REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 0	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

FRANCESCO
PATERNO'

SOMMARIO

1 DEFINIZIONI 5
1. DEFINIZIONI 5
2 ACRONIMI AZIENDALI 7
3 PROFILO DELLA SOCIETA' 7
3.1. PRESENTAZIONE DELLA SOCIETÀ 7
3.2 SISTEMA DI GOVERNANCE 8
3.3 SISTEMA DI CONTROLLO INTERNO 8
3.4 SISTEMA INTEGRATO DI COMPLIANCE 9
3.5 FINALITÀ DEL MODELLO 9
4. IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 10
4.1 PREMESSA 10
4.2 PRESUPPOSTI DELLA RESPONSABILITÀ DELL'ENTE 10
4.3 INTERESSE E VANTAGGIO 10
4.4 SOGGETTI RILEVANTI 11
4.5 ESCLUSIONE DELLA RESPONSABILITÀ DELL'ENTE 11
3.6 I REATI PRESUPPOSTOPRINCIPALI INTERVENTI NORMATIVI DI AGGIORNAMENTO DEL CATALOGO DEI REATI PRESUPPOSTO 12
4.7 LE SANZIONI PREVISTE DAL DECRETO 13
4.8 IL MODELLO QUALE STRUMENTO DI PREVENZIONE 13
5. LE AREE DI RISCHIO E LE PARTI SPECIALI DEL MODELLO 14
5.1 PREMESSA 14
5.2 LE PARTI SPECIALI DEL MODELLO 15
5. 3 AREE DI RISCHIO SPECIFICHE DI IDRAGEST 15
5.4 PRINCIPI GENERALI DI CONTROLLO 17
5.5 AGGIORNAMENTO DELL'ANALISI DEI RISCHI 17
6. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI IDRAGEST S.R.L. 18
6.1 FINALITÀ DEL MODELLO 18
6.2 PRINCIPI ISPIRATORI 18
6.3 STRUTTURA DEL MODELLO 19

6.4 DESTINATARI DEL MODELLO 19
6.5 OBBLIGHI DEI DESTINATARI 20
6.6 DIFFUSIONE DEL MODELLO 20
6.7 RAPPORTI CON IL SISTEMA AZIENDALE DI COMPLIANCE 21
7. L'ORGANISMO DI VIGILANZA 21
7.1 RUOLO E FUNZIONI 21
7.2 NOMINA E COMPOSIZIONE 21
7.3 COMPITI DELL'ORGANISMO DI VIGILANZA 22
7.4 POTERI DELL'ORGANISMO DI VIGILANZA 22
7.5 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 22
7.6 GESTIONE DELLE SEGNALAZIONI 23
7.7 REPORTING 23
7.8 CONSERVAZIONE DELLA DOCUMENTAZIONE 24
8 IL SISTEMA DI CONTROLLO INTERNO E I PROTOCOLLI DI PREVENZIONE 24
8.1 PRINCIPI GENERALI DEL SISTEMA DI CONTROLLO INTERNO 24
8.2 PRINCIPI DI CONTROLLO 25
8.3 SISTEMA DELLE DELEGHE E DELLE PROCURE 25
8.4 TRACCIABILITÀ DELLE OPERAZIONI 25
8.5 SEGREGAZIONE DELLE FUNZIONI 26
8.6 PROCEDURE AZIENDALI E PARTI SPECIALI 26
8.7 GESTIONE DELLE ANOMALIE 26
8.8 RIESAME DEL SISTEMA DI CONTROLLO INTERNO 27
9. FLUSSI INFORMATIVI, SEGNALAZIONI, FORMAZIONE E DIFFUSIONE DEL MODELLO 27
9.1 PRINCIPI GENERALI 27
9.2 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 28
9.3 FLUSSI INFORMATIVI STRAORDINARI 28
9.4 SISTEMA DI SEGNALAZIONE (WHISTLEBLOWING) 28
9.5 RAPPORTI TRA LA PROCEDURA WHISTLEBLOWING E L'ORGANISMO DI VIGILANZA 29
9.6 INFORMAZIONE E FORMAZIONE 29

9.7 DIFFUSIONE DEL MODELLO 30
9.8 CONSERVAZIONE DELLE EVIDENZE 30
9. SISTEMA DISCIPLINARE 30
9.1 PRINCIPI GENERALI 30
9.2 FINALITÀ 30
9.3 VIOLAZIONI RILEVANTI 31
9.4 DESTINATARI DELLE MISURE DISCIPLINARI 31
9.5 MISURE NEI CONFRONTI DEI DIPENDENTI 32
9.7 MISURE NEI CONFRONTI DEGLI AMMINISTRATORI 32
9.8 MISURE NEI CONFRONTI DI CONSULENTI, FORNITORI E PARTNER 32
9.9 RAPPORTI CON L'ORGANISMO DI VIGILANZA 32
10. AGGIORNAMENTO E MIGLIORAMENTO CONTINUO DEL MODELLO 32
10.1 PRINCIPI GENERALI 33
10.2 COMPETENZA ALL'AGGIORNAMENTO 33
10.3 RUOLO DELL'ORGANISMO DI VIGILANZA 33
10.4 PRESUPPOSTI PER L'AGGIORNAMENTO DEL MODELLO 33
10.5 RIESAME PERIODICO 34
10.6 AGGIORNAMENTO DELLE PARTI SPECIALI 34
10.7 COMUNICAZIONE DEGLI AGGIORNAMENTI 34
11. DISPOSIZIONI FINALI 35
11.1 ADOZIONE ED ENTRATA IN VIGORE 35
11.2 DIFFUSIONE E CONOSCIBILITÀ 35
11.3 COORDINAMENTO CON IL SISTEMA DI COMPLIANCE AZIENDALE 35
11.4 RIESAME DOCUMENTALE 36
12 IL CODICE ETICO 36

1. DEFINIZIONI

Ai fini della presente Parte Generale e delle Procedure Speciali che compongono il Modello di Organizzazione, Gestione e Controllo di IDRAGEST S.r.l., i termini di seguito indicati assumono il seguente significato.

Attività sensibili

Le attività aziendali nel cui ambito, in ragione della natura delle operazioni svolte o delle relazioni instaurate con soggetti pubblici o privati, sussiste il rischio di commissione dei reati presupposto previsti dal D.Lgs. 231/2001.

Codice Etico

Il documento approvato dal Consiglio di Amministrazione che definisce i principi etici, i valori e le regole di comportamento cui devono attenersi tutti i Destinatari del Modello.

Consiglio di Amministrazione (CdA)

L'organo amministrativo della Società competente, tra l'altro, all'adozione, all'attuazione e all'aggiornamento del Modello di Organizzazione, Gestione e Controllo.

Controlli preventivi

L'insieme dei presidi organizzativi, autorizzativi, procedurali, documentali e informatici finalizzati a prevenire la commissione dei reati presupposto e a garantire la tracciabilità delle attività aziendali.

Destinatari

Gli amministratori, i dirigenti, i dipendenti, i collaboratori, i consulenti, i professionisti, i partner commerciali, i fornitori e, più in generale, tutti i soggetti che operano, anche temporaneamente, nell'interesse o a vantaggio della Società e che sono tenuti al rispetto del Modello.

Decreto o D.Lgs. 231/2001

Il Decreto Legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", e successive modificazioni e integrazioni.

Flussi informativi

Le informazioni, i dati, gli atti, i documenti e le comunicazioni che devono essere trasmessi

all'Organismo di Vigilanza, con periodicità ordinaria ovvero in via immediata, secondo quanto previsto dal presente Modello e dalle procedure aziendali.

MODELLO O MOG 231: Il presente Modello di Organizzazione, Gestione e Controllo adottato da IDRAGEST S.r.l. ai sensi degli artt. 6 e 7 del D.Lgs. 231/2001, composto dalla Parte Generale, dalle Parti Speciali, dal Codice Etico, dal Sistema Disciplinare e dagli ulteriori documenti richiamati.

ORGANISMO DI VIGILANZA (ODV): L'organismo dotato di autonomi poteri di iniziativa e controllo cui è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello, verificarne l'efficacia e promuoverne l'aggiornamento mediante apposite segnalazioni e proposte al Consiglio di Amministrazione.

PARTI SPECIALI: Le procedure speciali che disciplinano i processi aziendali esposti al rischio di commissione dei reati presupposto e che costituiscono parte integrante e sostanziale del presente Modello.

PROCESSI SENSIBILI: I processi aziendali individuati a seguito dell'attività di risk assessment nei quali possono manifestarsi rischi di commissione dei reati previsti dal D.Lgs. 231/2001.

REATI PRESUPPOSTO: Le fattispecie di reato espressamente richiamate dal D.Lgs. 231/2001 e dalle successive disposizioni normative che possono determinare la responsabilità amministrativa della Società.

RISK ASSESSMENT: L'attività periodica di identificazione, analisi e valutazione dei rischi di commissione dei reati presupposto, finalizzata alla definizione e all'aggiornamento delle misure di prevenzione contenute nel Modello.

SEGNALAZIONE: Qualsiasi comunicazione avente ad oggetto comportamenti, fatti, omissioni o circostanze che possano costituire violazione del Modello, del Codice Etico, delle Procedure Speciali o della normativa rilevante ai fini del D.Lgs. 231/2001.

SISTEMA DISCIPLINARE: L'insieme delle misure sanzionatorie previste dalla Società nei confronti dei Destinatari che violino le disposizioni contenute nel Modello, nel Codice Etico o nelle Procedure Speciali.

SISTEMA DI CONTROLLO INTERNO: L'insieme delle regole organizzative, delle deleghe, delle procedure, dei controlli operativi, amministrativi e informatici adottati dalla Società per assicurare una gestione corretta, trasparente, efficiente e conforme alla normativa vigente.

WHISTLEBLOWING: Il sistema interno di segnalazione delle violazioni disciplinato dal D.Lgs. 24/2023 e dalla specifica procedura adottata dalla Società, volto a garantire la riservatezza dell'identità del segnalante e la tutela contro qualsiasi forma di ritorsione.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC	Responsabile Tecnico
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RFAM	Responsabile Facility Management
RPROG	Responsabile Progettazione
RGAD	Responsabili Gestione Archivi e Documenti
CDL	Consulente del Lavoro
REC	Responsabile Esterno Contabilità
RIA	Responsabile Intelligenza Artificiale
RA	Responsabile Anticorruzione

I suddetti acronimi aziendali corrispondono alle funzioni e ai ruoli dei soggetti affidatari, per la cui identificazione si rinvia all'organigramma aziendale di Idragest S.r.l..

3 PROFILO DELLA SOCIETA'

3.1. PRESENTAZIONE DELLA SOCIETÀ

IDRAGEST S.r.l. opera nel settore dell'ingegneria applicata ai servizi idrici, delle tecnologie informatiche e dei sistemi di monitoraggio delle infrastrutture, offrendo servizi specialistici ad elevato contenuto tecnico a favore di soggetti pubblici e privati.

In particolare, la Società svolge attività di:

1. progettazione, sviluppo e gestione di sistemi informativi territoriali (SIT);
2. rilievi topografici, georeferenziazione e acquisizione dati;
3. progettazione e modellazione di reti idriche e fognarie;
4. sviluppo e manutenzione di software dedicati alla gestione delle infrastrutture;
5. servizi di ingegneria, consulenza tecnica e supporto specialistico;

6. monitoraggio, digitalizzazione e gestione delle reti di distribuzione dei fluidi;
7. supporto tecnico nell'ambito di procedure di gara, collaudi e attività di formazione.

Le attività sono svolte nel rispetto dei principi di legalità, correttezza, trasparenza, imparzialità, professionalità e responsabilità sociale che costituiscono valori fondamentali dell'organizzazione aziendale.

3.2 SISTEMA DI GOVERNANCE

La Società adotta un sistema di governance volto ad assicurare una chiara attribuzione delle responsabilità, la separazione delle funzioni, la tracciabilità dei processi decisionali e l'efficacia del sistema dei controlli interni.

Il sistema di governo societario è fondato, tra l'altro, sui seguenti elementi:

1. Consiglio di Amministrazione;
2. organigramma aziendale costantemente aggiornato;
3. procedure organizzative e operative;
4. Codice Etico;
5. Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001;
6. Organismo di Vigilanza;
7. sistema disciplinare;
8. sistema di whistleblowing;
9. sistema documentale aziendale.

Tali strumenti operano in modo coordinato al fine di prevenire il rischio di commissione dei reati presupposto e garantire il rispetto della normativa applicabile.

3.3 SISTEMA DI CONTROLLO INTERNO

Il sistema di controllo interno di IDRAGEST costituisce parte integrante dell'organizzazione aziendale ed è finalizzato a garantire:

1. la conformità dell'attività aziendale alla normativa vigente;
2. la tutela del patrimonio aziendale;
3. l'affidabilità delle informazioni economiche, finanziarie e gestionali;
4. la corretta gestione dei rapporti con la Pubblica Amministrazione e con i soggetti privati;
5. la prevenzione dei rischi di commissione dei reati previsti dal D.Lgs. 231/2001;
6. il miglioramento continuo dell'efficacia dei processi aziendali.

Il sistema di controllo interno si fonda, in particolare, sui principi di:

1. separazione delle funzioni;
2. attribuzione formalizzata di responsabilità e poteri;
3. tracciabilità delle attività e delle decisioni;

4. documentazione delle operazioni rilevanti;
5. controlli preventivi e successivi;
6. verificabilità delle operazioni;
7. conservazione della documentazione;
8. monitoraggio continuo dei processi sensibili.

3.4 SISTEMA INTEGRATO DI COMPLIANCE

Il Modello di Organizzazione, Gestione e Controllo non costituisce un documento autonomo, ma si inserisce in un più ampio sistema aziendale di compliance.

Ne fanno parte, tra gli altri:

1. il Codice Etico;
2. le Parti Speciali del Modello;
3. il Sistema Disciplinare;
4. la procedura Whistleblowing;
5. la Politica Anticorruzione;
6. la Policy sull'utilizzo dell'Intelligenza Artificiale;
7. le procedure organizzative e operative adottate dalla Società;
8. le eventuali certificazioni di sistema conseguite dalla Società.

L'insieme di tali strumenti costituisce un sistema unitario di prevenzione dei rischi aziendali, orientato alla diffusione di una cultura della legalità, dell'etica d'impresa e della gestione responsabile.

3.5 FINALITÀ DEL MODELLO

Con l'adozione del presente Modello la Società intende:

1. prevenire il rischio di commissione dei reati previsti dal D.Lgs. 231/2001;
2. diffondere una cultura improntata alla legalità e alla trasparenza;
3. promuovere comportamenti conformi ai principi del Codice Etico;
4. rafforzare il sistema di controllo interno;
5. assicurare la corretta gestione dei processi sensibili;
6. tutelare il patrimonio, la reputazione e l'affidabilità della Società;
7. garantire la piena collaborazione con le Autorità competenti;
8. favorire il miglioramento continuo del sistema di compliance aziendale.

Il Modello rappresenta pertanto uno strumento dinamico di organizzazione, gestione e controllo che si integra con gli altri presidi aziendali e viene periodicamente verificato e aggiornato in relazione all'evoluzione normativa, organizzativa e ai risultati delle attività di vigilanza svolte dall'Organismo di Vigilanza.

4. IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

4.1 PREMESSA

Il Decreto Legislativo 8 giugno 2001, n. 231 (di seguito anche il "Decreto"), ha introdotto nell'ordinamento italiano la responsabilità amministrativa degli enti per determinati reati commessi nel loro interesse o vantaggio da soggetti che operano nell'ambito della loro organizzazione.

Tale disciplina ha profondamente innovato il sistema della responsabilità degli enti, affiancando alla responsabilità penale della persona fisica una distinta forma di responsabilità dell'ente, autonoma e diretta, che può comportare l'applicazione di rilevanti sanzioni pecuniarie e interdittive.

La responsabilità dell'ente non sostituisce quella della persona fisica autore del reato, ma si aggiunge ad essa, perseguendo la finalità di incentivare l'adozione di efficaci sistemi di organizzazione, gestione e controllo idonei a prevenire la commissione dei reati previsti dal Decreto.

4.2 PRESUPPOSTI DELLA RESPONSABILITÀ DELL'ENTE

Ai sensi del D.Lgs. 231/2001, la responsabilità amministrativa della Società può configurarsi quando ricorrono congiuntamente i seguenti presupposti:

1. è stato commesso uno dei reati espressamente previsti dal Decreto (reati presupposto);
2. il reato è stato commesso nell'interesse o a vantaggio della Società;
3. il reato è stato commesso da uno dei soggetti individuati dagli articoli 5, 6 e 7 del Decreto;
4. il Modello di Organizzazione, Gestione e Controllo risulti assente, inefficace, non correttamente attuato ovvero eluso fraudolentemente.

La mera commissione di un reato da parte di un soggetto appartenente all'organizzazione aziendale non determina automaticamente la responsabilità della Società, essendo necessario verificare la sussistenza di tutti i presupposti previsti dalla normativa.

4.3 INTERESSE E VANTAGGIO

Ai fini dell'applicazione del Decreto, la responsabilità dell'ente presuppone che il reato sia stato commesso nel suo interesse o a suo vantaggio.

Per **interesse** si intende la finalizzazione della condotta al perseguimento di un'utilità per la Società, valutata con riferimento al momento in cui il fatto viene posto in essere.

Per **vantaggio** si intende il beneficio, anche non esclusivamente economico, effettivamente conseguito dalla Società quale conseguenza della condotta illecita.

I due criteri sono alternativi e autonomi: la responsabilità dell'ente può sussistere anche quando ricorra uno solo di essi.

Resta esclusa la responsabilità della Società quando il soggetto agente abbia operato nell'interesse esclusivo proprio o di terzi.

4.4 SOGGETTI RILEVANTI

Ai sensi dell'art. 5 del Decreto, la responsabilità della Società può derivare dai reati commessi da:

1. SOGGETTI IN POSIZIONE APICALE

Sono tali le persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Società ovvero di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché coloro che esercitano, anche di fatto, la gestione o il controllo della Società.

2. SOGGETTI SOTTOPOSTI ALLA DIREZIONE O VIGILANZA

Rientrano in tale categoria i dipendenti, i collaboratori e tutti coloro che operano sotto la direzione o la vigilanza dei soggetti apicali.

4.5 ESCLUSIONE DELLA RESPONSABILITÀ DELL'ENTE

La Società non risponde dei reati commessi dai soggetti apicali qualora dimostri che, prima della commissione del fatto:

1. aveva adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi;
2. aveva affidato ad un Organismo di Vigilanza dotato di autonomi poteri di iniziativa e controllo il compito di vigilare sul funzionamento e sull'osservanza del Modello;
3. l'Organismo di Vigilanza ha esercitato efficacemente le proprie funzioni;
4. il reato è stato commesso eludendo fraudolentemente il Modello;
5. non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Per i reati commessi da soggetti sottoposti all'altrui direzione o vigilanza trovano applicazione i criteri previsti dall'art. 7 del Decreto.

4.6 I REATI PRESUPPOSTOPRINCIPALI INTERVENTI NORMATIVI DI AGGIORNAMENTO DEL CATALOGO DEI REATI PRESUPPOSTO

Successivamente all'entrata in vigore del D.Lgs. 8 giugno 2001, n. 231, il catalogo dei reati presupposto è stato progressivamente ampliato e modificato da numerosi interventi legislativi. Tra i principali si richiamano:

1. **Legge 16 marzo 2006, n. 146** – Introduzione della responsabilità degli enti per i reati transnazionali.
2. **D.Lgs. 8 novembre 2021, n. 184** – Introduzione dell'art. 25-octies.1 relativo ai delitti in materia di strumenti di pagamento diversi dai contanti.
3. **D.L. 10 marzo 2023, n. 20**, convertito con modificazioni – Modifiche ai reati in materia di immigrazione clandestina e di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25-duodecies).
4. **D.Lgs. 2 marzo 2023, n. 19** – Introduzione del reato di false o omesse dichiarazioni per il rilascio del certificato preliminare nelle operazioni transfrontaliere (art. 25-ter).
5. **D.L. 10 agosto 2023, n. 105**, convertito dalla **Legge 9 ottobre 2023, n. 137** – Introduzione dei delitti di turbata libertà degli incanti, turbata libertà del procedimento di scelta del contraente e trasferimento fraudolento di valori; modifiche ai reati ambientali e ai delitti in materia di strumenti di pagamento diversi dai contanti.
6. **Legge 14 luglio 2023, n. 93** – Aggiornamento della disciplina dei delitti in materia di violazione del diritto d'autore (art. 25-novies).
7. **Legge 27 dicembre 2023, n. 206** – Modifiche ai delitti contro l'industria e il commercio (art. 25-bis.1) nell'ambito della tutela del Made in Italy.
8. **Legge 22 gennaio 2024, n. 6** – Aggiornamento dei delitti contro il patrimonio culturale (art. 25-septiesdecies).
9. **D.Lgs. 14 giugno 2024, n. 87** – Revisione del sistema sanzionatorio tributario con modifiche ai reati tributari rilevanti ai sensi dell'art. 25-quinquiesdecies.
10. **Legge 28 giugno 2024, n. 90** – Rafforzamento della cybersicurezza nazionale e aggiornamento dei reati informatici e contro la Pubblica Amministrazione (artt. 24 e 24-bis).

