con caratteristiche significativamente diverse.

21.5. Flussi informativi verso l'Organismo di Vigilanza

Al fine di consentire all'Organismo di Vigilanza di svolgere le proprie funzioni di controllo sull'effettiva applicazione del Modello, sono previsti specifici flussi informativi riguardanti l'utilizzo dei sistemi di intelligenza artificiale.

Devono essere comunicate all'Organismo di Vigilanza, secondo le modalità stabilite dal Modello:

a) Informazioni periodiche

- *Aggiornamenti significativi dell'inventario dei sistemi di intelligenza artificiale utilizzati dalla Società.*
- *Esiti della valutazione dei rischi relativi all'art. 25-vicies.*
- *Eventuale introduzione di sistemi classificabili ad alto rischio.*
- *Stato di attuazione delle misure organizzative e dei controlli previsti.*
- *Principali attività formative realizzate in materia di utilizzo dell'intelligenza artificiale.*

b) Informazioni tempestive

- *Anomalie significative o violazioni delle misure di sicurezza e sorveglianza umana applicabili ai sistemi di intelligenza artificiale ad alto rischio.*
- *Alterazioni non autorizzate di sistemi ad alto rischio, quando potenzialmente rilevanti ai fini dell'art. 437-bis c.p.*

- *Contestazioni o segnalazioni relative alla diffusione illecita di contenuti audiovisivi generati o alterati mediante intelligenza artificiale.*
- *Circostanze che possano far presumere la commissione dei reati-presupposto previsti dall'art. 25-vicies.*
- *Avvio di procedimenti o ricezione di contestazioni da parte delle autorità competenti in relazione ai reati considerati.*
- *Violazioni significative delle procedure aziendali in materia di intelligenza artificiale.*

Le informazioni trasmesse all'Organismo di Vigilanza devono essere adeguatamente documentate, nei limiti della disponibilità delle evidenze e nel rispetto della normativa applicabile.

L'Organismo di Vigilanza può richiedere ulteriori informazioni, chiarimenti o documenti e proporre l'adozione di misure correttive o il riesame della valutazione dei rischi.

I flussi informativi ordinari sono coordinati con il sistema di segnalazione whistleblowing, nel rispetto del D.Lgs. 24/2023.

21.6. Presidi adottati

Per la prevenzione dei reati-presupposto previsti dall'art. 25-vicies, MI.ZAR. SRL individua quali presidi organizzativi di riferimento, da applicare secondo la loro effettiva pertinenza e attuazione:

1. *Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001.*
2. *Codice Etico aziendale e relativo sistema disciplinare.*
3. *Valutazione dei rischi di commissione dei reati-presupposto, comprensiva dell'analisi delle fattispecie previste dall'art. 25-vicies.*
4. *Procedura aziendale per l'utilizzo responsabile dei sistemi di intelligenza artificiale.*
5. *Inventario dei sistemi di intelligenza artificiale utilizzati nell'ambito delle attività aziendali.*
6. *Regole di autorizzazione e controllo degli accessi ai sistemi informatici e alle piattaforme di intelligenza artificiale.*
7. *Misure tecniche e organizzative di sicurezza informatica applicabili ai sistemi utilizzati.*
8. *Verifica e validazione dei risultati generati mediante intelligenza artificiale prima del loro utilizzo nei documenti professionali destinati ai clienti.*
9. *Regole per la produzione, verifica e diffusione di immagini, video e contenuti audio generati o alterati artificialmente.*

10. *Attività di informazione e formazione dei soggetti che utilizzano sistemi di intelligenza artificiale.*
11. *Sistema di registrazione e gestione delle anomalie, delle non conformità e delle azioni correttive.*
12. *Flussi informativi e attività di verifica dell'Organismo di Vigilanza.*
13. *Sistema di gestione per la qualità conforme alla UNI EN ISO 9001, per gli aspetti pertinenti alla gestione dei processi, delle responsabilità, delle competenze e delle informazioni documentate.*

L'efficacia dei presidi è verificata in occasione dell'aggiornamento del Risk Assessment, delle attività di vigilanza e del riesame delle procedure aziendali.

Eventuali carenze vengono gestite mediante la definizione di azioni correttive, con individuazione delle responsabilità, dei tempi di attuazione e delle modalità di verifica.

La documentazione relativa alle valutazioni e ai controlli costituisce evidenza dell'attuazione delle misure preventive previste dal presente Modello.

Aggiornamento normativo delle Parti Speciali effettuato al 31 ottobre 2026.