11. **D.L. 4 luglio 2024, n. 92**, convertito dalla **Legge 8 agosto 2024, n. 112**, e **Legge 9 agosto 2024, n. 114** – Introduzione del delitto di indebita destinazione di denaro o cose mobili, abrogazione dell'abuso d'ufficio e conseguente aggiornamento dell'art. 25 del D.Lgs. 231/2001.
12. **D.Lgs. 26 settembre 2024, n. 141** – Riforma della disciplina del contrabbando con aggiornamento dell'art. 25-sexiesdecies del D.Lgs. 231/2001.
13. **D.L. 11 ottobre 2024, n. 145**, convertito dalla **Legge 9 dicembre 2024, n. 187** – Modifiche alla disciplina dell'immigrazione irregolare e dello sfruttamento del lavoro, con aggiornamento dell'art. 25-duodecies.
14. **Legge 6 giugno 2025, n. 82** – Introduzione del nuovo **art. 25-undevicies** del D.Lgs. 231/2001 relativo ai delitti contro gli animali e contestuale aggiornamento di alcune fattispecie ambientali.
15. **Legge 9 giugno 2025, n. 80**, di conversione del D.L. n. 48/2025 – Modifiche ai delitti con finalità di terrorismo (art. 25-quater) e ad alcune fattispecie di truffa rilevanti ai sensi dell'art. 24 del D.Lgs. 231/2001.
16. **D.L. 8 agosto 2025, n. 116**, convertito dalla **Legge 3 ottobre 2025, n. 147** – Ampia revisione della disciplina dei reati ambientali di cui all'art. 25-undecies, con introduzione di nuove fattispecie e modifica di quelle esistenti.
17. **Legge 23 settembre 2025, n. 132** – Disposizioni in materia di intelligenza artificiale con riflessi sui reati societari, sugli abusi di mercato e sui delitti in materia di diritto d'autore (artt. 25-ter, 25-sexies e 25-novies del D.Lgs. 231/2001).

4.7 LE SANZIONI PREVISTE DAL DECRETO

Il Decreto prevede, nei confronti dell'ente ritenuto responsabile, le seguenti tipologie di sanzioni:

1. sanzioni pecuniarie;
2. sanzioni interdittive;
3. confisca del prezzo o del profitto del reato;
4. pubblicazione della sentenza nei casi previsti dalla legge.

Le sanzioni sono applicate dal giudice tenendo conto della gravità del fatto, del grado di responsabilità dell'ente, dell'attività svolta per eliminare o attenuare le conseguenze del reato e delle misure organizzative adottate per prevenire ulteriori illeciti.

4.8 IL MODELLO QUALE STRUMENTO DI PREVENZIONE

Il presente Modello costituisce il principale strumento attraverso il quale IDRAGEST S.r.l. persegue la prevenzione dei reati previsti dal D.Lgs. 231/2001.

Esso si fonda sui seguenti principi:

1. individuazione delle attività e dei processi sensibili;
2. valutazione periodica dei rischi;
3. adozione di procedure e controlli preventivi;
4. chiara attribuzione di ruoli, responsabilità e poteri;
5. tracciabilità delle operazioni;
6. segregazione delle funzioni;
7. diffusione della cultura della legalità e dell'etica d'impresa;
8. formazione del personale;
9. monitoraggio continuo dell'efficacia del Modello;
10. costante aggiornamento del sistema di compliance aziendale.

5. LE AREE DI RISCHIO E LE PARTI SPECIALI DEL MODELLO

5.1 PREMESSA

L'attività di analisi dei rischi (Risk Assessment) costituisce il presupposto essenziale per la predisposizione del Modello di Organizzazione, Gestione e Controllo adottato da IDRAGEST S.r.l.

La Società ha individuato i processi aziendali nel cui ambito potrebbero astrattamente essere commessi i reati presupposto previsti dal D.Lgs. 231/2001 e ha definito, per ciascuna area di rischio, specifici protocolli organizzativi e misure di controllo finalizzati a prevenire tali eventi.

L'analisi dei rischi è effettuata tenendo conto:

1. delle attività concretamente svolte dalla Società;

2. dell'assetto organizzativo e del sistema delle deleghe;

3. delle modalità operative adottate;

4. dei rapporti con soggetti pubblici e privati;

5. delle risultanze delle attività di vigilanza dell'Organismo di Vigilanza;

6. delle evoluzioni normative e giurisprudenziali;

7. delle eventuali modifiche organizzative o dei processi aziendali.

L'attività di Risk Assessment è oggetto di periodico aggiornamento al fine di garantire il costante allineamento del Modello ai rischi effettivamente presenti nell'organizzazione.

5.2 LE PARTI SPECIALI DEL MODELLO

Il presente Modello è composto dalla Parte Generale e dalle Parti Speciali che disciplinano i processi aziendali maggiormente esposti al rischio di commissione dei reati presupposto.

Le Parti Speciali costituiscono parte integrante e sostanziale del Modello e definiscono, per ciascuna area sensibile:

1. i processi interessati;

2. i reati presupposto rilevanti;

3. le attività sensibili;

4. le condotte vietate;

5. gli obblighi di comportamento;

6. i controlli preventivi;

7. i flussi informativi verso l'Organismo di Vigilanza;

8. la documentazione da conservare;

9. le responsabilità delle funzioni aziendali coinvolte.

Le disposizioni contenute nelle Parti Speciali integrano quelle della presente Parte Generale e devono essere osservate da tutti i Destinatari del Modello.

5. 3 AREE DI RISCHIO SPECIFICHE DI IDRAGEST

A seguito dell'attività di Risk Assessment sono state individuate le principali aree di rischio della Società, riepilogate nella seguente tabella.

Area di rischio	Parte Speciale	Principali reati presupposto
Rapporti con la Pubblica Amministrazione e gestione delle gare	PMOG 01 – PMOG 04 – PMOG 12	Reati contro la Pubblica Amministrazione, turbata libertà degli incanti, frodi nelle pubbliche forniture, frode informatica
Bilancio, amministrazione e tesoreria	PMOG 02 – PMOG 03	Reati societari, reati tributari, riciclaggio, autoriciclaggio

Area di rischio	Parte Speciale	Principali reati presupposto
Gestione delle risorse umane	PMOG 05	Impiego di cittadini di Paesi terzi irregolari, corruzione, delitti contro la persona
Gestione dei contenziosi	PMOG 06	Corruzione, induzione indebita, dichiarazioni mendaci all'Autorità Giudiziaria
Comunicazioni esterne e rapporti con il mercato	PMOG 07	Reati societari, false comunicazioni sociali, abuso di informazioni
Sistemi informatici e sicurezza digitale	PMOG 08	Delitti informatici, trattamento illecito dei dati, danneggiamento di sistemi informatici
Tutela dell'ambiente	PMOG 09	Reati ambientali
Salute e sicurezza sul lavoro	PMOG 10	Omicidio colposo e lesioni colpose commessi con violazione della normativa antinfortunistica
Proprietà intellettuale e gestione delle opere dell'ingegno	PMOG 11	Violazione del diritto d'autore, utilizzo illecito di software, contraffazione
Gestione degli appalti e dei rapporti con partner e fornitori	PMOG 12	Corruzione, turbativa d'asta, frodi contrattuali, riciclaggio

La presente tabella ha finalità esclusivamente ricognitiva e di coordinamento. La disciplina di dettaglio è contenuta nelle rispettive Parti Speciali.

5.4 PRINCIPI GENERALI DI CONTROLLO

Le Parti Speciali sono fondate su un insieme di principi comuni di controllo che trovano applicazione in tutti i processi sensibili della Società.

In particolare, ogni attività aziendale deve essere svolta nel rispetto dei seguenti principi:

1. rispetto della normativa vigente e delle procedure aziendali;

2. chiara attribuzione di ruoli, responsabilità e poteri autorizzativi;

3. segregazione delle funzioni incompatibili;

4. tracciabilità e documentazione delle operazioni;

5. verificabilità delle attività svolte;

6. conservazione della documentazione rilevante;

7. utilizzo esclusivo di sistemi informatici autorizzati;

8. controllo degli accessi ai dati e alle informazioni;

9. gestione trasparente dei rapporti con soggetti pubblici e privati;

10. tempestiva segnalazione di anomalie o violazioni.

Tali principi rappresentano i criteri generali cui devono conformarsi tutti i protocolli organizzativi previsti dalle Parti Speciali.

5.5 AGGIORNAMENTO DELL'ANALISI DEI RISCHI

L'analisi dei rischi è oggetto di riesame ogniqualvolta intervengano circostanze idonee ad incidere sull'efficacia del Modello.

Il riesame può essere determinato, a titolo esemplificativo, da:

1. modifiche dell'assetto organizzativo;

2. introduzione di nuovi processi aziendali;

3. avvio di nuove attività o linee di business;

4. modifiche normative rilevanti ai fini del D.Lgs. 231/2001;

5. commissione o tentata commissione di reati presupposto;

6. violazioni significative del Modello;

7. esiti delle attività di audit svolte dall'Organismo di Vigilanza;

8. segnalazioni ricevute, anche attraverso il sistema di whistleblowing, che evidenzino criticità del sistema di controllo interno.

Qualora emergano esigenze di aggiornamento del Modello, l'Organismo di Vigilanza ne informa il Consiglio di Amministrazione, formulando le opportune proposte di revisione. L'approvazione delle modifiche al Modello resta di esclusiva competenza del Consiglio di Amministrazione.

6. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI IDRAGEST S.R.L.

6.1 FINALITÀ DEL MODELLO

Il presente Modello di Organizzazione, Gestione e Controllo (di seguito, anche il "Modello") è adottato da IDRAGEST S.r.l. ai sensi degli articoli 6 e 7 del D.Lgs. 231/2001 quale strumento di prevenzione dei reati presupposto e quale elemento integrante del sistema di governo societario e di controllo interno.
L'adozione del Modello è finalizzata a perseguire i seguenti obiettivi:

1. prevenire il rischio di commissione dei reati previsti dal D.Lgs. 231/2001;

2. diffondere una cultura improntata alla legalità, alla trasparenza, all'etica e alla responsabilità;

3. rafforzare il sistema dei controlli interni;

4. assicurare una chiara attribuzione di ruoli, responsabilità e poteri;

5. garantire la tracciabilità delle attività aziendali;

6. promuovere comportamenti conformi al Codice Etico e alle procedure aziendali;

7. tutelare il patrimonio, la reputazione e l'affidabilità della Società;

8. favorire il miglioramento continuo del sistema di compliance.

6.2 PRINCIPI ISPIRATORI

Il Modello è predisposto nel rispetto dei principi elaborati dalla giurisprudenza, delle Linee Guida di Confindustria e delle migliori prassi nazionali in materia di responsabilità amministrativa degli enti.
Esso si fonda sui seguenti principi:

1. legalità;

2. correttezza;

3. trasparenza;

4. responsabilità;

5. segregazione delle funzioni;

6. tracciabilità delle operazioni;

7. proporzionalità dei controlli;

8. documentabilità dei processi decisionali;

9. gestione del rischio secondo un approccio basato sul Risk Assessment;

10. miglioramento continuo del sistema dei controlli.

6.3 STRUTTURA DEL MODELLO

Il Modello adottato da IDRAGEST S.r.l. è costituito da un sistema organico di regole, procedure e controlli tra loro coordinati.

Esso si compone dei seguenti documenti:

1. Parte Generale;

2. Parti Speciali;

3. Codice Etico;

4. Sistema Disciplinare;

5. Procedura Whistleblowing;

6. Composizione Organismo di Vigilanza;

7. Elen dei reati presupposto;

8. Clausole contrattuali

9. ogni ulteriore documentazione richiamata dal Modello quale parte integrante del sistema di controllo interno.

Tutti i documenti sopra indicati costituiscono un sistema unitario di prevenzione e devono essere interpretati in modo coordinato.

6.4 DESTINATARI DEL MODELLO

Le disposizioni contenute nel presente Modello si applicano a tutti i Destinatari che operano nell'interesse o a vantaggio della Società.

Sono Destinatari del Modello:

1. i componenti del Consiglio di Amministrazione;

2. i dirigenti;

3. i dipendenti;

4. i collaboratori;

5. i consulenti;

6. i professionisti incaricati dalla Società;

7. gli agenti;

8. i partner commerciali;

9. i fornitori, nei limiti previsti dai rapporti contrattuali;

10. ogni altro soggetto che operi, anche temporaneamente, per conto o nell'interesse della Società.

I Destinatari sono tenuti a conoscere e rispettare le disposizioni del Modello, del Codice Etico e delle Procedure Speciali applicabili alle attività di rispettiva competenza.

6.5 OBBLIGHI DEI DESTINATARI

Ciascun Destinatario è tenuto a contribuire all'effettiva attuazione del Modello nell'ambito delle proprie funzioni e responsabilità.

In particolare, ciascun Destinatario deve:

1. osservare le disposizioni contenute nel Modello;

2. rispettare il Codice Etico;

3. applicare le Procedure Speciali di competenza;

4. operare nel rispetto della normativa vigente;

5. collaborare con l'Organismo di Vigilanza nell'esercizio delle sue funzioni;

6. trasmettere all'Organismo di Vigilanza i flussi informativi previsti dal Modello;

7. segnalare eventuali violazioni, anomalie o situazioni di rischio mediante i canali previsti dalla Società;

8. partecipare alle attività formative organizzate dalla Società;

9. adottare comportamenti improntati ai principi di correttezza, trasparenza e buona fede.

L'inosservanza degli obblighi previsti dal Modello comporta l'applicazione delle misure disciplinari previste dalla normativa vigente e dal Sistema Disciplinare aziendale.

6.6 DIFFUSIONE DEL MODELLO

La Società assicura la diffusione del Modello mediante strumenti idonei a garantirne la conoscibilità da parte dei Destinatari.

A tal fine provvede a:

1. mettere a disposizione la documentazione del Modello attraverso i canali aziendali individuati;

2. consegnare o rendere accessibili il Codice Etico e gli altri documenti applicabili;

3. assicurare la formazione del personale;

4. acquisire, ove previsto, le dichiarazioni di presa visione e di impegno al rispetto del Modello;

5. promuovere la diffusione della cultura della legalità e della compliance;

6. pubblicazione sul sito internet aziendale.

6.7 RAPPORTI CON IL SISTEMA AZIENDALE DI COMPLIANCE

Il Modello costituisce parte integrante del sistema di controllo interno della Società e opera in modo coordinato con gli altri strumenti organizzativi e di compliance adottati.

In particolare, esso si integra con:

1. il Codice Etico;

2. la Politica Anticorruzione;

3. la Policy per l'utilizzo dei sistemi di Intelligenza Artificiale;

4. la Politica per la Sicurezza delle Informazioni;

5. la procedura Whistleblowing;

6. il Sistema Disciplinare;

7. le Procedure Speciali del Modello;

8. le procedure operative aziendali;

9. il sistema delle deleghe e delle procure;

10. le eventuali certificazioni e sistemi di gestione adottati dalla Società.

Tutti gli strumenti sopra indicati concorrono, nell'ambito delle rispettive finalità, alla prevenzione dei rischi di non conformità e alla diffusione di una cultura aziendale improntata alla legalità, alla trasparenza e alla responsabilità.

7. L'ORGANISMO DI VIGILANZA

7.1 RUOLO E FUNZIONI

Ai sensi dell'art. 6 del D.Lgs. 231/2001, IDRAGEST S.r.l. ha istituito un Organismo di Vigilanza (di seguito anche "OdV"), dotato di autonomi poteri di iniziativa e controllo, cui è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello, verificarne l'efficacia nel tempo e promuoverne il costante miglioramento.

L'Organismo di Vigilanza opera con autonomia, indipendenza, continuità d'azione e professionalità, nel rispetto delle disposizioni del Decreto, del presente Modello e del proprio Regolamento.

L'OdV non esercita funzioni gestionali né assume decisioni operative di competenza degli organi societari, limitandosi a svolgere attività di vigilanza, controllo, verifica e proposta.

7.2 NOMINA E COMPOSIZIONE

L'Organismo di Vigilanza è nominato dal Consiglio di Amministrazione, che ne determina la composizione, la durata dell'incarico e il compenso.

La composizione dell'Organismo è individuata tenendo conto delle caratteristiche organizzative della Società e dell'esigenza di garantire adeguati requisiti di autonomia, indipendenza, professionalità, continuità d'azione e onorabilità.

I requisiti, le cause di ineleggibilità, decadenza, sospensione e revoca sono disciplinati dal Regolamento dell'Organismo di Vigilanza e dagli atti di nomina.

7.3 COMPITI DELL'ORGANISMO DI VIGILANZA

Nello svolgimento delle proprie funzioni l'Organismo di Vigilanza provvede, in particolare, a:

1. vigilare sull'effettiva attuazione del Modello da parte dei Destinatari;

2. verificare l'idoneità del Modello a prevenire i reati previsti dal D.Lgs. 231/2001;

3. monitorare l'efficacia delle Procedure Speciali e dei controlli preventivi;

4. predisporre ed attuare il piano annuale delle attività di vigilanza;

5. svolgere audit e verifiche sui processi sensibili individuati nel Modello;

6. acquisire e analizzare i flussi informativi previsti dal Modello;

7. ricevere ed esaminare le informazioni e le segnalazioni di propria competenza;

8. monitorare l'evoluzione normativa e giurisprudenziale rilevante ai fini del D.Lgs. 231/2001;

9. formulare al Consiglio di Amministrazione proposte motivate di aggiornamento del Modello quando ne ravvisi la necessità;

10. verificare l'attuazione delle azioni correttive conseguenti alle attività di vigilanza.

7.4 POTERI DELL'ORGANISMO DI VIGILANZA

Per l'espletamento delle proprie funzioni, l'Organismo di Vigilanza può:

1. accedere, senza limitazioni, alla documentazione aziendale rilevante ai fini del Modello;

2. richiedere informazioni, dati e chiarimenti alle funzioni aziendali;

3. effettuare verifiche documentali e ispettive;

4. promuovere incontri con le funzioni interessate;

5. avvalersi, previa autorizzazione del Consiglio di Amministrazione ove necessaria, del supporto di consulenti esterni per attività che richiedano specifiche competenze tecniche.

Tutte le funzioni aziendali sono tenute a prestare la massima collaborazione all'Organismo di Vigilanza nello svolgimento delle proprie attività.

7.5 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Le funzioni aziendali trasmettono all'Organismo di Vigilanza le informazioni previste dal Modello, dalle Procedure Speciali e dalle procedure interne.

Devono inoltre essere tempestivamente comunicate tutte le circostanze che possano incidere sull'efficacia del Modello, ivi comprese:

1. violazioni accertate o presunte del Modello;

2. procedimenti giudiziari o amministrativi rilevanti ai fini del D.Lgs. 231/2001;

3. provvedimenti adottati da Autorità competenti;

4. gravi anomalie riscontrate nello svolgimento dei processi sensibili;

5. violazioni del Codice Etico;

6. eventi che rendano necessario l'aggiornamento del Modello.

Le modalità operative di trasmissione dei flussi informativi sono disciplinate dalle Parti Speciali e dal Regolamento dell'Organismo di Vigilanza.

7.6 GESTIONE DELLE SEGNALAZIONI

L'Organismo di Vigilanza riceve le informazioni di propria competenza e valuta le segnalazioni concernenti presunte violazioni del Modello, del Codice Etico e delle Procedure Speciali.

Le segnalazioni effettuate mediante il sistema di whistleblowing sono gestite secondo la procedura adottata dalla Società in attuazione del D.Lgs. 24/2023.

L'Organismo di Vigilanza, nell'ambito delle proprie competenze:

1. valuta la rilevanza delle segnalazioni ricevute;

2. svolge gli approfondimenti ritenuti necessari;

3. richiede eventuali chiarimenti alle funzioni interessate;

4. propone, ove necessario, l'adozione di misure correttive;

5. informa il Consiglio di Amministrazione qualora emergano violazioni significative del Modello o fatti di particolare rilevanza.

Resta fermo il rispetto degli obblighi di riservatezza previsti dalla normativa vigente e dalla procedura whistleblowing.

7.7 REPORTING

L'Organismo di Vigilanza assicura un costante flusso informativo nei confronti del Consiglio di Amministrazione.

A tal fine:

1. redige una **Relazione Annuale** contenente l'attività svolta, gli audit effettuati, gli esiti delle verifiche, le eventuali criticità riscontrate, le segnalazioni rilevanti ricevute e le proposte di aggiornamento del Modello;

2. informa tempestivamente il Consiglio di Amministrazione qualora emergano violazioni significative del Modello, gravi carenze del sistema di controllo interno, novità normative che richiedano un aggiornamento del Modello ovvero fatti suscettibili di determinare la responsabilità amministrativa della Società.

L'Organismo di Vigilanza può inoltre formulare, in qualsiasi momento, osservazioni e raccomandazioni finalizzate al miglioramento del sistema di controllo interno.

7.8 CONSERVAZIONE DELLA DOCUMENTAZIONE

L'Organismo di Vigilanza conserva la documentazione relativa alle attività svolte in un archivio informatico riservato, accessibile esclusivamente ai componenti dell'Organismo e ai soggetti espressamente autorizzati.

Sono conservati, in particolare:

1. il piano annuale delle attività;

2. i verbali delle riunioni;

3. i verbali di audit;

4. la Relazione Annuale;

5. la documentazione acquisita nel corso delle verifiche;

6. i flussi informativi ricevuti;

7. la documentazione relativa alle attività di monitoraggio del Modello.

Le modalità di conservazione e i tempi di archiviazione sono disciplinati dal Regolamento dell'Organismo di Vigilanza e dalle procedure aziendali in materia di gestione documentale.

8 IL SISTEMA DI CONTROLLO INTERNO E I PROTOCOLLI DI PREVENZIONE

8.1 PRINCIPI GENERALI DEL SISTEMA DI CONTROLLO INTERNO

Il sistema di controllo interno adottato da IDRAGEST S.r.l. costituisce l'insieme dei presidi organizzativi, procedurali e gestionali finalizzati a garantire il corretto svolgimento delle attività aziendali, la tutela del patrimonio sociale, l'affidabilità delle informazioni, il rispetto della normativa vigente e la prevenzione dei reati previsti dal D.Lgs. 231/2001.

Il sistema di controllo interno è parte integrante del Modello e si fonda su un approccio di prevenzione del rischio basato sulla definizione di responsabilità, sulla tracciabilità delle attività e sulla verifica dell'efficacia dei controlli.

8.2 PRINCIPI DI CONTROLLO

Nello svolgimento delle attività aziendali devono essere osservati i seguenti principi generali di controllo:

1. rispetto della normativa vigente, del Codice Etico, del Modello e delle procedure aziendali;

2. chiara individuazione delle responsabilità e dei livelli autorizzativi;

3. separazione, ove possibile, tra le funzioni di autorizzazione, esecuzione, controllo e registrazione delle operazioni;

4. tracciabilità dell'intero processo decisionale e delle operazioni effettuate;

5. verificabilità delle attività svolte mediante adeguata documentazione;

6. conservazione della documentazione secondo le procedure aziendali;

7. utilizzo di sistemi informatici autorizzati e adeguatamente protetti;

8. monitoraggio periodico dei processi sensibili;

9. gestione tempestiva delle anomalie e delle non conformità;

10. adozione di misure correttive e di miglioramento continuo.

8.3 SISTEMA DELLE DELEGHE E DELLE PROCURE

La Società adotta un sistema di deleghe e procure coerente con la struttura organizzativa e con le responsabilità attribuite alle singole funzioni aziendali.

Le deleghe e le procure devono rispettare i seguenti principi:

1. essere conferite in forma scritta;

2. individuare chiaramente i poteri attribuiti e gli eventuali limiti di esercizio;

3. essere coerenti con le responsabilità organizzative attribuite al delegato;

4. essere portate a conoscenza dei soggetti interessati;

5. essere costantemente aggiornate in caso di modifiche organizzative.

Nessun soggetto può esercitare poteri non formalmente attribuiti ovvero eccedenti i limiti previsti dall'atto di conferimento.

8.4 TRACCIABILITÀ DELLE OPERAZIONI

Ogni attività rilevante ai fini del Modello deve essere adeguatamente documentata in modo da consentire la ricostruzione delle fasi del processo decisionale, delle responsabilità coinvolte e dei controlli effettuati.

La documentazione deve consentire di individuare:

1. il soggetto che ha avviato il procedimento;

2. il soggetto che ha autorizzato l'operazione;

3. il soggetto che ha eseguito l'attività;

4. gli eventuali controlli effettuati;

5. la documentazione a supporto delle decisioni adottate.

8.5 SEGREGAZIONE DELLE FUNZIONI

La Società adotta, compatibilmente con la propria struttura organizzativa, il principio della segregazione delle funzioni, volto ad evitare che un unico soggetto possa gestire autonomamente tutte le fasi di un medesimo processo.

A tal fine, ove possibile, sono mantenute distinte le attività di:

1. autorizzazione;

2. esecuzione;

3. controllo;

4. registrazione;

5. verifica finale.

Qualora, per esigenze organizzative, non sia possibile una completa segregazione delle funzioni, la Società adotta controlli compensativi idonei ad assicurare un adeguato livello di presidio del rischio.

8.6 PROCEDURE AZIENDALI E PARTI SPECIALI

Le Procedure Speciali costituiscono l'attuazione operativa dei principi contenuti nella presente Parte Generale.

Esse disciplinano, con riferimento ai singoli processi sensibili:

1. le attività da svolgere;

2. i soggetti responsabili;

3. i controlli preventivi;

4. i divieti di comportamento;

5. gli obblighi dei Destinatari;

6. i flussi informativi verso l'Organismo di Vigilanza;

7. la documentazione da predisporre e conservare.

Le Procedure Speciali devono essere applicate congiuntamente alla presente Parte Generale e al Codice Etico.

8.7 GESTIONE DELLE ANOMALIE

Qualora, nello svolgimento delle attività aziendali, siano riscontrate anomalie, violazioni procedurali o situazioni suscettibili di esporre la Società ai rischi previsti dal D.Lgs. 231/2001, i Destinatari sono tenuti ad attivare senza ritardo i canali informativi previsti dal Modello.

Le anomalie possono riguardare, a titolo esemplificativo:

1. inosservanza delle procedure aziendali;

2. violazioni del Codice Etico;

3. mancato rispetto dei livelli autorizzativi;

4. irregolarità documentali;

5. anomalie nei sistemi informatici;

6. conflitti di interesse non dichiarati;

7. richieste o comportamenti non conformi alla normativa vigente.

La gestione delle segnalazioni avviene secondo quanto previsto dal presente Modello e dalla procedura Whistleblowing.

8.8 RIESAME DEL SISTEMA DI CONTROLLO INTERNO

L'efficacia del sistema di controllo interno è oggetto di verifica continua mediante:

1. gli audit svolti dall'Organismo di Vigilanza;

2. il monitoraggio dei flussi informativi;

3. l'analisi delle segnalazioni ricevute;

4. la verifica dello stato di attuazione delle misure correttive;

5. il monitoraggio delle modifiche normative e organizzative;

6. il riesame periodico dei processi sensibili.

Gli esiti delle attività di verifica costituiscono elemento di valutazione ai fini dell'eventuale aggiornamento del Modello.

9. FLUSSI INFORMATIVI, SEGNALAZIONI, FORMAZIONE E DIFFUSIONE DEL MODELLO

9.1 PRINCIPI GENERALI

L'efficace attuazione del Modello richiede la costante circolazione delle informazioni rilevanti tra le funzioni aziendali, l'Organismo di Vigilanza e gli organi sociali.

A tal fine la Società assicura un sistema di comunicazione interno fondato sui principi di:

1. completezza delle informazioni;

2. tempestività delle comunicazioni;

3. tracciabilità dei flussi informativi;

4. riservatezza delle informazioni trattate;

5. collaborazione tra le funzioni aziendali e l'Organismo di Vigilanza.

9.2 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Le funzioni aziendali trasmettono all'Organismo di Vigilanza le informazioni previste dalla presente Parte Generale, dalle Parti Speciali e dalle procedure aziendali.

I flussi informativi possono essere:

1. Ordinari, quando previsti con periodicità definita dal Modello o dalle Procedure Speciali;

2. Straordinari, quando riguardano eventi o circostanze che possono incidere sull'efficacia del Modello o comportare un rischio di responsabilità ai sensi del D.Lgs. 231/2001.

9.3 FLUSSI INFORMATIVI STRAORDINARI

Devono essere comunicati senza ritardo all'Organismo di Vigilanza, a titolo esemplificativo:

1. violazioni accertate o presunte del Modello;

2. violazioni del Codice Etico;

3. anomalie significative riscontrate nello svolgimento dei processi sensibili;

4. provvedimenti dell'Autorità Giudiziaria o di altre Autorità competenti riguardanti la Società o i Destinatari, qualora rilevanti ai fini del D.Lgs. 231/2001;

5. avvio di procedimenti disciplinari per violazioni del Modello;

6. modifiche dell'assetto organizzativo che incidano sui processi sensibili;

7. conferimento, modifica o revoca di deleghe e procure rilevanti;

8. esiti di verifiche ispettive da cui emergano criticità significative;

9. situazioni di conflitto di interessi non precedentemente dichiarate;

10. ogni ulteriore circostanza che possa compromettere l'efficacia del sistema di controllo interno.

9.4 SISTEMA DI SEGNALAZIONE (WHISTLEBLOWING)

La Società ha adottato una specifica procedura per la gestione delle segnalazioni in conformità al D.Lgs. 10 marzo 2023, n. 24.

La procedura disciplina:

1. i soggetti legittimati ad effettuare segnalazioni;

2. i canali di segnalazione interni;

3. le modalità di gestione delle segnalazioni;

4. le garanzie di riservatezza;

5. le misure di protezione del segnalante;

6. il divieto di atti ritorsivi o discriminatori;

7. il trattamento dei dati personali.

Le segnalazioni sono gestite secondo quanto previsto dalla procedura Whistleblowing, che costituisce parte integrante del sistema di compliance della Società.

9.5 RAPPORTI TRA LA PROCEDURA WHISTLEBLOWING E L'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza riceve le informazioni di propria competenza derivanti dalle segnalazioni gestite secondo la procedura Whistleblowing.

Nel rispetto della normativa vigente e della riservatezza del segnalante, l'Organismo di Vigilanza:

1. valuta gli elementi rilevanti ai fini del Modello;

2. svolge gli approfondimenti di competenza;

3. verifica l'eventuale sussistenza di violazioni del Modello;

4. propone, ove necessario, interventi correttivi;

5. informa il Consiglio di Amministrazione qualora emergano violazioni significative del Modello o situazioni che richiedano l'adozione di misure organizzative.

L'Organismo di Vigilanza non sostituisce il soggetto competente alla gestione della procedura Whistleblowing, ma esercita le proprie funzioni nei limiti previsti dal Modello e dalla normativa vigente.

9.6 INFORMAZIONE E FORMAZIONE

La Società promuove la conoscenza del Modello attraverso un programma di informazione e formazione rivolto ai Destinatari.

Le attività formative sono programmate in relazione al ruolo ricoperto e al livello di esposizione ai rischi disciplinati dal D.Lgs. 231/2001.

In particolare, la formazione è finalizzata a:

1. diffondere la conoscenza del D.Lgs. 231/2001;

2. illustrare i principi del Codice Etico;

3. far conoscere la struttura del Modello;

4. approfondire le Procedure Speciali applicabili;

5. sensibilizzare il personale sui rischi connessi alle attività svolte;

6. illustrare il sistema disciplinare;

7. promuovere la cultura della legalità e della prevenzione.

La partecipazione alle iniziative formative costituisce adempimento dei doveri derivanti dal rapporto di lavoro o di collaborazione.

9.7 DIFFUSIONE DEL MODELLO

La Società garantisce la conoscibilità del Modello mediante adeguate forme di comunicazione interna.

A tal fine provvede a:

1. mettere a disposizione il Modello e i documenti ad esso collegati attraverso gli strumenti aziendali individuati;

2. informare il personale in occasione dell'adozione o dell'aggiornamento del Modello;

3. richiedere, ove previsto, la presa visione della documentazione aziendale;

4. promuovere iniziative di sensibilizzazione sui principi della compliance e dell'etica d'impresa.

9.8 CONSERVAZIONE DELLE EVIDENZE

Le evidenze relative alle attività di informazione, formazione e trasmissione dei flussi informativi sono conservate dalla Società secondo le procedure interne di gestione documentale.

La documentazione deve consentire di verificare:

1. l'avvenuta diffusione del Modello;

2. la partecipazione alle attività formative;

3. l'invio dei flussi informativi previsti;

4. l'attuazione delle eventuali misure correttive.

10. SISTEMA DISCIPLINARE

10.1 PRINCIPI GENERALI

Ai sensi degli articoli 6 e 7 del D.Lgs. 231/2001, l'efficace attuazione del Modello presuppone l'adozione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle disposizioni in esso contenute.

Il sistema disciplinare costituisce parte integrante del presente Modello ed è finalizzato ad assicurare l'effettività delle misure organizzative e di controllo adottate dalla Società.

L'applicazione delle misure disciplinari è autonoma rispetto all'eventuale instaurazione o definizione di procedimenti penali e prescinde dall'accertamento della responsabilità penale dell'autore della condotta.

10.2 FINALITÀ

Il sistema disciplinare è volto a:

1. garantire l'effettiva osservanza del Modello, del Codice Etico e delle Procedure Speciali;

2. prevenire comportamenti contrari ai principi di legalità, correttezza e trasparenza;

3. assicurare il rispetto delle procedure aziendali;

4. tutelare l'efficacia del sistema di controllo interno;

5. rafforzare la cultura della compliance e della responsabilità individuale.

10.3 VIOLAZIONI RILEVANTI

Costituisce violazione del Modello qualsiasi comportamento, attivo od omissivo, posto in essere in contrasto con le disposizioni contenute nella presente Parte Generale, nelle Parti Speciali, nel Codice Etico o nelle procedure aziendali richiamate dal Modello.

A titolo esemplificativo, costituiscono violazioni:

1. l'inosservanza delle prescrizioni contenute nel Modello;

2. il mancato rispetto delle Procedure Speciali;

3. la violazione dei principi del Codice Etico;

4. l'omessa collaborazione con l'Organismo di Vigilanza;

5. l'omessa, incompleta o non veritiera trasmissione dei flussi informativi previsti dal Modello;

6. l'ostacolo all'attività di vigilanza dell'Organismo di Vigilanza;

7. la falsificazione o l'alterazione della documentazione rilevante ai fini del Modello;

8. l'adozione di comportamenti idonei ad eludere fraudolentemente il sistema dei controlli;

9. la violazione delle disposizioni in materia di whistleblowing, ivi compresi gli atti ritorsivi, le segnalazioni effettuate con dolo o colpa grave e la violazione degli obblighi di riservatezza;

10. ogni altro comportamento idoneo a compromettere l'efficacia del Modello.

10.4 DESTINATARI DELLE MISURE DISCIPLINARI

Le disposizioni del presente capitolo si applicano, nei limiti previsti dalla normativa vigente e dai rapporti giuridici instaurati con la Società, ai seguenti soggetti:

1. dipendenti;

2. dirigenti;

3. componenti del Consiglio di Amministrazione;

4. componenti del Collegio Sindacale, ove nominato;

5. collaboratori;

6. consulenti;

7. professionisti incaricati dalla Società;

8. fornitori;

9. partner commerciali;

10. ogni altro soggetto tenuto al rispetto del Modello.

10.5 MISURE NEI CONFRONTI DEI DIPENDENTI

Le violazioni commesse dai dipendenti sono sanzionate nel rispetto delle disposizioni del Codice Civile, dello Statuto dei Lavoratori, del contratto collettivo nazionale di lavoro applicato dalla Società e del Sistema Disciplinare aziendale.

La tipologia e la misura della sanzione sono determinate tenendo conto:

1. della gravità della violazione;

2. dell'intenzionalità della condotta;

3. del grado di negligenza o imprudenza;

4. delle conseguenze prodotte;

5. dell'eventuale reiterazione;

6. delle circostanze aggravanti o attenuanti.

10.6 MISURE NEI CONFRONTI DEGLI AMMINISTRATORI

Qualora emergano violazioni del Modello da parte dei componenti del Consiglio di Amministrazione o del Collegio Sindacale, ove nominato, l'Organismo di Vigilanza informa tempestivamente l'organo competente affinché siano assunte le determinazioni ritenute opportune ai sensi della legge e dello Statuto sociale.

Restano ferme le eventuali responsabilità civili, penali e amministrative previste dall'ordinamento.

10.7 MISURE NEI CONFRONTI DI CONSULENTI, FORNITORI E PARTNER

La violazione delle disposizioni del Modello da parte di consulenti, collaboratori, fornitori, partner commerciali o altri soggetti terzi può costituire inadempimento contrattuale.

Nei casi più gravi, la Società può adottare le misure previste dai contratti applicabili, ivi compresa la risoluzione del rapporto, fatto salvo il risarcimento dell'eventuale danno subito.

10.8 RAPPORTI CON L'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza non esercita poteri disciplinari.

Qualora, nello svolgimento delle proprie attività, accerti fatti suscettibili di rilevanza disciplinare, ne informa tempestivamente il Consiglio di Amministrazione affinché siano avviate le valutazioni e i procedimenti di competenza.

L'Organismo di Vigilanza monitora l'attuazione delle misure eventualmente adottate, limitatamente ai profili rilevanti ai fini dell'efficacia del Modello.

11. AGGIORNAMENTO E MIGLIORAMENTO CONTINUO DEL MODELLO

11.1 PRINCIPI GENERALI

Il Modello di Organizzazione, Gestione e Controllo costituisce uno strumento dinamico di prevenzione dei reati e di governo dei rischi aziendali.

Al fine di garantirne l'idoneità e l'efficacia nel tempo, il Modello è sottoposto a periodico riesame e aggiornamento, in relazione all'evoluzione della normativa, dell'organizzazione aziendale e dei rischi cui la Società risulta esposta.

L'aggiornamento del Modello costituisce parte integrante del sistema di miglioramento continuo adottato dalla Società.

11.2 COMPETENZA ALL'AGGIORNAMENTO

L'adozione, la modifica e l'aggiornamento del Modello competono esclusivamente al Consiglio di Amministrazione.

Il Consiglio di Amministrazione delibera gli aggiornamenti sulla base delle valutazioni effettuate e delle proposte formulate dalle funzioni competenti, ivi compreso l'Organismo di Vigilanza.

11.3 RUOLO DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza monitora costantemente l'idoneità del Modello rispetto ai rischi disciplinati dal D.Lgs. 231/2001.

Nell'ambito delle proprie competenze l'Organismo di Vigilanza:

1. verifica la persistente efficacia del Modello;

2. monitora l'evoluzione normativa e giurisprudenziale rilevante;

3. analizza gli esiti degli audit svolti;

4. valuta le informazioni ricevute mediante i flussi informativi;

5. esamina gli elementi rilevanti emersi nell'ambito delle segnalazioni ricevute, anche attraverso la procedura di whistleblowing;

6. propone al Consiglio di Amministrazione gli interventi ritenuti necessari per l'aggiornamento del Modello.

L'Organismo di Vigilanza non apporta direttamente modifiche al Modello, ma svolge funzioni di vigilanza, monitoraggio e proposta.

11.4 PRESUPPOSTI PER L'AGGIORNAMENTO DEL MODELLO

L'aggiornamento del Modello è valutato ogniqualvolta intervengano circostanze idonee ad incidere sulla sua efficacia.

A titolo esemplificativo, ciò può avvenire in caso di:

1. modifiche del D.Lgs. 231/2001 o della normativa ad esso collegata;

2. introduzione di nuove fattispecie di reato presupposto;

3. significative modifiche dell'assetto organizzativo della Società;

4. introduzione di nuovi processi aziendali o nuove attività;

5. modifiche del sistema delle deleghe e delle procure;

6. violazioni significative del Modello;

7. commissione o tentata commissione di reati rilevanti ai fini del D.Lgs. 231/2001;

8. esiti delle attività di audit che evidenzino carenze del sistema di controllo interno;

9. segnalazioni che evidenzino criticità organizzative o procedurali;

10. ulteriori circostanze che rendano necessario l'adeguamento del sistema di prevenzione.

11.5 RIESAME PERIODICO

L'Organismo di Vigilanza verifica periodicamente l'efficacia del Modello mediante le attività di vigilanza previste dal piano annuale.

Le risultanze delle attività di verifica confluiscono nella Relazione Annuale predisposta dall'Organismo di Vigilanza e costituiscono elemento di valutazione ai fini dell'eventuale aggiornamento del Modello.

Qualora l'Organismo di Vigilanza rilevi la necessità di procedere ad una revisione del Modello, trasmette al Consiglio di Amministrazione una relazione contenente le motivazioni della proposta e gli interventi ritenuti opportuni.

11.6 AGGIORNAMENTO DELLE PARTI SPECIALI

Le Parti Speciali sono aggiornate con le medesime modalità previste per il presente Modello.

Ogni modifica apportata alle Parti Speciali deve essere coordinata con la Parte Generale, il Codice Etico, il Sistema Disciplinare e gli altri documenti che compongono il sistema di compliance aziendale.

11.7 COMUNICAZIONE DEGLI AGGIORNAMENTI

Successivamente all'approvazione delle modifiche da parte del Consiglio di Amministrazione, la Società provvede a:

1. informare i Destinatari interessati;

2. aggiornare la documentazione aziendale;

3. rendere disponibili le nuove versioni del Modello;

4. organizzare, ove necessario, specifiche attività informative o formative;

5. conservare evidenza delle modifiche apportate e delle relative deliberazioni.

12. DISPOSIZIONI FINALI

12.1 ADOZIONE ED ENTRATA IN VIGORE

Il presente Modello di Organizzazione, Gestione e Controllo è adottato dal Consiglio di Amministrazione di IDRAGEST S.r.l. ai sensi del D.Lgs. 8 giugno 2001, n. 231 ed entra in vigore dalla data della relativa deliberazione.

Con l'adozione del presente Modello sono abrogate e sostituite le precedenti versioni, fatti salvi gli effetti degli atti e delle attività già validamente compiuti in applicazione delle stesse.

12.2 DIFFUSIONE E CONOSCIBILITÀ

La Società assicura la diffusione del Modello ai Destinatari mediante modalità idonee a garantirne la conoscibilità e l'effettiva applicazione.

Il Modello, unitamente ai documenti che ne costituiscono parte integrante, è reso disponibile secondo le modalità individuate dalla Società.

I Destinatari sono tenuti a conoscere e rispettare le disposizioni contenute nel Modello, nel Codice Etico, nelle Parti Speciali e negli altri documenti del sistema di compliance applicabili alle attività di rispettiva competenza.

12.3 COORDINAMENTO CON IL SISTEMA DI COMPLIANCE AZIENDALE

Il presente Modello costituisce parte integrante del sistema di controllo interno e di compliance della Società.

Esso deve essere interpretato e applicato in modo coordinato con:

1. il Codice Etico;

2. le Parti Speciali del Modello;

3. il Sistema Disciplinare;

4. la procedura Whistleblowing;

5. il Regolamento dell'Organismo di Vigilanza;

6. le procedure aziendali richiamate dal Modello;

7. il sistema delle deleghe e delle procure;

8. le ulteriori politiche e procedure aziendali rilevanti ai fini della prevenzione dei reati.

In caso di contrasto tra la presente Parte Generale e gli altri documenti del sistema di compliance, prevalgono le disposizioni di legge e le deliberazioni del Consiglio di Amministrazione, ferma restando la necessità di procedere al tempestivo coordinamento della documentazione aziendale.

12.4 RIESAME DOCUMENTALE

La Società assicura il costante aggiornamento della documentazione che compone il Modello.

Ogni revisione del presente documento è identificata mediante un numero di versione e una data di approvazione ed è accompagnata da un'apposita cronologia delle revisioni, nella quale sono riportate le principali modifiche intervenute.

La documentazione aggiornata è conservata secondo le procedure aziendali vigenti ed è resa disponibile ai Destinatari nelle modalità stabilite dalla Società.

13 IL CODICE ETICO

Il Codice Etico e il Modello sono due strumenti complementari e integrati.

Il Codice Etico è stato adottato in via autonoma da IDRAGEST con lo scopo di definire i principi di condotta degli affari della Societ,à nonchè gli impegni e le responsabilità dei propri collaboratori; inoltre, tale strumento fornisce agli stessi soggetti informazioni in ordine alla soluzione di problemi di natura etica e commerciale.

Il Modello risponde, invece, a specifiche prescrizioni contenute nel D.Lgs. 231/2001 finalizzate a prevenire la commissione di particolari tipologie di reati.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO 5

2 ACRONIMI AZIENDALI 6

3 RIFERIMENTI NORMATIVI 6

4 CAMPO DI APPLICAZIONE RESPONSABILE DELLA PROCEDURA 7

5 PROCESSI SENSIBILI E SOGGETTI DESTINATARI 8

5.1 PARTECIPAZIONE A GARE D'APPALTO E PROCEDURE DI AFFIDAMENTO.... 8

5.2 EROGAZIONE DI SERVIZI IT E SVILUPPO DI SOFTWARE PERSONALIZZATO PER LA P.A. 8

5.3 ATTIVITÀ DI RILIEVO TOPOGRAFICO E CAMPAGNA PER CONTO DELLA P.A. 8

5.4 CONSULENZA TECNICA E SUPPORTO ALLA REDAZIONE DI SPECIFICHE TECNICHE 9

5.5 SELEZIONE DI FORNITORI E SUBFORNITORI PER COMMESSE PUBBLICHE 9

5.6 ATTIVITÀ DI COLLAUDO DI SISTEMI E FORNITURE PER LA P.A..... 9

5.7 FORMAZIONE DEL PERSONALE DELLA CLIENTELA PUBBLICA 9

5.8 GESTIONE DI FINANZIAMENTI PUBBLICI E AGEVOLAZIONI PER L'INNOVAZIONE.....10

5.9 ADEMPIMENTI TRIBUTARI, PREVIDENZIALI E AUTORIZZATIVI.....10

6 reati contro la Pubblica Amministrazione 10

6.1 CRITERI PER LA DEFINIZIONE DI PUBBLICA AMMINISTRAZIONE E DI SOGGETTI INCARICATI DI UN PUBBLICO SERVIZIO.....11

6.2 Peculato (Art. 314 c.p.) e peculato mediante profitto dell'errore altrui (Art.316 c.p. modificato dal D.Lgs. n.75 del 14 luglio). 14

6.3 Malversazione di erogazioni pubbliche (Art. 316-bis c.p. modificato da D.L. n.13 del 25 febbraio 2022) 15

6.4 Indebita percezione di erogazioni pubbliche (Art. 640 modificato da D.Lgs.n.75 del 14 luglio 2020, dal D.Lgs. n. 150 del 10 Ottobre 2022, dalla Legge n.90 del 28 giugno 2024 e modificato dal D. L. n.48 dell'11 aprile 2025 e convertito dalla L. n.80 del 9 giugno 2025) 15

6.5 Truffa a danno dello Stato o di un altro ente pubblico o dell'Unione Europea (Art. 640 modificato dal D.Lgs.n.75 del 14 luglio 2020, dal D.Lgs. 150 del 10 Ottobre 2022 e dalla Legge n.90 del 28 giugno 2024 e convertito dalla L. n.80 del 9 giugno 2025) 16

6.6 Truffa aggravata per il conseguimento di erogazioni pubbliche (Art. 640 bis c.p. modificato da D.L. n.13 del 25 febbraio 2022) 17

6.7 Frode informatica in danno dello Stato o di altro Ente Pubblico (Art. 640-ter c.p.) 18

6.8 Concussione (Art. 317 c.p.) 19

6.9 Corruzione per un atto d'ufficio – Corruzione per un atto contrario ai doveri d'ufficio – Circostanze aggravanti-Induzione indebita a dare o promettere utilità-Corruzione di persona incaricata di pubblico servizio (Artt. 318 modificato da L.3 del 9 gennaio 2019, 319, 319-bis, e 320 c.p. modificati da L.69 del 27 maggio 2015 e 319-quater c.p. modificato dal D.Lgs. n. 75 del 14 luglio 2020). 20

7 PRINCIPI GENERALI DI COMPORTAMENTO 22

7.1 REGOLE SPECIFICHE DI CONDOTTA 23

8 PRINCIPI DI CONTROLLO 25

9 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO 26

9.2 SEGNALAZIONI IMMEDIATE 27

9.3 Archivio Digitale e Tracciabilità 27

9.4 Poteri di Controllo dell'OdV **28**

9.5 Sistema Sanzionatorio **28**

1 OBIETTIVI E FUNZIONI DEL MODELLO

Il D.Lgs. 8 giugno 2001, n. 231 ("Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica") ha introdotto nel nostro ordinamento la responsabilità amministrativa degli enti per reati commessi, nell'interesse o a vantaggio dell'ente stesso, da soggetti che rivestono posizione apicale ovvero da soggetti sottoposti alla direzione o vigilanza di questi ultimi.

Tra i reati presupposto rilevanti ai fini della predetta responsabilità, gli artt. 24 e 25 del D.Lgs. 231/01 includono un'ampia gamma di fattispecie commesse in danno della Pubblica Amministrazione o con il suo coinvolgimento: truffa, frode informatica, indebita percezione di erogazioni, corruzione nelle sue plurime declinazioni, concussione, malversazione.

LA PRESENTE PROCEDURA COSTITUISCE PARTE INTEGRANTE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (DI SEGUITO "MODELLO" O "MOG") DI IDRAGEST E HA LO SCOPO DI:

1. definire i principi di comportamento e i protocolli di controllo cui sono tenuti gli Organi Sociali, i dipendenti, i collaboratori, i consulenti e i partner di IDRAGEST che, nell'esercizio delle proprie funzioni, instaurano o gestiscono rapporti con la Pubblica Amministrazione;
2. identificare le aree e i processi sensibili in cui possono concretizzarsi i rischi di commissione dei reati di cui agli artt. 24 e 25 D.Lgs. 231/01, con particolare attenzione alle specificità operative di IDRAGEST (servizi informatici, sviluppo e gestione SIT, ingegneria e topografia per il rilievo di reti di fluidi, progettazione, consulenza tecnico-specialistica per la redazione di specifiche tecniche, selezione fornitori, collaudo e formazione);
3. garantire la tracciabilità delle attività svolte nei confronti della P.A. e la piena ricostruibilità delle decisioni adottate;
4. supportare l'Organismo di Vigilanza (OdV) nell'esercizio delle proprie funzioni di controllo e vigilanza sull'efficace attuazione del Modello.

La presente procedura è parte della Parte Speciale del Modello e deve essere letta in combinato disposto con la Parte Generale, con il Codice Etico e con le altre procedure operative adottate da IDRAGEST.

IDRAGEST si impegna al rispetto assoluto della legalità nei rapporti con la Pubblica Amministrazione, adottando una politica di tolleranza zero verso qualsiasi condotta, anche solo tentata, che possa integrare o favorire la commissione dei reati indicati nella presente procedura.

2 ACRONIMI AZIENDALI

CDA Consiglio di Amministrazione

PRES Presidente CDA

RSPP Responsabile del Servizio Prevenzione e Protezione

RSGQ Responsabile Sistema di Gestione Qualità

RTEC Responsabile Tecnico

RAM/RRU Responsabile Amministrazione - Risorse Umane

RCOM/APVG Responsabile Commerciale - Approvvigionamento

RFAM Responsabile Facility Management

RPROG Responsabile Progettazione

CDL Consulente del Lavoro

REC Responsabile Esterno Contabilità

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

La presente procedura è redatta in conformità e con riferimento alle seguenti fonti normative e documenti interni:

- **D.LGS. 8 GIUGNO 2001, N. 231** e successive modificazioni ed integrazioni: Disciplina della responsabilità amministrativa delle persone giuridiche;
- **CODICE PENALE**, con particolare riferimento agli artt. 314, 316, 316-bis, 316-ter, 317, 318, 319, 319-bis, 319-ter, 319-quater, 320, 322, 353, 353-bis, 357, 358, 640, 640-bis, 640-ter;
- **L. 9 GENNAIO 2019, N. 3 ("SPAZZACORROTTI"):** disposizioni per la lotta alla corruzione, e successive modificazioni;
- **L. 27 MAGGIO 2015, N. 69:** Disposizioni in materia di delitti contro la pubblica amministrazione;
- **L. 28 GIUGNO 2024, N. 90** ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici"): modifiche e integrazioni alle fattispecie di cui agli artt. 615-ter, 640-ter e connesse del

c.p., rilevanti per i reati informatici commessi ai danni della P.A. da parte di soggetti che operano nel settore dei servizi IT e SIT;

- **CODICE DEI CONTRATTI PUBBLICI (D.LGS. 31 MARZO 2023, N. 36):** disciplina delle procedure di affidamento di appalti e concessioni;
- **D.P.R. 28 DICEMBRE 2000, N. 445:** Testo unico in materia di documentazione amministrativa;
- **CODICE ETICO DI IDRAGEST**;
- **MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI IDRAGEST** (Parte Generale e restanti Procedure Speciali);
- **PROCEDURA "FLUSSI INFORMATIVI VERSO L'ODV** ex D.Lgs. 231/01" di IDRAGEST;
- **PROCEDURA DI GESTIONE DEL WHISTLEBLOWING DI IDRAGEST.**

4 CAMPO DI APPLICAZIONE RESPONSABILE DELLA PROCEDURA

Rientrano nel campo di applicazione della procedura tutti coloro (compresi i Responsabili di funzione ed i Consulenti esterni all'uopo incaricati) che entrano in contatto per qualsivoglia ragione con la Pubblica Amministrazione, anche nei casi di accertamenti, ispezioni e verifiche. Tra i Responsabili di funzione ed i Consulenti all'uopo incaricati, rientrano:

1. RSPP (consulente esterno all'uopo incaricato dalla Società) per quanto riguarda le verifiche in materia di igiene e sicurezza sui luoghi di lavoro;
2. il PRES, con il supporto del CDL, per quanto riguarda le verifiche in materia di lavoro e previdenza;
3. il PRES, con il supporto del REC, per quanto riguarda le verifiche di tipo fiscale e tributario;
4. il PRES, con il supporto del RAM/RRU e del RTEC, per verifiche in materia di gare.

In occasione delle ispezioni, i soggetti interessati possono avvalersi di professionisti esterni, scelti in relazione alla rilevanza e alle implicazioni giuridiche dell'ispezione, anche al fine di verificare la legittimità della stessa.

Resta inteso, che il responsabile della procedura è il PRES, il quale dovrà essere a conoscenza di tutti i procedimenti.

I relativi verbali dovranno essere sottoscritti dal Presidente o dal professionista e/o funzione all'uopo incaricato con apposita delega o autorizzazione scritta.

5 PROCESSI SENSIBILI E SOGGETTI DESTINATARI

Ai fini della presente procedura, sono identificati come processi sensibili — in quanto esposti al rischio di commissione dei reati di cui agli artt. 24 e 25 D.Lgs. 231/01 — i seguenti ambiti di attività:

5.1 PARTECIPAZIONE A GARE D'APPALTO E PROCEDURE DI AFFIDAMENTO

La partecipazione di IDRAGEST a procedure di gara (appalti pubblici, accordi quadro, manifestazioni di interesse, procedura negoziata) bandite da stazioni appaltanti pubbliche o da enti assimilati costituisce un'area ad alta sensibilità. Il rischio si concretizza principalmente nelle fasi di:

1. predisposizione e presentazione dell'offerta tecnica ed economica;
2. interlocuzioni con la commissione giudicatrice o con il RUP (Responsabile Unico del Procedimento);
3. redazione di documenti di gara (relazioni tecniche, curricula, dichiarazioni sostitutive).

5.2 EROGAZIONE DI SERVIZI IT E SVILUPPO DI SOFTWARE PERSONALIZZATO PER LA P.A.

Lo sviluppo, la personalizzazione, la manutenzione e la gestione di sistemi software destinati ad enti pubblici (inclusi SIT, piattaforme per la gestione di reti di fluidi, applicativi GIS) espone IDRAGEST a rischi specifici in materia di frode informatica (art. 640-ter c.p.) e accesso abusivo a sistemi informativi.

LA SENSIBILITÀ SI MANIFESTA NELLE FASI DI:

1. accesso a sistemi informativi e banche dati della P.A. in fase di sviluppo, test e manutenzione;
2. trattamento di dati geografici, cartografici e tecnici di proprietà dell'ente committente;
3. rilascio di aggiornamenti software e gestione di credenziali di accesso.

5.3 ATTIVITÀ DI RILIEVO TOPOGRAFICO E CAMPAGNA PER CONTO DELLA P.A.

L'esecuzione di rilievi sul campo (topografici, batimetrici, di tracciamento delle reti di fluidi), effettuati su incarico di enti pubblici o in aree demaniali/pubbliche, comporta interazione continuativa con tecnici e funzionari pubblici. **IL RISCHIO RIGUARDA:**

1. la veridicità dei dati e delle elaborazioni restituiti (bilanci idrici, cartografia, modelli);

2. il rischio che la relazione operativa con i referenti tecnici della P.A. diventi canale per utilità indebite.

5.4 CONSULENZA TECNICA E SUPPORTO ALLA REDAZIONE DI SPECIFICHE TECNICHE

L'attività di supporto a enti pubblici nella definizione di specifiche tecniche (capitolati, schemi di gara, standard di qualità), svolta in qualità di consulente tecnico-specialistico, espone al rischio di condizionamento delle procedure di acquisto successive, anche in via indiretta. Il rischio è elevato nelle situazioni in cui IDRAGEST redige o contribuisce a specifiche che poi confluiscono in gare a cui la stessa intende partecipare.

5.5 SELEZIONE DI FORNITORI E SUBFORNITORI PER COMMESSE PUBBLICHE

La selezione e la gestione di fornitori, subfornitori e partner tecnici chiamati a partecipare all'esecuzione di commesse pubbliche deve avvenire nel rispetto di criteri oggettivi e documentati. Il rischio riguarda l'eventualità che la selezione sia influenzata da pressioni esterne o da interessi di soggetti collegati alla P.A. committente.

5.6 ATTIVITÀ DI COLLAUDO DI SISTEMI E FORNITURE PER LA P.A.

Le attività di collaudo, verifica di conformità e accettazione di sistemi, apparecchiature o software commissionate da enti pubblici — svolte da IDRAGEST in qualità di collaudatore terzo o sub-collaudatore — sono aree sensibili perché:

1. il collaudatore interagisce direttamente con funzionari pubblici responsabili dell'accettazione;
2. esiste il rischio che l'esito del collaudo venga condizionato da vantaggi indebiti offerti dal fornitore o richiesti dal funzionario.

5.7 FORMAZIONE DEL PERSONALE DELLA CLIENTELA PUBBLICA

L'erogazione di servizi di formazione e affiancamento a personale di enti pubblici (sull'utilizzo di software, metodologie di rilievo, gestione SIT) comporta una relazione prolungata e diretta con

dipendenti e dirigenti della P.A. Il rischio si concretizza nella possibilità di scambi di vantaggi indebiti nell'ambito di tale relazione.

5.8 GESTIONE DI FINANZIAMENTI PUBBLICI E AGEVOLAZIONI PER L'INNOVAZIONE

La richiesta, la rendicontazione e la gestione di contributi pubblici, finanziamenti agevolati o incentivi (nazionali, regionali, europei) per lo sviluppo di soluzioni tecnologiche e informatiche costituisce un'area ad alta esposizione ai reati di indebita percezione, truffa e malversazione.

5.9 ADEMPIMENTI TRIBUTARI, PREVIDENZIALI E AUTORIZZATIVI

Gli adempimenti verso le Autorità fiscali, previdenziali e amministrative (richiesta di autorizzazioni, licenze, permessi), la gestione di ispezioni e le relazioni con funzionari competenti nelle materie di salute, sicurezza e igiene dei luoghi di lavoro, restano processi sensibili trasversali a tutta l'organizzazione.

6 REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

La presente Parte Speciale ha lo scopo di:

- Indicare le procedure che i Dipendenti, gli Organi Sociali, i Collaboratori esterni e i Partner della Società sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- Fornire all'organismo di Vigilanza e ai responsabili delle altre funzioni aziendali che cooperano con esso, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

In particolare, lo scopo della presente procedura speciale è quello di stabilire i principi e le regole finalizzare a prevenire i reati connessi al Decreto ed eventualmente integrandoli a quelli previsti nel Codice Etico e nelle procedure aziendali interne attualmente in vigore, quali individuati nella Parte Generale del Modello.

In via generale, a tutto il personale dell'azienda:

- È fatto obbligo di rispettare le regole, i principi e le procedure aziendali previste nel Modello e nei documenti interni della Società richiamati nel Modello;
- È fatto divieto di:
  - Porre in essere, dare causa o concorrere alla realizzazione di comportamenti che possano integrare, direttamente o indirettamente, qualsiasi fattispecie di reato disciplinata nella legislazione tempo per tempo vigente e, in particolare, i reati di cui al Decreto;

o Violare in tutto o in parte le regole, i principi e le procedure aziendali previste nel Modello e nei documenti interni della società richiamati nel Modello e nei quali il medesimo si articola La violazione delle norme aziendali e, in particolare, di quelle richiamate nel presente documento, comporta l'applicazione del sistema disciplinare illustrato nella Parte Generale.

6.1 CRITERI PER LA DEFINIZIONE DI PUBBLICA AMMINISTRAZIONE E DI SOGGETTI INCARICATI DI UN PUBBLICO SERVIZIO

Obiettivo del presente capitolo è quello di indicare dei criteri generali e fornire un elenco esemplificativo di quei soggetti qualificati come "soggetti attivi" nei reati rilevanti ai fini del Decreto.

ENTI DELLA PUBBLICA AMMINISTRAZIONE

Agli effetti della legge penale, viene comunemente considerato come "Ente della pubblica amministrazione" qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.

Sebbene non esista nel Codice penale una definizione di pubblica amministrazione, in base a quanto stabilito nella Relazione Ministeriale al codice stesso ed in relazione ai reati in esso previsti, sono ritenuti appartenere alla pubblica amministrazione quegli enti che svolgano "tutte le attività dello Stato e degli altri enti pubblici".

Nel tentativo di formulare una preliminare classificazione di soggetti giuridici appartenenti a tale categoria è possibile richiamare, da ultimo, l'art. 1, comma 2, D.Lgs.n.165/2001 in tema di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, il quale definisce come amministrazioni pubbliche tutte le amministrazioni dello Stato.

A titolo esemplificativo, si possono indicare quali soggetti della pubblica amministrazione, i seguenti enti o categorie di enti:

Istituti e scuole di ogni ordine e grado e le istituzioni educative	=
Enti ed amministrazioni dello Stato ad ordinamento autonomo	Ministeri - Camera e Senato - Dipartimento Politiche Comunitarie -Autorità Garante della Concorrenza e del Mercato - Autorità per l'Energia Elettrica ed il Gas - Autorità per le Garanzie nelle Comunicazioni - Banca d'Italia – Consob - Autorità Garante per la protezione dei dati personali - Agenzia delle Entrate – ISVAP - COVIP
Regioni	=
Province	=
Comuni	=
Comunità montane e loro consorzi ed associazioni	=
Camere di Commercio, Industria, Artigianato e Agricoltura e loro associazioni	=
Tutti gli enti pubblici non economici nazionali, regionali e locali	INPS – CNR – INAIL – INPDAI - ISTAT – ENASARCO – ASL - Enti e Monopoli di Stato - RAI
Unione europea e Stati esteri	=

Ferma restando la natura puramente esemplificativa degli enti pubblici sopra elencati, si evidenzia come non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose previste dal Decreto.
In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali¨ e degli "Incaricati di Pubblico Servizio.

PUBBLICI UFFICIALI

Ai sensi dell'Art. 357, primo comma, Codice penale, è considerato pubblico ufficiale agli effetti della legge penale "*colui il quale esercita una pubblica funzione legislativa, giudiziaria o amministrativa*".

Il secondo comma si preoccupa poi di definire la nozione di "pubblica funzione amministrativa". Non si è compiuta invece un'analoga attività definitoria per precisare la nozione di funzione legislativa e funzione giudiziaria in quanto la individuazione dei soggetti che rispettivamente le esercitano non ha di solito dato luogo a particolari problemi o difficoltà.
Pertanto, il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale "*è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*".
Tale ultima definizione normativa individua, innanzitutto, la delimitazione "esterna" della funzione amministrativa. Tale delimitazione è attuata mediante il ricorso a un criterio formale che fa riferimento alla natura della disciplina, per cui è definita pubblica la funzione amministrativa disciplinata da "norme di diritto pubblico", ossia da quelle norme volte al perseguimento di uno scopo pubblico ed alla tutela di un interesse pubblico e, come tali, contrapposte alle norme di diritto privato.
Il secondo comma dell'Art. 357 c.p. traduce poi in termini normativi alcuni dei principali criteri di massima individuati dalla giurisprudenza e dalla dottrina per differenziare la nozione di "pubblica funzione" da quella di "servizio pubblico" .
Vengono quindi pacificamente definite come "funzioni pubbliche" quelle attività amministrative che rispettivamente ed alternativamente costituiscono esercizio di:

- Poteri deliberativi
- Poteri autoritativi
- Poteri certificativi

Alla luce dei principi sopra enunciati, si può affermare che la categoria di soggetti più problematica è certamente quella che ricopre una "pubblica funzione amministrativa"

Per fornire un contributo pratico alla risoluzione di eventuali "casi dubbi", può essere utile ricordare che assumono la qualifica di pubblici ufficiali non solo i soggetti al vertice politico amministrativo dello Stato o di enti territoriali, ma anche – sempre riferendoci ad un'attività di altro ente pubblico retta da norme pubblicistiche – tutti coloro che, in base allo statuto nonché alle deleghe che esso consenta, ne formano legittimamente la volontà e/o la portino all'esterno in forza di un potere di rappresentanza.

INCARICATI DI UN PUBBLICO SERVIZIO

La definizione della categoria di "soggetti incaricati di un pubblico servizio" si rinviene all'Art. 358 c. p. il quale recita che "*sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio*".

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

Il legislatore puntualizza la nozione di "pubblico servizio" attraverso due ordini di criteri, uno positivo ed uno negativo. Il "servizio", affinché possa definirsi pubblico, deve essere disciplinato – del pari alla "pubblica funzione" - da norme di diritto pubblico ma con la differenziazione relativa alla mancanza dei poteri di natura certificativa, autorizzativa e deliberativa propri della pubblica funzione.

Il legislatore ha inoltre precisato che non può mai costituire "servizio pubblico" lo svolgimento di "semplici mansioni di ordine" né la "prestazione di opera meramente materiale". Con riferimento alle attività che vengono svolte da soggetti privati in base ad un rapporto concessorio con un soggetto pubblico, si ritiene che ai fini della definizione come pubblico servizio dell'intera attività svolta nell'ambito di tale rapporto concessorio non è sufficiente l'esistenza di un atto autoritativo di investitura soggettiva del pubblico servizio, ma è necessario accertare se le singole attività che vengono in questione siano a loro volta soggette a una disciplina di tipo pubblicistico.

La giurisprudenza ha individuato la categoria degli incaricati di un pubblico servizio, ponendo l'accento sul carattere della strumentalità ed accessorietà delle attività rispetto a quella pubblica in senso stretto.

Essa ha quindi indicato una serie di "indici rivelatori" del carattere pubblicistico dell'ente, per i quali è emblematica la casistica in tema di società per azioni a partecipazione pubblica. In particolare, si fa riferimento ai seguenti indici:

- La sottoposizione ad un'attività di controllo e di indirizzo a fini sociali, nonché ad un potere di nomina e revoca degli amministratori da parte dello Stato o di altri enti pubblici
- La presenza di una convenzione e/o concessione con la pubblica amministrazione
- L'apporto finanziario da parte dello Stato
- L'immanenza dell'interesse pubblico in seno all'attività economica.

6.2 PECULATO (ART. 314 C.P.) E PECULATO MEDIANTE PROFITTO DELL'ERRORE ALTRUI (ART.316 C.P. MODIFICATO DAL D.LGS. N.75 DEL 14 LUGLIO).

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio che avendo per ragioni del suo ufficio o servizio il possesso o comunque la disponibilità di danaro o di altra cosa se ne appropria.

La pena prevista per tale reato dall'Art. 1. della legge n.69 del 27 maggio 2015 che ha modificato l'Art. 314 c.p., è la reclusione da quattro a dieci anni e sei mesi.

Si applica invece la pena della reclusione da sei mesi a tre anni quando il colpevole ha agito al solo scopo di fare uso momentaneo della cosa e questa viene immediatamente restituita.

Se poi il pubblico ufficiale o l'incaricato di un pubblico servizio, nell'esercizio delle funzioni o del servizio giovandosi dell'errore altrui riceve o ritiene indebitamente, per sé o per un terzo, denaro od altra utilità, è punito con la reclusione da sei mesi a tre anni incorrendo nell'Art.316 c.p.

La pena della reclusione da sei mesi a quattro anni si applica quando il fatto offende gli interessi finanziari dell'Unione e il danno o il profitto sono superiori a euro 100.000.

Sulla base di quanto sopra riportato, si potrebbe ritenere che l'elemento discriminante per indicare se un soggetto rivesta o meno la qualifica di "incaricato di un pubblico servizio" è rappresentato, non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

Tali fattispecie sono rilevanti per IDRAGEST nella misura in cui il privato (la Società o suoi incaricati) possa indurre o favorire condotte appropriative da parte del P.U. con cui si relaziona, ovvero possa essere parte di meccanismi che facilitano tali condotte in sede di esecuzione di commesse pubbliche o di gestione di procedure di rimborso/accredito.

6.3 MALVERSAZIONE DI EROGAZIONI PUBBLICHE (ART. 316-BIS C.P. MODIFICATO DA D.L. N.13 DEL 25 FEBBRAIO 2022)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi pubbliche, non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta). La pena prevista per il reato in oggetto è la reclusione da sei mesi a quattro anni.

Per i dipendenti il reato in oggetto potrà configurarsi nell'ipotesi in cui le sovvenzioni siano erogate a favore della azienda perché ne fruisca direttamente ovvero perché si faccia tramite della loro distribuzione ai privati destinatari dell'erogazione.

Tenuto conto che il momento in cui il reato viene consumato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

LA FATTISPECIE È PARTICOLARMENTE RILEVANTE PER IDRAGEST CON RIFERIMENTO:

1. alla gestione di finanziamenti pubblici ottenuti per lo sviluppo di soluzioni software, piattaforme SIT o sistemi di monitoraggio delle reti;
2. alla rendicontazione di spese nell'ambito di bandi europei o nazionali per l'innovazione tecnologica e la digitalizzazione dei servizi idrici.

6.4 INDEBITA PERCEZIONE DI EROGAZIONI PUBBLICHE (ART. 640 MODIFICATO DA D.LGS.N.75 DEL 14 LUGLIO 2020, DAL D.LGS. N. 150 DEL 10 OTTOBRE 2022, DALLA LEGGE N.90 DEL 28 GIUGNO 2024 E MODIFICATO DAL D. L. N.48 DELL'11 APRILE 2025 E CONVERTITO DALLA L. N.80 DEL 9 GIUGNO 2025)

Tale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute – si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni pubbliche.

In questo caso, contrariamente a quanto visto in merito al punto precedente (Art. 316-bis), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

Il reato in oggetto è punito con la reclusione da sei mesi a tre anni.

La legge n.3 del 9 gennaio 2019 ha aggiunto che la pena è della reclusione da uno a quattro anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso della sua qualità' o dei suoi poteri.

La pena della reclusione da sei mesi a quattro anni si applica quando il fatto offende gli interessi finanziari dell'Unione e il danno o il profitto sono superiori a euro 100.000.

Tuttavia, quando la somma indebitamente percepita è pari o inferiore a 3.999,96 euro, si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da 5.164 Euro a 25.822 Euro. Tale sanzione non può, comunque, superare il triplo del beneficio conseguito.

Il reato di cui all'art. 316-ter c.p. potrebbe configurarsi in capo alla società sotto forma di concorso nel reato. In particolare, eventuali comportamenti scorretti dell'azienda nel rilascio di garanzie fideiussorie necessarie per l'ottenimento di erogazioni pubbliche da parte di propri clienti garantiti possono integrare gli estremi di un concorso nel reato previsto dal Decreto.

La fattispecie si differenzia dalla Truffa aggravata per il mancato requisito dell'induzione in errore: è sufficiente che le dichiarazioni siano false o incomplete. È altamente rilevante per IDRAGEST in sede di partecipazione a bandi e di rendicontazione di contributi per la ricerca, lo sviluppo tecnologico e la digitalizzazione.

6.5 TRUFFA A DANNO DELLO STATO O DI UN ALTRO ENTE PUBBLICO O DELL'UNIONE EUROPEA (ART. 640 MODIFICATO DAL D.LGS.N.75 DEL 14 LUGLIO 2020, DAL D.LGS. 150 DEL 10 OTTOBRE 2022 E DALLA LEGGE N.90 DEL 28 GIUGNO 2024 E CONVERTITO DALLA L. N.80 DEL 9 GIUGNO 2025)

Tale ipotesi di reato si configura nel caso in cui, siano posti in essere degli artifici o raggiri tali da indurre in errore e procurare a sé o ad altri un ingiusto profitto con altrui danno.

La pena prevista è quella della reclusione da sei mesi a tre anni e della multa da 51 euro a 1.032 Euro.

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:

1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione Europea o col pretesto di far esonerare taluno dal servizio militare

2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità

2 bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5).

Con l'ultima modifica apportata dalla Legge n.90 del 28 Giugno 2024 è stato introdotto il comma 2-ter) con cui si è estesa la punibilità anche quando il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal secondo comma, a eccezione di quella di cui al numero 2-ter).

Con il D.L. n.48 dell'11 aprile 2025, convertito dalla legge n.80 del9 giugno 2025 è stato abrogato il punto 2-bis del comma II e contestualmente è stato aggiunto il comma II-bis

Tale novità, applica l'Art. 61 c. p. comma 5, ovvero è prevista la pena della reclusione ora aumentata da 2 a 6 anni e una sanzione pecuniaria da 700 a euro 3000, qualora taluno, approfittando di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa, pone in essere degli artifici o raggiri per indurre l'altra persona in errore.

Nella predisposizione di documenti o dati per la partecipazione a procedure di gara, la società fornisce alla Pubblica Amministrazione informazioni non veritiere o anche attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione

Nell'ambito delle attività di IDRAGEST, il rischio si concretizza in particolare con riferimento a: presentazione di relazioni tecniche, elaborati grafici o dati di rilievo non veritieri o alterati, al fine di

1. ottenere SAL (stati avanzamento lavori) o collaudi favorevoli;
2. dichiarazioni non veritiere in sede di gara (requisiti di qualificazione, referenze, risorse impiegate).

6.6 TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (ART. 640 BIS C.P. MODIFICATO DA D.L. N.13 DEL 25 FEBBRAIO 2022)

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa.

La pena prevista per il reato in oggetto è quella della reclusione della reclusione da due a sette anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati

ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

Per la configurazione della suddetta fattispecie di reato è necessario che la finalità deve consistere nell'ottenimento di un finanziamento o contributo pubblico.

La fattispecie è rilevante per IDRAGEST con riferimento alla presentazione di dichiarazioni o documentazione tecnica artefatta nell'ambito di domande di accesso a fondi strutturali europei, contributi PNRR o incentivi nazionali destinati alla digitalizzazione e all'innovazione.

6.7 FRODE INFORMATICA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ART. 640-TER C.P.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi Tale reato è punito con la reclusione da sei mesi a tre anni e con la multa da 51 a 1.032 euro ovvero, se il fatto è commesso a danno dello Stato o di un altro ente pubblico.

L'articolo 640-ter è stato modificato dal D.Lgs.n.184 dell'8 novembre 2021 e dal D.Lgs.n.150 del 10 ottobre 2022 per cui la pena è applicata la reclusione da uno a cinque anni e la multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.

Infine, se il fatto è commesso con furto o indebito utilizzo dell'identità digitale, in danno di uno o più soggetti, la pena è la reclusione da due a sei anni e la multa da 600 a 3000 Euro.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età.

In concreto, tale ipotesi di reato è configurabile qualora, una volta ottenuto un finanziamento, l'azienda violasse il sistema informatico della Pubblica Amministrazione al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

QUESTA FATTISPECIE ASSUME UNA RILEVANZA PRIORITARIA PER IDRAGEST IN RAGIONE DEL CARATTERE INFORMATICO DELLE SUE ATTIVITÀ CORE. I PROFILI DI RISCHIO SPECIFICI RIGUARDANO:

1. **ACCESSO A SISTEMI DELLA P.A.:** nell'ambito di attività di sviluppo, manutenzione o integrazione di software (SIT, applicativi gestionali di reti idriche), il personale IDRAGEST può avere accesso privilegiato a sistemi informativi di enti pubblici. L'utilizzo di tale accesso per finalità diverse da quelle contrattuali o l'acquisizione non autorizzata di dati costituisce potenziale frode informatica;
2. **MANIPOLAZIONE DI DATI TECNICI:** l'alterazione di dati geografici, topografici o di rilievo caricati su piattaforme SIT della P.A., al fine di conseguire vantaggi economici (es. far risultare completate attività non eseguite), integra la fattispecie in esame;
3. **UTILIZZO DI CREDENZIALI ALTRUI:** l'impiego di credenziali di accesso attribuite a funzionari pubblici, anche con il loro consenso per finalità non autorizzate, espone al rischio di responsabilità ai sensi dell'art. 640-ter c.p.

6.8 CONCUSSIONE (ART. 317 C.P.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della sua posizione, costringa taluno a procurare o a promettere a sé o ad altri denaro o altre utilità non dovutegli.

La pena prevista per tale reato dall'Art.3 della legge n.69 del 27 maggio 2015 che ha modificato l'Art. 317 c.p. è la reclusione da sei a dodici anni.

Questo reato è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal Decreto, o allorquando la società svolga attività di incaricato di pubblico servizio (ad es. quando svolge l'attività volta alla riscossione tributi).

Tale fattispecie di reato può configurarsi quando ad esempio un dipendente, nell'esercizio delle proprie funzioni nell'attività di riscossione dei tributi, costringe un soggetto a versare una somma maggiore rispetto al tributo dovuto, procurando un vantaggio all'azienda. Tuttavia, sembra più plausibile un'ipotesi di concorso in concussione; oppure quando si consideri il caso di una società che partecipi ad una gara pubblica. In questo caso è possibile che i funzionari pubblici pongano in essere dei comportamenti concussivi in danno di terzi, per avvantaggiare la società che in ipotesi potrebbe concorrere con i funzionari pubblici per trarne beneficio e aggiudicarsi la gara.

Per IDRAGEST, il rischio si configura nella posizione di soggetto privato che potrebbe subire condotte concussive da parte di funzionari pubblici nell'ambito di procedure di gara, ispezioni o nelle fasi di esecuzione di commesse. È obbligo dei destinatari della presente procedura segnalare immediatamente all'OdV e al PRES qualsiasi richiesta o pressione indebita proveniente da funzionari pubblici.

6.9 CORRUZIONE PER UN ATTO D'UFFICIO – CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI D'UFFICIO – CIRCOSTANZE AGGRAVANTI-INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ-CORRUZIONE DI PERSONA INCARICATA DI PUBBLICO SERVIZIO (ARTT. 318 MODIFICATO DA L.3 DEL 9 GENNAIO 2019, 319, 319-BIS, E 320 C.P. MODIFICATI DA L.69 DEL 27 MAGGIO 2015 E 319-QUATER C.P. MODIFICATO DAL D.LGS. N. 75 DEL 14 LUGLIO 2020).

ART.318 CORRUZIONE PER UN ATTO D'UFFICIO

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, riceve indebitamente per sé o per altri, denaro o altri vantaggi o ne accetta la promessa.
L'attività del pubblico ufficiale potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).
Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

ART.319 CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI D'UFFICIO

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, per omettere o ritardare un atto d'ufficio (determinando un vantaggio in favore dell'offerente), riceve indebitamente per sé o per altri, denaro o altri vantaggi o ne accetta la promessa.
La pena prevista per tale reato dall'Art.1 della legge n.69 del 27 maggio 2015 che ha modificato l'Art. 319 c.p. è la reclusione da sei a dieci anni.

ART.319-BIS CIRCOSTANZE AGGRAVANTI

La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

ART.319-QUATER INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale abusando dei suoi poteri induce taluno a dare o a promettere per sé o per altri, denaro o altre utilità.
La pena prevista per tale reato dall'Art.1 dal D.Lgs.n.75 del 14 luglio 2020 che ha modificato l'Art. 319-quater è la reclusione da sei a dieci anni e sei mesi

Chi dà o promette denaro o altre utilità è punito con la reclusione fino a tre anni, ovvero con la reclusione fino a quattro anni quando il fatto offende gli interessi finanziari dell'Unione Europea e il danno o il profitto sono superiori a euro 100.000.

Tale ipotesi di reato si configura quando un dirigente offre una somma di denaro ad un funzionario di un ufficio pubblico allo scopo di ottenere il rapido rilascio di un provvedimento amministrativo necessario per l'esercizio dell'attività della società.

ART.320 CORRUZIONE DI PERSONA INCARICATA DI UN PUBBLICO SERVIZIO

Le disposizioni degli artt. 318 e 319 si applicano anche all'incaricato di un pubblico servizio.

L'art. 165 del codice penale, in materia di sospensione condizionale della pena prevede che: "*Nei casi di condanna per i reati previsti dagli articoli 314, 317, 318, 319, 319-ter, 319-quater, 320 e 322-bis, la sospensione condizionale della pena è comunque subordinata al pagamento di una somma equivalente al profitto del reato ovvero all'ammontare di quanto indebitamente percepito dal pubblico ufficiale o dall'incaricato di un pubblico servizio, a titolo di riparazione pecuniaria in favore dell'amministrazione lesa dalla condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio, ovvero, nel caso di cui all'articolo 319-ter, in favore dell'amministrazione della giustizia, fermo restando il diritto all'ulteriore eventuale risarcimento del danno*".

ART. 319-TER C.P. CORRUZIONE IN ATTI GIUDIZIARI

Tale ipotesi di reato si configura nel caso in cui la società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere o altro funzionario) per ottenere un vantaggio. Ad esempio, un soggetto apicale corrompa un cancelliere ad accettare fuori termine il deposito di memorie o altri scritti difensivi.

ART. 322 C.P. ISTIGAZIONE ALLA CORRUZIONE

Tale ipotesi di reato rappresenta una "forma anticipata" del reato di corruzione. In particolare, il reato di istigazione alla corruzione si configura tutte le volte in cui, in presenza di un comportamento finalizzato alla commissione di un reato di corruzione, questa non si perfezioni in quanto il pubblico ufficiale rifiuta l'offerta o la promessa non dovuta e illecitamente avanzatagli per indurlo a compiere ovvero ad omettere o ritardare un atto del suo ufficio.

*

In ordine alla gestione ed alle attività poste in essere da IDRAGEST per prevenire la commissioni dei reati di corruzione, si precisa che la società ha dedicato una specifica procedura

in materia e precisamente la PMOG15 e ciò in quanto la stessa assicura il proprio impegno a prevenire e contrastare il rischio di corruzione.

**

7 PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti divieti di carattere generale si applicano agli organi sociali, ai dirigenti e ai dipendenti di IDRAGEST in via diretta mentre ai consulenti, ai fornitori e ai partner in forza di apposite ed eventuali clausole contrattuali.

Ai suddetti soggetti è fatto divieto di porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (artt. 24 e 25 del D.Lgs. 231/2001); sono altresì proibite le violazioni ai principi ed alle procedure aziendali indicate nella presente procedura.

Conformemente a quanto previsto nel Codice Etico, nelle procedure e nelle norme aziendali, ai soggetti sopra individuati è fatto divieto di:

a) effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;

b) promettere o versare somme o beni in natura a qualsiasi soggetto (sia esso un dirigente, funzionario o dipendente della Pubblica Amministrazione o un soggetto privato) per promuovere o favorire gli interessi della Società anche a seguito di illecite pressioni. Sono consentiti omaggi e cortesie di uso commerciale di modesto valore seguendo il protocollo previsto nella procedura 09 "Scelta Omaggi";

c) ricorrere a forme diverse di aiuti o contribuzioni che, sotto veste di sponsorizzazioni, incarichi, consulenze o pubblicità abbiano invece le stesse finalità sopra vietate;

d) accordare vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione italiana o straniera che possano determinare le stesse conseguenze previste al precedente punto b);

e) selezionare personale ovvero favorire l'avanzamento interno di carriera o il riconoscimento di premi per il raggiungimento di obiettivi a beneficio di taluni dipendenti, non ispirandosi a criteri strettamente meritocratici o in base a criteri di valutazione non oggettivi;

f) assumere personale gradito a pubblici ufficiali, a meno che la selezione non abbia seguito un processo ispirato a criteri di valutazione oggettivi e rigorosamente meritocratici;

g) effettuare prestazioni in favore dei consulenti e dei partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;

h) assegnare incarichi di fornitura a persone o società vicine o gradite a soggetti pubblici in assenza dei necessari requisiti di qualità, sicurezza e convenienza dell'operazione di acquisto;

i) creare fondi a fronte di beni/servizi contrattualizzati a prezzi superiori a quelli di mercato oppure di fatturazioni inesistenti in tutto o in parte;

j) assegnare incarichi o negoziare condizioni contrattuali con controparti vicine / gradite a soggetti pubblici o legate a dipendenti o collaboratori della Società da interessi personali, in assenza di riconosciuti requisiti di qualità e convenienza economica dell'operazione

k) riconoscere compensi in favore di consulenti, agenti o intermediari che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale;

l) presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;

m) destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati;

n) alterare e/o utilizzare abusivamente e in modo improprio i sistemi informatici aziendali;

o) utilizzare un finanziamento pubblico per scopi diversi da quelli per i quali lo stesso è stato erogato (ad esempio, fondi ricevuti per scopi di formazione del personale dipendente vengono utilizzati per coprire le spese di corsi già effettuati autonomamente dalla società).

p) nella predisposizione di documenti o dati per la partecipazione a procedure di gara, la società fornire alla Pubblica Amministrazione informazioni non veritiere o anche attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione;

q) offrire una somma di denaro ad un funzionario di un ufficio pubblico allo scopo di ottenere il rapido rilascio di un provvedimento amministrativo necessario per l'esercizio dell'attività della società.

7.1 REGOLE SPECIFICHE DI CONDOTTA

È FATTO DIVIETO A TUTTI I DESTINATARI DELLA PRESENTE PROCEDURA DI:

a) offrire, promettere, corrispondere o far corrispondere — direttamente o indirettamente, anche tramite terzi, intermediari, consulenti o partner — denaro, regali, omaggi, servizi, utilità di qualsiasi natura a funzionari pubblici, dipendenti di enti pubblici, componenti di commissioni di gara, collaudatori, direttori dell'esecuzione del contratto o a loro familiari conviventi, al fine di ottenere un vantaggio per IDRAGEST;

b) promettere o fare promettere assunzioni, collaborazioni, incarichi, forniture o qualsiasi altro vantaggio economico a soggetti collegati a funzionari pubblici, anche in forma mediata, in cambio di condotte favorevoli;

c) elargire omaggi, liberalità o sponsorizzazioni a P.U. o I.P.S. che eccedano i limiti di modico valore stabiliti dal Codice Etico di IDRAGEST, ovvero che siano effettuati al di fuori dei canali e delle modalità approvate dalla procedura specifica sugli omaggi;

d) presentare, nell'ambito di procedure di gara, di richieste di finanziamento o di rendicontazioni a enti pubblici, documenti, dichiarazioni, relazioni tecniche, certificati o dati che contengano informazioni non veritiere, incomplete o fuorvianti, anche se la falsità è parziale o riguarda elementi apparentemente secondari dell'offerta o della rendicontazione;

e) utilizzare sistemi informatici o telematici della P.A. per finalità diverse da quelle contrattuali autorizzate, accedere a dati o sezioni di sistema non contemplati dal contratto, o consentire a terzi l'utilizzo delle credenziali di accesso assegnate a IDRAGEST;

f) alterare, modificare o manipolare dati geografici, topografici, cartografici o tecnici di qualsiasi natura caricati o trattati su piattaforme SIT o altri sistemi informativi di enti pubblici, anche in presenza di un'istruzione in tal senso proveniente dal committente;

g) redigere specifiche tecniche per conto di un ente pubblico committente in modo tale da favorire artificiosamente IDRAGEST stessa o soggetti a essa correlati nelle successive procedure di gara;

h) partecipare a intese, accordi collusivi o qualsiasi forma di coordinamento con concorrenti in sede di gara, finalizzati a limitare la concorrenza o a determinare artificiosamente l'esito della procedura;

i) corrispondere compensi, onorari o rimborsi spese a consulenti, intermediari o agenti in misura non proporzionata alle prestazioni effettivamente rese, o in assenza di un incarico formalmente documentato, nei casi in cui tali erogazioni possano celare accordi con funzionari pubblici;

l) omettere di dichiarare, in sede di partecipazione a gara o di stipula di contratti con enti pubblici, l'esistenza di situazioni di conflitto di interessi, di rapporti di parentela o affinità con funzionari dell'ente, ovvero di qualsiasi altra circostanza idonea a influenzare la correttezza della procedura;

m) versare somme o corrispondere utilità a soggetti pubblici con la motivazione di accelerare il rilascio di autorizzazioni, concessioni, licenze o permessi, anche qualora il pagamento sia richiesto dall'interlocutore pubblico o sia usuale nel contesto;

n) effettuare pagamenti in contanti o attraverso canali non tracciabili nell'ambito di rapporti con la P.A. o nell'esecuzione di commesse pubbliche;

o) porre in essere qualsivoglia altra condotta che, ancorché non specificamente vietata dai punti precedenti, sia idonea a integrare o a favorire la commissione dei reati di cui agli artt. 24 e 25 D.Lgs. 231/01 come descritti nella presente procedura.

8 PRINCIPI DI CONTROLLO

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

• LIVELLI AUTORIZZATIVI DEFINITI. IN PARTICOLARE:

o i soggetti che esercitano poteri autorizzativi e/o negoziali nei confronti della Pubblica Amministrazione:

▪ sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal responsabile all'uopo delegato o autorizzato;

▪ operano esclusivamente nell'ambito del perimetro di clientela loro assegnato;

o gli atti che impegnano contrattualmente IDRAGEST devono essere sottoscritti soltanto da soggetti appositamente incaricati;

o il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale per natura di spesa ed impegno, ivi incluse quelle nei confronti della Pubblica Amministrazione; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri.

• SEGREGAZIONE DEI COMPITI TRA I SOGGETTI COINVOLTI NEL PROCESSO DI DEFINIZIONE DELL'ACCORDO CONTRATTUALE CON GLI ENTI PUBBLICI. IN PARTICOLARE:

o le attività di sviluppo commerciale sono svolte principalmente dal RCOM e APVG;

o la definizione dell'accordo è affidata al responsabile al PRES in virtù dell'oggetto del contratto; l'atto formale della stipula del contratto avviene in base al vigente sistema dei poteri e delle deleghe e/o di apposite autorizzazioni scritte;

o i soggetti deputati alla predisposizione della documentazione per la presentazione dell'offerta tecnica ed economica, ovvero per la partecipazione a bandi di gara pubblica, possono essere differenti da coloro che sottoscrivono la stessa.

• ATTIVITÀ DI CONTROLLO:

o la documentazione relativa alla stipula dei rapporti contrattuali è sottoposta per il controllo al PRES che la sottoscrive;

o tutta la documentazione predisposta da IDRAGEST per l'accesso a bandi di gara pubblici deve essere verificata, in termini di veridicità e congruità sostanziale e formale, dal responsabile aziendale competente in virtù dell'oggetto del contratto o da soggetti a ciò facoltizzati.

• TRACCIABILITÀ DEL PROCESSO SIA A LIVELLO DI SISTEMA INFORMATIVO SIA IN TERMINI DOCUMENTALI:

o ciascuna fase rilevante degli accordi con la Pubblica Amministrazione deve risultare da apposita documentazione scritta;

o ogni accordo/convenzione/contratto con enti pubblici è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe e/o apposite autorizzazioni scritte in essere;

o al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, il preposto aziendale è responsabile dell'archiviazione e della conservazione della documentazione di competenza, relativa anche alle singole operazioni, prodotta anche in via telematica o elettronica, nonché degli accordi/convenzioni/contratti definitivi, nell'ambito delle attività proprie del processo della stipula di rapporti con la Pubblica Amministrazione.

• in ordine ai sistemi premianti o di incentivazione, pur se attualmente non previsti, qualora venissero effettuati devono essere in grado: di assicurare la coerenza con le disposizioni di legge, con i principi contenuti nel presente protocollo, nonché con le previsioni del Codice Etico, anche prevedendo idonei meccanismi correttivi a fronte di eventuali comportamenti devianti.

9 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto su apposita piattaforma informatica – tutta la documentazione necessaria.

Conclusa l'ispezione, il PRES, o il responsabile della Funzione aziendale interessata, all'uopo incaricata, dovrà inviare una relazione riepilogativa all'OdV.

In ogni caso, il Responsabile della procedura informa, tempestivamente, l'Organismo di Vigilanza sulle ispezioni della Pubblica Amministrazione e sugli adempimenti richiesti alla Società.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse ai Processi Sensibili, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute; infatti, è obbligo per chiunque entri in contatto con la Pubblica Amministrazione in occasione d'ispezioni, accertamenti e verifiche di segnalare, tempestivamente, all'OdV anomalie o fatti straordinari nei rapporti con la Pubblica Amministrazione commessi (o tentati) in violazione nella presente procedura, nonché di eventuali violazioni del Modello e del Codice Etico.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

9.2 SEGNALAZIONI IMMEDIATE

Fermo restando l'obbligo di comunicazione periodica, tutti i destinatari della presente procedura sono tenuti a informare tempestivamente e senza ritardo l'OdV, anche attraverso i canali di Whistleblowing previsti dalla procedura aziendale dedicata, al verificarsi di:

1. qualsiasi richiesta di denaro, utilità o favori proveniente da funzionari pubblici, anche se declinata o non raccolta;
2. qualsiasi anomalia rilevata nei comportamenti di controparti pubbliche o di terzi nell'ambito di procedure di gara, collaudo o gestione di finanziamenti;
3. qualsiasi tentativo, anche solo prospettato, di commettere uno dei reati descritti nella presente procedura;
4. ispezioni non programmate o comunicazioni di avvio di procedimenti da parte di Autorità pubbliche che possano avere rilevanza ai sensi del D.Lgs. 231/01.

9.3 ARCHIVIO DIGITALE E TRACCIABILITÀ

Tutta la documentazione rilevante ai fini della presente procedura (verbali di ispezione, contratti con enti pubblici, documentazione di gara, registri degli accessi ai sistemi della P.A., relazioni di rendicontazione) è archiviata in formato digitale nella piattaforma documentale aziendale, con accesso garantito all'OdV in ogni momento.

9.4 Poteri di Controllo dell'OdV

L'OdV esercita, in conformità con il proprio Regolamento e con la Parte Generale del Modello, le seguenti attività di controllo in relazione alla presente procedura:

1. Verifiche a campione sulla documentazione relativa alle gare pubbliche e alle commesse in corso, anche con frequenza non programmata;
2. Verifiche a campione sui registri degli accessi ai sistemi informativi di enti pubblici;
3. Richiesta di documentazione integrativa rispetto a qualsiasi operazione o rapporto che presenti profili di rischio ai sensi della presente procedura.

9.5 Sistema Sanzionatorio

La violazione delle disposizioni della presente procedura, dei principi di comportamento e dei protocolli di controllo in essa contenuti costituisce illecito disciplinare, da trattarsi in conformità con quanto previsto dal sistema sanzionatorio adottato da IDRAGEST ai sensi del D.Lgs. 231/01.

Le sanzioni applicabili sono proporzionate alla gravità della violazione, alla posizione ricoperta dal soggetto, all'eventuale recidiva e alle conseguenze prodotte, e sono irrogate nel rispetto delle procedure previste dal CCNL applicabile (per i dipendenti) e dalle clausole contrattuali (per i collaboratori, consulenti e partner).

Le violazioni gravi, ovvero quelle idonee a integrare le fattispecie di reato descritte nella presente procedura, possono dare luogo alla risoluzione del rapporto di lavoro o del contratto di collaborazione, nonché all'adozione delle misure legali appropriate.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO 3

2 ACRONIMI AZIENDALI 4

3 RIFERIMENTI NORMATIVI 4

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA 5

5 PRINCIPI GENERALI DI COMPORTAMENTO 5

5.1 LA TENUTA DELLA CONTABILITÀ PRESSO UN CONSULENTE ESTERNO 6

5.2 PREVENZIONE DEI RISCHI E PROCEDURE DI CONTROLLO 6

5.3 CONTROLLO DEI BILANCI INFRANNUALI 8

5.4 DISTRIBUZIONE DI DIVIDENDI E GESTIONE DELLE OPERAZIONI STRAORDINARIE 8

5.5 AREA SENSIBILE CONCERNENTE I REATI TRIBUTARI - MANCATO PAGAMENTO DI IMPOSTE 9

6 Le attività sensibili relative ai reati tributari 15

6.1 PRINCIPI E REGOLE DI COMPORTAMENTO 15

6.2 PRINCIPI E NORME GENERALI DI COMPORTAMENTO 16

6.3 PRINCIPI DI CONTROLLO 16

7 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO 17

1 OBIETTIVI E FUNZIONI DEL MODELLO

Il presente protocollo ha lo scopo di definire le condotte che ciascuna Funzione Aziendale coinvolta deve osservare ai fine di garantire la corretta gestione delle attività inerenti la redazione ed approvazione del bilancio.

La procedura relativa alla predisposizione ed approvazione del bilancio viene posta in essere nel rispetto di quanto previsto nel Codice Etico e nel Modello adottati dalla Società ed in particolar modo nel rispetto delle procedure speciali disciplinate dal Modello 231 e relative ai "Reati societari e corruzione tra privati" ed ai "Reati tributari".

TUTTI I DESTINATARI DELLA PRESENTE PROCEDURA DEVONO:

a) tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società;

b) attivarsi affinché i fatti di gestione siano rappresentati correttamente e tempestivamente nella contabilità;

c) garantire la tempestività, l'accuratezza e il rispetto del principio di competenza nell'effettuazione

d) delle registrazioni contabili;

e) assicurarsi che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima e coerente con la documentazione di supporto in modo da consentire la ricostruzione accurata dell'operazione;

f) assicurare il rispetto dei principi contabili adottati e la tracciabilità nelle scritture di chiusura, assestamento e rettifica e le poste estimative/valutative;

g) assicurare la corretta contabilizzazione delle operazioni di acquisto, cessione / dismissione di immobilizzazioni immateriali, materiali e finanziarie e relative plusvalenze o svalutazioni;

h) applicare adeguate procedure di controllo in caso di sopravvenienze attive apparentemente non giustificate o in caso di registrazioni di incassi (e pagamenti) di cui non si riscontri una contropartita di credito (o debito) corrispondente;

i) osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;

l) assicurare il regolare funzionamento della società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare;

m) assicurare che i rapporti con i funzionari delle Autorità di Vigilanza siano gestiti esclusivamente dai soggetti dotati di idonei poteri;

n) effettuare con tempestività, correttezza e buona fede tutte le comunicazioni nei confronti di Autorità di Vigilanza – siano esse previste dalla legge o richieste dall'Autorità stessa - evitando ogni comportamento che possa risultare di ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate;

o) dare notizia, da parte di ogni Amministratore, agli altri amministratori di situazioni di conflitto di interessi relative a una determinata operazione, precisandone la natura, i termini, l'origine e la portata e astenersi dal partecipare alla relativa deliberazione.

p) assicurare che ogni tipo di operazione straordinaria sia condotta dalla Società nel pieno rispetto delle norme di legge o dei regolamenti applicabili;

q) mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei propri compiti e, in particolare, assicurare che la circolazione interna e verso Terzi di documenti contenenti informazioni potenzialmente privilegiate sia soggetta ad ogni necessaria attenzione e cautela, onde evitare pregiudizi ad IDRAGEST e indebite divulgazioni;

r) non comunicare ad altri, se non per motivi d'ufficio, le informazioni potenzialmente privilegiate di cui si viene a conoscenza;

s) far sottoscrivere, ai Terzi cui si comunicano informazioni potenzialmente privilegiate, in occasione del conferimento dell'incarico, un impegno di riservatezza.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale – Approvvigionamento
REC	Responsabile Esterno Contabilità
SOC	Soci

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di IDRAGEST S.r.l.;

- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutti i soggetti coinvolti nelle attività di contabilità generale e predisposizione del bilancio della Società ed in particolare nei confronti del PRES, del RAM e del REC

Il responsabile principale dell'attività di predisposizione del bilancio è l'Organo amministrativo. In via sussidiaria ne rispondono il RAM/RRU e il REC, nonché tutti i soggetti esterni (ovvero i consulenti) che operano per conto della Società.

5 PRINCIPI GENERALI DI COMPORTAMENTO

L'Organo Amministrativo è responsabile della predisposizione del Bilancio e della pubblicazione di dati non veritieri e corretti, salvo il caso in cui il fatto sia imputabile al comportamento colposo o doloso del professionista incaricato della medesima predisposizione.

Tutte le Funzioni Aziendali, interne ed esterne, a qualsiasi titolo coinvolte nelle attività di tenuta della contabilità e della successiva predisposizione/deposito delle comunicazioni sociali in merito alla situazione economico e patrimoniale di IDRAGEST, sono tenute ad osservare le modalità esposte nella presente procedure, nelle previsioni di legge esistenti in materia, nonché nelle procedure che disciplinano le attività in questione, norme tutte improntate a principi di trasparenza, accuratezza e completezza delle informazioni contabili al fine di produrre situazioni economiche, patrimoniali e finanziarie veritiere e tempestive anche ai sensi ed ai fini di cui agli artt. 2621 e 2622 del Codice Civile.

IN PARTICOLARE, LE FUNZIONI AZIENDALI SONO TENUTE A:

• rappresentare i fatti di gestione in modo corretto, completo e tempestivo nella contabilità e nei dati aziendali allo scopo di garantire la corretta e veritiera rappresentazione dei risultati economici, patrimoniali e finanziari di IDRAGEST;

• tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria di IDRAGEST.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

• rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria di IDRAGEST;

• omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria di IDRAGEST.

I Responsabili sono tenuti a porre in essere, oltre che le condotte di cui al punto 1) e 5) della presente procedura, anche tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

5.1 LA TENUTA DELLA CONTABILITÀ PRESSO UN CONSULENTE ESTERNO

IDRAGEST conferisce - con apposito mandato o lettera di incarico professionale, contenenti specifiche clausole relative all'osservanza dei principi e delle norme di condotta previste dal Codice Etico e dal Modello 231 – l'affidamento per la tenuta della contabilità a professionisti esterni, coadiuvati da un responsabile interno ad IDRAGEST e preposto alla raccolta, tenuta e trasmissione di tutta la contabilità della Società al REC.

L'attività di registrazione dei dati contabili deve essere svolta in osservanza agli obblighi di legge ed ai principi contabili nazionali e deve essere finalizzata ad assicurare la correttezza e l'affidabilità delle medesime registrazioni e dei *report* gestionali, nonché il tempestivo adempimento di tutti gli obblighi previsti dalle vigenti disposizioni di legge.

5.2 PREVENZIONE DEI RISCHI E PROCEDURE DI CONTROLLO

Le norme penali a cui il Decreto 231 fa riferimento in tema di reati societari, richiedono l'intenzionalità della condotta, ossia la volontarietà della falsa comunicazione. Pertanto, se non vi è una forma di partecipazione cosciente e volontaria il reato non sarà configurabile.

IDRAGEST garantisce la sussistenza delle necessarie competenze specialistiche dei professionisti esterni incaricati della tenuta della contabilità e, dunque, in ordine alla corretta applicazione delle norme tecniche in materia di formazione e valutazioni di bilancio (i c.d. principi contabili). La procedura di contabilizzazione e rilevazione dei dati, a sua volta, garantirà la correttezza delle informazioni sottostanti. Tutto ciò, complessivamente, si ritiene idoneo ad impedire la formulazione di una errata indicazione di importi nel bilancio o una errata esposizione di fatti nella nota integrativa.

Va peraltro evidenziato che, in generale, la definizione delle procedure aziendali in ambito amministrativo e dei connessi sistemi di controllo interno, acquisisce ulteriore valenza in termini di prevenzione dai rischi

di commissione dei reati, se viene supportata dal monitoraggio dei relativi comportamenti e adempimenti; tale monitoraggio costituisce un valido strumento d'individuazione delle "*aree a rischio*" nel sistema gestionale di settore e d'impresa.

IL CDA HA IL DOVERE DI VIGILARE SULL'INTERO PROCEDIMENTO CHE PORTA ALLA FORMAZIONE DEL BILANCIO ED, IN PARTICOLARE DOVRÀ:

1. monitorare l'identificazione dei dati e le notizie ricevute dal RAM/RRU e dal REC ai fini della predisposizione del bilancio;

2. assicurare che i documenti analizzati dovranno essere caricati e tenuti in apposito archivio informatico all'uopo predisposto nella piattaforma digitale di condivisione;

3. effettuare, a campione, un controllo sulla correttezza delle registrazioni contabili, eseguite dalle funzioni preposte;

4. garantire la formazione dei dipendenti coinvolti nella redazione del bilancio. All'uopo verranno organizzati dal PRES e/o RAM/RRU dei corsi di formazione sulle principali nozioni e problematiche giuridiche e contabili relative alla predisposizione del bilancio;

5. assicurare l'applicazione dei principi di trasparenza e veridicità nei controlli effettuati dal CDA;

6. prima di procedere all'approvazione del bilancio, riunirsi con l'Organismo di Vigilanza, il PRES (o, se delegato, il RAM/RRU) e il REC, al fine di analizzare eventuali criticità nell'attività di revisione.

Il rispetto dei principi fissati dal presente protocollo per le procedure aziendali di redazione ed approvazione del bilancio, unitamente al rispetto della legislazione vigente ed all'applicazione dei principi contabili nazionali e internazionali, consentiranno l'adozione di decisioni sui valori delle poste valutative del conto economico e dello stato patrimoniale, improntate sulla base di riscontri oggettivi e documentati, nel rispetto dei criteri di prudenza, veridicità e trasparenza, con riscontro esaustivo nella nota integrativa.

Inoltre, in occasione dell'approvazione del bilancio, il RAM/RRU, o la funzione eventualmente preposta a coadiuvare il REC nella redazione del bilancio, dovrà rilasciare un'apposita attestazione convalidata dal medesimo REC, attestante:

a. la veridicità e correttezza, la precisione e completezza dei dati e delle informazioni contenute nel bilancio, ovvero di tutti i documenti connessi, nonché degli elementi informativi messi a disposizione dalla società;

b. l'insussistenza di elementi da cui poter desumere che le dichiarazioni e i dati raccolti contengano elementi incompleti o inesatti;

c. l'insussistenza di elementi di non conformità riscontrati nell'attività prestata e l'indicazione della competenza dimostrata da parte del professionista incaricato della consulenza per la redazione del bilancio;

d. il rispetto delle procedure tese a fornire una ragionevole certezza sulla completezza delle informazioni e dei dati contenuti nei documenti utilizzati.

La suddetta attestazione deve essere trasmessa, prima dell'approvazione del bilancio, all'OdV, il quale potrà chiedere di esaminare la bozza di bilancio prima della data fissata per la sua adozione.

5.3 CONTROLLO DEI BILANCI INFRANNUALI

Il REC, trimestralmente e previo confronto con il RAM/RRU, dovrà caricare nell'apposito archivio informatico all'uopo predisposto nella piattaforma digitale di condivisione, le liquidazioni periodiche IVA, così da sottoporle all'attenzione del PRES, il quale dovrà controllarle e vistarle, con firma digitale o con firma olografa.

Il REC dovrà segnalare eventuali difformità rilevate nella disamina di documenti contabili per la redazione del bilancio all'OdV.

In particolare, dovranno essere attenzionate, a titolo meramente esemplificativo e non esaustivo, le seguenti voci: operazioni esenti IVA, gestione degli omaggi, capitalizzazione di cespiti e diritti pluriennali e relativi ammortamenti, dismissione di cespiti e diritti pluriennali, valorizzazione del magazzino, gestione dei fondi svalutazione e rischi, *etc.*

Di tali attività, l'OdV dovrà avere puntuale evidenza attraverso la trasmissione, con cadenza trimestrale, dei suddetti documenti.

5.4 DISTRIBUZIONE DI DIVIDENDI E GESTIONE DELLE OPERAZIONI STRAORDINARIE

Ogni operazione idonea a incidere nel patrimonio indisponibile della Società, non può essere effettuata se non previa e puntuale verifica della consistenza dello stato patrimoniale.

L'Organo Amministrativo dovrà, previamente, informare l'OdV delle adunanze dell'assemblea dei soci aventi all'ordine del giorno la distribuzione dei dividendi, l'approvazione del bilancio e l'autorizzazione a potere eseguire operazioni straordinarie di impresa (come fusione, scissione *etc.*).

In particolare, nella gestione delle operazioni straordinarie (es. fusioni, acquisizioni e dismissioni, ecc.) è richiesto che:

• ogni operazione sia sottoposta ed approvata dal Consiglio di amministrazione delle società interessate all'operazione straordinaria;

• sia sempre predisposta idonea documentazione a supporto dell'operazione, da parte della funzione aziendale proponente o competente all'istruzione della pratica con particolare attenzione ad operazioni di acquisizione e/o cessione con controparti che hanno la propria sede in stati esteri che non garantiscono la trasparenza societaria o abbiano una fiscalità privilegiata;

• prima di effettuare qualsiasi operazione di costituzione e/o acquisizione del controllo, anche in via indiretta, di società o enti assimilabili aventi sede legale in uno Stato estero, deve essere preventivamente verificato che lo Stato in cui la società ha sede: **(a)** garantisca un regime di trasparenza dell'informazione societaria compatibile con il regime di trasparenza in materia garantito dagli Stati dell'Unione Europea; **(b)** non sia presente nell'elenco dei Paesi a regime fiscale privilegiato (c.d. "black list");

• nelle ipotesi di costituzione e/o acquisizione del controllo, anche in via indiretta, di società o enti assimilabili che abbiano la propria sede in Stati esteri che non garantiscano la trasparenza societaria devono essere espresse le ragioni di natura imprenditoriale che giustificano l'operazione;

• sia verificata preliminarmente da parte della funzione aziendale competente, la completezza, inerenza e correttezza della documentazione di supporto dell'operazione, ai fini della registrazione contabile;

• in caso di operazioni straordinarie, sia previsto, anche attraverso il supporto di eventuali Advisor specialistici, l'avvio di attività di Due Diligence sull'oggetto della compravendita.

IL RAPPORTO DI DUE DILIGENCE DEVE CONTENERE:

- nominativi delle persone che hanno condotto le attività di Due Diligence;
- esami effettuati e i relativi esiti;
- deduzioni e raccomandazioni fatte;
- eventuali modifiche agli accordi da proporre alla controparte.

5.5 AREA SENSIBILE CONCERNENTE I REATI TRIBUTARI - MANCATO PAGAMENTO DI IMPOSTE

La disciplina dei reati tributari, che la puntuale ed attenta osservanza della presente procedura mira a prevenire, è stata riformata dal D. L. 124/2019, il cui articolo 39 ha introdotto nel D. Lgs. 231/2001 i reati tributari con effetto dal 24 dicembre 2019. L'articolo 5 del D. Lgs. 75/2020 vi ha poi aggiunto i reati di omessa o infedele dichiarazione e di indebita compensazione, ed ha reso punibili - modificando l'articolo 6 del D. Lgs.74/2000 - anche i reati dichiarativi di cui agli articoli 2, 3 e 4 solo tentati, con effetto dal 30 luglio 2020.

Ancora, si osserva che la normativa in materia è stata, nuovamente, modificata dal D. Lgs. N. 87 del 14.06.2024, "revisione del sistema sanzionatorio tributario", con la modifica del testo art. 10

quater D. Lgs 74/2000 (indebita compensazione) che ha interessato la fattispecie dei reati previsti dall'art. 25- quinquesdecies (reati tributari) D. Lgs. 231/2001.

Si ricorda che ai sensi dell'art. 26 del D. Lgs. 231/2001 la responsabilità degli enti per i delitti tentati non sussiste se l'ente volontariamente impedisce la finalizzazione dell'azione o il verificarsi dell'evento.

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di IDRAGEST S.r.l. i seguenti reati:

DICHIARAZIONE FRAUDOLENTA MEDIANTE FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 2 D. LGS. 74/2000)

L'Art.2 punisce chi al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.

Si riporta il testo dell'Art. 2 del D.L.gs 74 modificato al comma 1, con l'aggiunta del comma 2-bis.

"*1. È punito con la reclusione da quattro a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.*

2. Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.

2-bis. Se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, si applica la reclusione da un anno e sei mesi a sei anni".

Per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dal comma 1, la sanzione pecuniaria fino a cinquecento quote.

Per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dal comma 2-bis, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

DICHIARAZIONE FRAUDOLENTA MEDIANTE ALTRI ARTIFICI

(Art. 3 D.Lgs.n.74 modificato da Art. 39 del D.L. n.124 del 26 ottobre 2019)

L'Art.3 punisce chi al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti tende ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria.

Si riporta il testo dell'Art. 3 del D.L.gs.n.74 modificato al comma 1

"*1. Fuori dai casi previsti dall'articolo 2, è punito con la reclusione da tre a otto anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, quando, congiuntamente:*

- *L'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila*
- *L'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.*

2. Il fatto si considera commesso avvalendosi di documenti falsi quando tali documenti sono registrati nelle scritture contabili obbligatorie o sono detenuti a fini di prova nei confronti dell'amministrazione finanziaria.

3. Ai fini dell'applicazione della disposizione del comma 1, non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali."

Per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

Il reato di cui all'art 3 del D. Lgs. 74/2000 si realizza con la condotta di chi al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'Amministrazione Finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi.

Rispetto alla fattispecie prevista all'art. 2 devono essere posti in essere mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria (indicazione nel libro giornale e nel registro iva delle vendite di ricavi e iva a debito inferiori a quelli reali; sostituzione di documenti di vendita originariamente emessi con altri riportanti importi inferiori; indicazione nel libro giornale di costi fittizi; infedele e omessa registrazione di molteplici fatture di vendita e acquisto in modo da ridurre i ricavi e aumentare i costi).

DICHIARAZIONE INFEDELE (ART. 4 D. LGS. 74/2000)

(ART. 4 D.LGS.N.74 MODIFICATO DA ART. 39 DEL D.L. N.124 DEL 26 OTTOBRE 2019 E INSERITO DA D.LGS.N.75 DEL 14 LUGLIO 2020

L'Art.4 punisce chi al fine di evadere le imposte sui redditi o sul valore aggiunto, indica nella dichiarazione annuale elementi attivi o passivi diversi o inesistenti.

Si riporta il testo dell'Art. 4 del D.L.gs.n.74

"*1. Fuori dei casi previsti dagli articoli 2 e 3, è punito con la reclusione da due anni a quattro anni e sei mesi chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni annuali relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi inesistenti, quando, congiuntamente:*

a) l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro centomila

b) l'ammontare complessivo degli elementi attivi sottratti all'imposizione anche mediante indicazione di elementi passivi inesistenti, è superiore al dieci per cento dell'ammontare complessivo degli elementi attivi indicati in dichiarazione, o, comunque, è superiore a euro due milioni

1-bis. Ai fini dell'applicazione della disposizione del comma 1, non si tiene conto della non corretta classificazione, della valutazione di elementi attivi o passivi oggettivamente esistenti, rispetto ai quali i criteri concretamente applicati sono stati comunque indicati nel bilancio ovvero in altra documentazione rilevante ai fini fiscali, della violazione dei criteri di determinazione dell'esercizio di competenza, della non inerenza, della non deducibilità di elementi passivi reali.

1-ter. Fuori dei casi di cui al comma 1-bis, non danno luogo a fatti punibili le valutazioni che complessivamente considerate, differiscono in misura inferiore al 10 per cento da quelle corrette. Degli importi compresi in tale percentuale non si tiene conto nella verifica del superamento delle soglie di punibilità previste dal comma 1, lettere a) e b)."

Per il delitto di dichiarazione infedele, previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

OMESSA DICHIARAZIONE (ART. 5 D. LGS. 74/2000)

(ART. 5 D.LGS.N.74 MODIFICATO DA ART. 39 DEL D.L. N.124 DEL 26 OTTOBRE 2019 E INSERITO DA D.LGS.N.75 DEL 14 LUGLIO 2020)

L'Art.5 punisce il soggetto obbligato o il sostituto di imposta che, al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta una delle dichiarazioni relative a dette imposte

Si riporta il testo dell'Art. 5 del D.L.gs.n.74

"*1. È punito con la reclusione da due a cinque anni chiunque al fine di evadere le imposte sui redditi o sul valore aggiunto, non presenta, essendovi obbligato, una delle dichiarazioni relative a dette imposte, quando l'imposta evasa è superiore, con riferimento a taluna delle singole imposte ad euro cinquantamila.*

1-bis. È punito con la reclusione da due a cinque anni chiunque non presenta, essendovi obbligato, la dichiarazione di sostituto d'imposta, quando l'ammontare delle ritenute non versate è superiore ad euro cinquantamila.

2. Ai fini della disposizione prevista dai commi 1 e 1-bis non si considera omessa la dichiarazione presentata entro novanta giorni dalla scadenza del termine o non sottoscritta o non redatta su uno stampato conforme al modello prescritto."

Per il delitto di omessa dichiarazione, previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

EMISSIONE DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 8 D. LGS. 74/2000)

Il reato di cui all'art. 8 comma 1, 2 e 2-bis D. Lgs 74/2000 si realizza con la condotta di chi, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

OCCULTAMENTO O DISTRUZIONE DI DOCUMENTI CONTABILI (ART.10 D.LGS.N.74 MODIFICATO DA ART. 39 DEL D.L. N.124 DEL 26 OTTOBRE 2019)

L'Art.10 punisce chi distrugge o occulta documentazione per evadere o far evadere imposte sui redditi o sul valore aggiunto

Si riporta il testo dell'Art. 10 del D.L.gs 74 modificato al comma 1

"*1. Salvo che il fatto costituisca più grave reato, è punito con la reclusione da tre a sette anni chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.*"

Per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

INDEBITA COMPENSAZIONE (ART. 10-QUATER D. LGS. 74/2000) INSERITO DA D.LGS.N.75 DEL 14 LUGLIO 2020 E MODIFICATO DA D.LGS N. 87 DEL 14 GIUGNO 2024)

L'Art.10-quater punisce chi vantando crediti non spettanti, li utilizza in compensazione su somme dovute.

Si riporta il testo dell'Art. 10-quater del D.L.gs.n.74

"1. *È punito con la reclusione da sei mesi a due anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti non spettanti, per un importo annuo superiore a cinquantamila euro.*

2. È punito con la reclusione da un anno e sei mesi a sei anni chiunque non versa le somme dovute, utilizzando in compensazione, ai sensi dell'articolo 17 del decreto legislativo 9 luglio 1997, n. 241, crediti inesistenti per un importo annuo superiore ai cinquantamila euro.

2-bis La punibilità dell'agente per il reato di cui al comma 1 è esclusa quando, anche per la natura tecnica delle valutazioni, sussistono condizioni di obiettiva incertezza in ordine agli specifici elementi o alle particolari qualità che fondano la spettanza del credito".

Per il delitto di indebita compensazione, previsto dall'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1 e 2, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

La modifica apportata dal D.Lgs n. 87 del 14 Giugno 2024 con l'aggiunta del comma 2-bis tratta esclusivamente la punibilità dell'agente.

Invero, con il D.Lgs. n.87 del 14 Giugno 2024 sono state apportate modifiche all'interno dell'Art.25-quinquiesdecies del D.Lgs 231/01 (Reati tributari), ed in particolare, all'art.10-quater "Indebita compensazione" è stato aggiunto il comma 2-bis che tratta della eventuale esclusione della punibilità dell'agente in merito a spettanze del credito.

In particolare, il testo del comma 2 bis prevede testualmente: "*La punibilità dell'agente per il reato di cui al comma 1 è esclusa quando, anche per la natura tecnica delle valutazioni, sussistono condizioni di obiettiva incertezza in ordine agli specifici elementi o alle particolari qualità che fondano la spettanza del credito"*

SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DI IMPOSTE (ART. 11 D. LGS. 74/2000)

L'Art.11 punisce chi, per non pagare imposte sui redditi o sul valore aggiunto o altro, si adopera per rendere inefficace la procedura di riscossione

Si riporta il testo dell'Art. 11 del D.L.gs.n.74 e s.m.i.

"*1. Salvo che il fatto costituisca più grave reato è punito con la reclusione da sei mesi a quattro anni chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni.*

2. Salvo che il fatto costituisca più grave reato è punito con la reclusione da sei mesi a quattro anni chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila si applica la reclusione da un anno a sei anni."

Per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote.

Se, in seguito alla commissione dei delitti indicati al comma 1 e 2, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

Nel caso di mancato pagamento di imposte, il PRES deve verificare, annualmente, l'eventuale superamento delle soglie penali integranti reati perseguibili a carico del rappresentante legale. L'esito di tale verifica dovrà essere trasmesso all'OdV.

AL FINE DI PREVENIRE LA COMMISSIONE DI REATI FISCALI E LA SOTTRAZIONE FRAUDOLENTA, È FATTO ESPRESSO DIVIETO DI:

1) eludere o tentare di eludere, la procedura di riscossione coattiva, attraverso l'alienazione simulata di beni e/o la realizzazione di atti fraudolenti su beni propri o altrui;

2) indicare, nella documentazione presentata nell'ambito di contenziosi fiscali, elementi attivi o passivi diversi da quelli reali.

3) indicare, nella documentazione presentata nell'ambito di contenziosi fiscali, elementi attivi o passivi diversi da quelli reali.

Tutti i Destinatari dei superiori obblighi dovranno informare, tempestivamente, l'ODV di tutti i contenziosi della Società con l'Erario.

TENTATIVO (ART.6 D.LGS.N.74 MODIFICATO DA D.LGS. N. 156 DEL 4 OTTOBRE 2022)

L'Art.6 descrive la punibilità del solo tentativo di commissione del reato

Si riporta il testo dell'Art. 6 del D.L.gs.n.74/2000 e s.m.i.

"*[I]. I delitti previsti dagli articoli 2, 3 e 4 non sono punibili a titolo di tentativo , salvo quanto previsto al comma 1-bis.*

[I-bis]. Quando la condotta è posta in essere al fine di evadere l'imposta sul valore aggiunto 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 euro 10.000.000, il delitto previsto dall'articolo 4 è punibile a titolo di tentativo.

Fuori dei casi di concorso nel delitto di cui all'articolo 8, i delitti previsti dagli articoli 2 e 3 sono punibili a titolo di tentativo, quando ricorrono le medesime condizioni di cui al primo periodo.»".

6 LE ATTIVITÀ SENSIBILI RELATIVE AI REATI TRIBUTARI

L'analisi svolta ha permesso di individuare le attività della Società che potrebbero essere considerate "sensibili" con riferimento al rischio di commissione dei reati richiamati dall'Art. 25-quinquiesdecies del D.Lgs.n.231/2001 e da detta analisi è emerso come le aree a rischio "diretto" riguardano l'intera area amministrativa-contabile ed, in modo particolare, quelle interessate alle operazioni in materia di imposte e di versamenti di IVA.

6.1 PRINCIPI E REGOLE DI COMPORTAMENTO

Tutti i Processi Sensibili devono essere svolti conformandosi alle leggi vigenti, alle procedure aziendali e ai valori e alle regole contenute nella presente procedura.

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli, in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

6.2 PRINCIPI E NORME GENERALI DI COMPORTAMENTO

La presente Parte Speciale prevede l'espresso divieto a carico degli Organi Sociali aziendali (e dei Destinatari, Dipendenti, e Consulenti/Partner nella misura necessaria alle funzioni dagli stessi svolte) di:

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- Violare i principi e le procedure esistenti in azienda e/o previste nella presente Parte Speciale

La presente Parte Speciale prevede, conseguentemente, l'espresso obbligo a carico dei soggetti sopra indicati di:

- Tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività amministrativo–contabile;
- Assicurare che il processo di assunzione ed impiego del personale del settore amministrativo sia motivato da effettive necessità aziendali, che sia condotto in maniera trasparente e documentabile e che sia basato su criteri non arbitrari e quanto possibile oggettivi.
- Assicurare l'esistenza nell'impresa di un sistema sia organizzativo, sia amministrativo–contabile adeguati e che ricomprendano anche un sistema gestionale efficace.

6.3 PRINCIPI DI CONTROLLO

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

LIVELLI AUTORIZZATIVI DEFINITI NELL'AMBITO DEL PROCESSO:

- tutti i soggetti che intervengono nella gestione delle attività inerenti alla predisposizione delle dichiarazioni fiscali e nelle prodromiche attività di emissione / contabilizzazione delle fatture, sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale o all'uopo espressamente autorizzata dal Presidente. Tutta la documentazione dovrà essere accuratamente conservata.

- nel caso in cui intervengano consulenti esterni/fornitori, questi ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali; ogni eventuale accordo e/o convenzione con l'Agenzia delle Entrate è formalizzato in un documento, che dovrà essere debitamente autorizzato dal CDA e firmato dal Presidente

SEGREGAZIONE DEI COMPITI TRA I DIFFERENTI SOGGETTI COINVOLTI NEI PROCESSI DI GESTIONE DEI RISCHI E DEGLI ADEMPIMENTI AI FINI DELLA PREVENZIONE DEI REATI TRIBUTARI. IN PARTICOLARE:

- le attività di cui alle diverse fasi del processo devono essere poste in essere da Funzioni Aziendali diverse e devono essere autorizzate dal Presidente.

ATTIVITÀ DI CONTROLLO:

le Funzioni Aziendali all'uopo preposte dovranno effettuare:

- controlli di completezza, correttezza ed accuratezza delle informazioni trasmesse alle autorità fiscali;
- controlli di carattere giuridico sulla conformità alla normativa di riferimento della dichiarazione fiscale;
- controlli continuativi automatici di sistema, con riferimento alle dichiarazioni periodiche;
- controlli sulla corretta emissione, applicazione delle aliquote IVA e contabilizzazione delle fatture del ciclo attivo e sulla loro corrispondenza con i contratti e impegni posti in essere con i terzi;
- controlli sull'effettività, sia dal punto di vista soggettivo che oggettivo, del rapporto sottostante alle fatture passive ricevute e sulla corretta registrazione e contabilizzazione.

7 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutti i *Destinatari* coinvolti nella predisposizione del bilancio e della relativa documentazione, devono comunicare, tempestivamente, all'Organismo di Vigilanza:

- eventuali situazioni anomale;
- eventuali violazioni della presente procedura;
- eventuali comportamenti non conformi a quanto previsto dal Modello e dal Codice Etico.

INOLTRE, L'ORGANO AMMINISTRATIVO È TENUTO A TRASMETTERE ALL'ORGANISMO DI VIGILANZA, CON PERIODICITÀ ALMENO SEMESTRALE, ULTERIORI INFORMAZIONI SPECIFICAMENTE RICHIESTE OVVERO:

- rilievi eventualmente segnalati dal RAMM e/o dal REC;
- rilevante modifica dell'assetto sociale ed eventuali casi di esclusione del diritto di voto per determinate categorie di soci.

I *Destinatari*, qualora dal processo di tenuta della contabilità e dalla redazione del Bilancio risultino voci e/o movimenti non giustificati – come ad es. "*sopravvenienze attive apparentemente non giustificate*" o casi "*di registrazioni di incassi e/o pagamenti*" di cui non si riscontri una contropartita di credito (o debito) corrispondente, sarà necessario comunicare, tempestivamente, le predette anomalie all'OdV.

I *Destinatari* devono, altresì, garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto nell'apposita piattaforma di condivisione - tutta la documentazione necessaria.

Tutta la documentazione relativa alla tenuta della contabilità, alla predisposizione del bilancio e della documentazione connessa, è archiviata a cura del RAM/RRU, o della funzione eventualmente incaricata dal PRES, ed è tenuta a disposizione dell'OdV.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati di false comunicazioni sociali;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI E LA FUNZIONE DEL MODELLO 4

2 ACRONIMI AZIENDALI 4

3 RIFERIMENTI NORMATIVI 5

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA 5

5 PRINCIPI GENERALI DI COMPORTAMENTO 6

5.1 LA GESTIONE DEI PAGAMENTI ED UTILIZZO DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI 7

5.2 GESTIONE INCASSI 9

5.3 GESTIONE RAPPORTI CON ISTITUTI DI CREDITO 9

5.4 GESTIONE CASSA CONTANTE 10

5.5 FATTURAZIONE ATTIVA E PASSIVA E TRASMISSIONE PERIODICA LIQUIDAZIONE IVA 10

6 TRASFERIMENTO FRAUDOLENTO DI VALORI (EX ART. 512 BIS C.P.) E MODIFICATO DA D.L. N.19 DEL 2 MARZO 2024 COORDINATO CON LA LEGGE DI CONVERSIONE N.56 DEL 29 APRILE 2024) 12

7 ACQUISIZIONE DI NUOVI CESPITI E DISMISSIONE DEI CESPITI 15

8 Aggiotaggio (Art. 2637 c.c. modificato da legge n.32 del 23 settembre 2025) 15

9 Aree a rischio 17

10 PRINCIPI DI COMPORTAMENTO 18

10.1 Principi procedurali specifici 19

11 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO 20

1 OBIETTIVI E LA FUNZIONE DEL MODELLO

Con la presente procedura vengono definiti, nell'ambito dei sistemi di incasso e di pagamento, i ruoli, le responsabilità, le attività di controllo ed i principi di comportamento adottati da IDRAGEST S.r.l.

La presente procedura definisce, altresì, l'adeguamento alla riforma delle norme penali in materia di contrasto alle frodi e alle falsificazioni di mezzi di pagamento diversi dai contanti, attuata con il D.Lgs. 8 novembre 2021 n. 184, il D.Lgs. n. 195 dell'8 Novembre 2021 e la Legge n. 238 del 23.12.2021.

Invero, la suddetta riforma, ha fissato i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento adottati da IDRAGEST S.r.l. nell'ambito del processo di gestione ed utilizzo di sistemi informatici, per le attività a rischio, connesse con la fattispecie di reato prevista dall'art. 25-octies, rubricato "*Delitti in materia di strumenti di pagamento diversi dai contanti*", che ha, dunque, ampliato il catalogo dei reati presupposto 231(ovvero dei reati relativi alla responsabilità amministrativa degli enti in materia di strumenti di pagamento diversi dai contanti, quali l'art. 493-ter e l'art. 493-quater).

Infatti, è stato modificato il reato presupposto 231 di cui all'art. 24 bis D.lgs. n. 231/2001, prevedendo che, con riferimento all'art. 640-ter cod. pen., per l'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale, la sanzione pecuniaria arrivi sino a 500 quote. Inoltre, è stato previsto un generale inasprimento delle sanzioni qualora si verifichino trasferimenti illeciti di mezzi di pagamento diversi dal contante. Dunque, tali prescrizioni integrano, altresì, i principi di comportamento di cui al Modello e al Codice Etico.

La presente procedura costituisce, inoltre, uno strumento essenziale per l'adempimento del dovere, in capo all'organo amministrativo, di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa, ai sensi dell'art. 2086 del Codice Civile

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale
RATTR	Responsabile Attrezzature e Mezzi
CDL	Consulente del Lavoro
REC	Responsabile Esterno Contabilità

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Regolamento (UE) 2024/1624 del Parlamento europeo e del Consiglio, del 31 maggio 2024, relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo;
- Decreto Legislativo 21 novembre 2007, n. 231, in materia di prevenzione del riciclaggio e del finanziamento del terrorismo;
- Decreto Legislativo 10 marzo 2023, n. 24, in materia di protezione delle persone che segnalano violazioni (Whistleblowing);
- Codice Etico di IDRAGEST S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutti i *Destinatari* che hanno, all'interno di IDRAGEST S.r.l., il potere di ricevere denaro o di eseguire pagamenti in nome e per conto della Società, nonché di gestire per conto di IDRAGEST gli adempimenti di natura fiscale-amministrativo-contabile.

In particolare, sono *Destinatari* della presente parte speciale, ciascuno nell'ambito delle proprie attività, l'Organo Amministrativo, il Responsabile dell'Amministrazione e delle Risorse Umane, il Responsabile Commerciale e dell'Approvvigionamento, le funzioni preposte agli adempimenti contabili e fiscali, il Responsabile Esterno della Contabilità, nonché tutte le controparti commerciali e/o di lavoro della IDRAGEST S.r.l. che potrebbero concorrere alla realizzazione delle fattispecie di reato ivi previste dalla presente procedura.

Dunque, il principale responsabile della presente procedura è l'Organo Amministrativo. Sono, altresì, responsabili, ciascuno nell'ambito delle proprie attività, il RAM/RRU e il REC, nonché tutti i consulenti esterni che operano per conto e nell'interesse della *Società*.

5 PRINCIPI GENERALI DI COMPORTAMENTO

La presente procedura disciplina l'attività di controllo e di monitoraggio delle risorse economiche e finanziarie, nonché degli incassi e dei pagamenti che vengono gestiti dalle diverse Funzioni Aziendali, nei limiti degli importi che vengono autorizzati e nel rispetto della presente procedura.

I flussi finanziari, ovvero le procedure relative agli incassi ed ai pagamenti sono regolati dalle disposizioni di legge, in modo tale da garantire la tracciabilità di tutte le operazioni di tesoreria, riscontrabili anche presso i principali Istituti di Credito nazionali.

I *Destinatari* della presente procedura:

- ✓ Non dovranno porre in essere comportamenti che possano configurare le fattispecie delittuose di cui all'art. 25 quinquiesdecies del Decreto e, più in generale, di tutte le ipotesi criminali ivi previste;
- ✓ Non dovranno intrattenere rapporti commerciali con soggetti fisici o giuridici dei quali sia conosciuta o anche solo sospettata l'appartenenza ad organizzazioni criminali di qualsiasi tipo, o la cui reputazione e integrità siano dubbie, previa adeguata verifica;
- ✓ Non dovranno accettare denaro e titoli per importi superiori a quelli previsti dal D.lgs.25 maggio 2017 n. 90 ss.mm.ii. e dalle successive modifiche e integrazioni, se non tramite intermediari a ciò abilitati, quali Istituti Bancari, gli Istituti di moneta elettronica e Poste Italiane S.p.A;
- ✓ non dovranno accettare denaro e titoli trasferiti attraverso l'utilizzo di dispositivi, materiali o immateriali, o una loro combinazione, diversa dalla moneta a corso legale;
- ✓ Non dovranno porre in essere le condotte aventi ad oggetto mezzi di pagamento digitali attraverso ai quali viene scambiata moneta elettronica avente corso legale, ma anche le c.d. criptovalute, prive di valore legale ma sempre più accettate come mezzi di pagamento;
- ✓ Non dovranno adottare comportamenti finalizzati a trarre profitto per sé e per gli altri acquistando, ricevendo od occultando danaro o cose provenienti da un qualsiasi delitto, o comunque intromettendosi nel farli acquistare, ricevere od occultare;
- ✓ Non dovranno sostituire o trasferire denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compiere operazioni tese ad ostacolare l'identificazione della loro provenienza delittuosa;
- ✓ Non dovranno impiegare in attività economiche o finanziarie di denaro, beni o altre utilità provenienti dai casi di cui agli artt. 648 e 648 bis c.p;

- ✓ Non dovranno impiegare, sostituire, trasferire in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di un delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa;
- ✓ Non dovranno porre in essere una condotta che abbia, anche solo, creato intralcio non definitivo, ma concreto, rispetto all'identificazione della provenienza delittuosa del bene;
- ✓ Non dovranno commettere negozi simulati riguardanti non solo denaro contante su un conto corrente o beni immobili, ma beni della più diversa natura, quali a titolo esemplificativo la cessione di quote o azioni eseguita al fine di estraniarsi dalla compagine della società solo apparentemente, poiché chi si è spogliato formalmente della titolarità delle quote o azioni continua di fatto a determinarne l'attività come amministratore o socio occulto ed a partecipare alla gestione e agli utili derivanti dall'attività imprenditoriale;
- ✓ Non dovranno attribuire, fittiziamente, ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di ricettazione, riciclaggio e impiego di denaro o beni di provenienza illecita (di cui agli artt. 648, 648-bis e 648-ter c.p.).

5.1 LA GESTIONE DEI PAGAMENTI ED UTILIZZO DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

La Funzione Aziendale autorizzata ad effettuare il pagamento è tenuta al rispetto delle fasi qui di seguito riportate:

1. Il RAM deve predisporre un piano di pagamenti mensile, che verrà condiviso in una piattaforma digitale (ad es. TEAMS o simili) e che dovrà essere validato, con firma digitale o con firma olografa, dal PRES.;
2. per il pagamento dei dipendenti, è necessario acquisire, prima di eseguire il pagamento, il documento giustificativo della spesa (come ad esempio le buste paga, i giustificativi per rimborso spese, *etc.*), validato da una diversa Funzione Aziendale;
3. il pagamento delle prestazioni di consulenza e della fornitura richiede l'attuazione dei seguenti presidi:
   - il pregresso inserimento nella anagrafica del gestionale;
   - la regolare emissione della fattura;

- l'effettiva esecuzione della prestazione per la quale si richiede o si effettua il pagamento, mentre nel caso di forniture di merci, di materiale, di beni strumentali, la funzione incaricata dovrà verificare e confermare l'avvenuta consegna dei beni);
- la corrispondenza tra il pagamento effettuato ed il corrispettivo indicato nel contratto o in eventuali preventivi.

4. I pagamenti superiori ad € 15.000,00 giornalieri, dovranno essere, previamente autorizzati, per iscritto, dal PRES e dovranno essere indicati nello specifico *report* semestrale che dovrà essere trasmesso all'OdV.

Infatti, in ordine alla predetta autorizzazione, si precisa che il RAM inserirà, nel piano di pagamenti mensile, un'apposita voce e, precisamente "*pagamenti superiori ad € 15.000,00*", in modo tale che il PRESIDENTE possa autorizzare, con firma digitale o con firma olografa, i pagamenti effettuati oltre la soglia "*ordinaria*";

5. non sono ammessi pagamenti in contanti, oltre a quanto previsto dalla normativa vigente ed, in ogni caso, non sono ammessi pagamenti in contanti per importi superiori ad euro 500,00 giornalieri;

6. in caso di tenuta di contabilità esterna, il professionista terzo è tenuto a segnalare all'OdV i pagamenti effettuati in carenza di documentazione giustificativa.

Il PRES, infatti, verifica che vengano osservati tutti gli obblighi di legge in materia di limitazione all'uso del contante e dei titoli al portatore.

Il presente protocollo si applica a tutte le Funzioni aziendali coinvolte nella gestione e nell'utilizzo degli strumenti di pagamento diversi dai contanti.

IDRAGEST è costantemente impegnata nella ricerca e nell'attuazione di soluzioni operative il più possibile aggiornate, finalizzate a prevenire e ad ostacolare gli utilizzi fraudolenti degli strumenti di pagamento e quindi l'esecuzione di operazioni di pagamento non autorizzate.

Ai sensi del D. Lgs 231/2001, il processo potrebbe presentare occasioni per la commissione del reato di "*Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti*" e ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale a condizione che ne siano oggetto materiale strumenti di pagamento diversi dai contanti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte di IDRAGEST, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

DESCRIZIONE DEL PROCESSO

Il processo di gestione e utilizzo degli strumenti di pagamento diversi dai contanti si articola nei seguenti processi:

• Carte di pagamento (carte di debito e di servizio, carte di credito, carte prepagate);

• Incassi e pagamenti (es. assegni, bonifici, addebiti diretti, RIBA – MAV – effetti);

• Servizi di Accesso ai Canali Digitali (accesso ed identificazione a distanza destinati a persone fisiche e persone giuridiche, altri servizi);

• Gestione risorse Umane con riferimento alle carte di credito aziendali e, laddove erogate dalla Società ai Dipendenti, ai buoni pasto, alle carte di servizio per le autovetture (carta carburante, telepass).

5.2 GESTIONE INCASSI

Relativamente al processo di gestione degli incassi, il RAM/RRU, o altra Funzione Aziendale eventualmente incaricata per iscritto, deve:

- ✓ Verificare l'identità della persona fisica o giuridica che esegue il pagamento;
- ✓ verificare che per ciascun incasso corrisponda un documento giustificativo.

Il RAM deve predisporre un "*piano degli incassi mensile*", che verrà condiviso, unitamente ad un "*piano pagamenti mensile*", su una piattaforma digitale (come ad es. TEAMS o simili) e verrà validato, con firma digitale o con firma olografa, apposta dal Presidente.

Il PRES verifica che le movimentazioni di somme di denaro avvengano sempre attraverso intermediari finanziari, come Banche, Istituti di moneta elettronica od altri soggetti tenuti all'osservanza della Direttiva 2005/60/CE (III Direttiva antiriciclaggio) e che vengano osservati tutti gli obblighi di legge in materia di limitazione all'uso del contante e dei titoli al portatore.

Per ciò che concerne gli incassi in contante, è preferibile evitare qualsiasi forma di cosiddetto "*pagamento facilitato*", salvo che si tratti di piccole somme. Tuttavia, in tal caso, prima di accettare i suddetti pagamenti, occorre consultare l'Organo Amministrativo della Società.

5.3 GESTIONE RAPPORTI CON ISTITUTI DI CREDITO

La gestione dei rapporti con gli Istituti di Credito (come l'apertura di c/c bancari, la costituzione di depositi e la gestione di strumenti finanziari, la costituzione e la stipulazione di finanziamenti e di fidi, etc.) è di esclusiva competenza dell'Organo Amministrativo e, particolarmente, del Presidente.

Il REC esegue, con cadenza trimestrale, il controllo della riconciliazione dei saldi bancari con le risultanze contabili, verificando, dunque, la quadratura dei saldi bancari. La Società, con cadenza trimestrale, comunica l'avvenuta verifica della predetta quadratura dei saldi bancari all'OdV con specifici report. In tale sede, il REC segnala all'OdV anche eventuali condizioni anomale, ingiustificate o l'emersione di rischi non precedentemente valutati.

5.4 GESTIONE CASSA CONTANTE

I prelevamenti di cassa sono eseguiti dai componenti dell'Organo Amministrativo o dai soggetti muniti di bancomat e all'uopo espressamente autorizzati dal CDA.

Solo per spese impreviste - documentalmente rendicontate - potranno essere prelevate, senza la previa autorizzazione del CDA, somme per un ammontare non superiore ad € 300,00 mensili.

Il soggetto che ha eseguito la predetta operazione dovrà darne comunicazione al RAM, precisando, altresì, la causale.

La documentazione cartacea attestante la gestione della cassa (ricevute, scontrini, prelievo) viene archiviata secondo regole interne che ne assicurino la rintracciabilità.

L'Organo Amministrativo, con cadenza trimestrale, effettua la quadratura di cassa, ove vi sia stata, ed in tal caso il RAM la sottoporrà al Presidente per il visto, che verrà apposto con firma digitale o con firma olografa.

5.5 FATTURAZIONE ATTIVA E PASSIVA E TRASMISSIONE PERIODICA LIQUIDAZIONE IVA

Le Funzioni Aziendali all'uopo preposte - come il REC e il RAM/RRU – devono garantire una corretta gestione dei processi di fatturazione attiva e passiva, ovvero delle diverse fasi di emissione e/o ricezione, nonché della fase di registrazione del pagamento.

In particolare, le predette Funzioni Aziendali devono: **1)** controllare le fatture emesse e/o ricevute, nonchè i controlli di registrazione delle medesime; **2)** accertare la coerenza delle informazioni contenute nei documenti giustificativi delle operazioni e la conformità dei dati inseriti nei medesimi documenti.

Le Funzioni Aziendali all'uopo preposte, dovranno dare immediata comunicazione all'OdV di eventuali anomalie che venissero riscontrate a seguito dei predetti controlli.

Gli adempimenti relativi alla trasmissione periodica dell'IVA dovranno essere tempestivamente messi a conoscenza dell'OdV mediante apposito report.

IDRAGEST adotta un sistema gestionale relativo a tutte le attività fiscali-amministrativo-contabili, ed in particolare per le attività di fatturazione attiva e passiva, nonché dei relativi incassi ed acquisti, dovrà assicurare che:

1) i soggetti incaricati di porre in essere le citate attività, e con particolare riferimento alle attività di formazione, trasmissione, archiviazione ed eventuale aggiornamento della documentazione rilevante;

2) la registrazione di tutte le fasi del procedimento, ivi compresa, ove prevista, l'eventuale fase autorizzativa;

3) l'esistenza di appositi supporti, analogici e/o digitali, finalizzati ad assicurare la tracciabilità delle fatture emesse e/o ricevute dalla Società;

4) la tracciabilità dei pagamenti e/o degli incassi ricevuti, al fine di consentire la corretta emissione/registrazione della fattura (attiva/passiva) e del perfezionamento della fase di pagamento/incasso;

5) l'applicazione di procedure specifiche per la gestione degli accessi, tali da consentire la tracciabilità dei singoli passaggi, l'identificazione dei soggetti che inseriscono i dati nel sistema e di quelli autorizzati ad apportare modifiche, nonché la rilevazione degli accessi non autorizzati.

5.6 PRESIDI DI PREVENZIONE DEL RICICLAGGIO

In ottemperanza ai principi del Regolamento (UE) 2024/1624 e del D.Lgs. 231/2007, e in misura proporzionata al rischio specifico della Società, sono istituiti i seguenti presidi per prevenire i reati di riciclaggio, autoriciclaggio e finanziamento del terrorismo:

A) ADEGUATA VERIFICA DELLA CLIENTELA (CUSTOMER DUE DILIGENCE): Prima di instaurare un rapporto d'affari o eseguire un'operazione significativa, la funzione competente (es. RCOM/APVG) effettua un'adeguata verifica del cliente/fornitore. Tale verifica, basata su un approccio commisurato al rischio (risk-based approach), include l'identificazione del cliente e del suo titolare effettivo, e l'acquisizione di informazioni sullo scopo e la natura del rapporto d'affari.

B) MONITORAGGIO DELLE OPERAZIONI: Il RAM/RRU, monitora costantemente le operazioni finanziarie per individuare anomalie indicative di un potenziale rischio di riciclaggio. Costituiscono indicatori di anomalia, a titolo esemplificativo, operazioni di importo elevato non giustificate dall'attività corrente,

operazioni con controparti in paesi a rischio, utilizzo ingiustificato di contanti, o schemi di pagamento anomali (es. pagamenti a cifra tonda, rapido movimento di fondi) [6][13].

c) Segnalazione di Operazioni Sospette (S.O.S.): Qualsiasi Destinatario (dipendente, amministratore, consulente) che nutra il sospetto che un'operazione possa essere collegata ad attività criminose, ha l'obbligo di effettuare una segnalazione riservata all'Organismo di Vigilanza (OdV), fornendo tutti gli elementi a disposizione.

d) Gestione della Segnalazione e inoltro alla UIF: L'OdV valuta la segnalazione ricevuta. Se la ritiene fondata, provvede a trasmetterla senza ritardo all'Unità di Informazione Finanziaria (UIF) per l'Italia, secondo le modalità previste dalla legge.

e) Divieto di "Tipping-Off": È fatto divieto assoluto a chiunque sia coinvolto nel processo di segnalazione di comunicare al cliente interessato o a terzi l'avvenuta segnalazione o che sia in corso un'indagine in materia di riciclaggio.

6 TRASFERIMENTO FRAUDOLENTO DI VALORI (EX ART. 512 BIS C.P.) E MODIFICATO DA D.L. N.19 DEL 2 MARZO 2024 COORDINATO CON LA LEGGE DI CONVERSIONE N.56 DEL 29 APRILE 2024)

L'art. 6-ter della Legge 137/2023 ha introdotto all'interno dell'art. 25-octies.1, concernente i delitti in materia di strumenti di pagamento diversi dai contanti, la fattispecie di trasferimento fraudolento di valori (art. 512-bis c.p.), in relazione al quale è prevista per gli Enti la sanzione pecuniaria da 250 a 600 quote; alle citate sanzioni si aggiungono le sanzioni interdittive di cui ex art. 9, co. 2 del D.Lgs. n. 231/2001.

Pertanto, la suddetta Legge 137/2023 ha inserito tra i reati-presupposto il delitto di trasferimento fraudolento di valori di cui all'art. 512-bis c.p..

L'art. 512-bis c.p. prevede che "*Salvo che il fatto costituisca più grave reato, chiunque attribuisce fittiziamente ad altri la titolarità o disponibilità di denaro, beni o altre utilità al fine di eludere le disposizioni di legge in materia di misure di prevenzione patrimoniali o di contrabbando, ovvero di agevolare la commissione di uno dei delitti di cui agli articoli 648, 648-bis e 648-ter, è punito con la reclusione da due a sei anni*".

Dunque, il delitto di "trasferimento fraudolento di valori" si aggiunge all'indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.); alla detenzione e diffusione di dispositivi diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.) e alla frode informatica (art. 640-ter c.p.) aggravata dal trasferimento di denaro.

Dall'esame della citata disposizione emerge come si tratta di un reato che può essere commesso con una grande varietà di negozi simulati riguardanti non solo denaro contante su un conto corrente o beni immobili, ma beni della più diversa natura.

Invero, a titolo meramente esemplificativo, si può ritenere che l'ipotesi più ricorrente, nell'ambito della quale si può configurare il predetto reato, è quella della cessione di quote o azioni eseguita al fine di estraniarsi dalla compagine della società solo apparentemente, poiché chi si è spogliato formalmente della titolarità delle quote o delle azioni continua di fatto a determinarne l'attività come amministratore o socio occulto e a partecipare alla gestione e agli utili derivanti dall'attività imprenditoriale.

Il reato di cui all'art. 512-bis c.p., è un reato solo eventualmente plurisoggettivo, con la conseguenza che il terzo fittiziamente interposto (non punito direttamente dalla stessa disposizione) risponde a titolo di concorso con chi ha operato la fittizia attribuzione in quanto con la sua condotta cosciente e volontaria, contribuisce alla lesione dell'interesse protetto dalla norma (Corte di Cassazione sentenza n. 35826/2019).

È, quindi, sufficiente, ai fini della configurabilità del dolo del concorrente, che la particolare finalità tipizzata dalla disposizione incriminatrice sia perseguita almeno da uno dei soggetti che concorrono alla realizzazione del fatto (Corte di Cassazione sentenza n. 38044/2021).

La Legge n. 56/2024 - rubricata "Conversione in legge, con modificazioni, del D.L. 2 marzo 2024, n. 19, recante ulteriori disposizioni urgenti per l'attuazione del Piano Nazionale di Ripresa e Resilienza (PNRR) - ha modificato, ampliando il campo di applicazione, il testo di cui all'art. 512 – bis c.p., rubricato "Trasferimento fraudolento di valori", peraltro inserito di recente all'interno del catalogo dei reati presupposto di cui al d.lgs. 231/2001, all'art. 25 – octies.1.

E' stato quindi aggiunto il nuovo secondo comma, secondo cui: "*La stessa pena di cui al primo comma [reclusione da due a sei anni] si applica a chi, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni*".

Tale ultima modifica assume particolare rilevanza per le Società, specie per quelle che partecipano a bandi pubblici, in ragione della documentazione richiesta e da produrre in fase di gara, ma anche per ciò che concerne le procedure di qualificazione dei fornitori, e più in generale per tutte quelle che hanno particolari obblighi di segnalazione e vigilanza sulla clientela e che effettuano operazioni di trasferimento di beni, denaro o partecipazioni societarie.

È necessario pertanto, in logica preventiva, procedere ad un aggiornamento ed implementazione dei Protocolli e delle Istruzioni Operative aziendali, prevendendo specifici presidi per questa nuova fattispecie criminosa.

Invero, con l'ultima modifica apportata all'Art.512-bis c.p. la pena della reclusione da due a sei anni prevista dal primo comma si applica a chi, al fine di eludere le disposizioni in materia di documentazione antimafia, attribuisce fittiziamente ad altri la titolarità di imprese, quote societarie o azioni ovvero di cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o di concessioni.

PERTANTO, I DESTINATARI DELLA PRESENTE PROCEDURA DOVRANNO ASTENERSI:

- Dall'eludere le disposizioni in materia di misure di prevenzione patrimoniali o di contrabbando o per agevolare la commissione dei delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, spogliandosi fittiziamente della titolarità di denaro, beni o altre utilità, attribuendola a terzi.

IL SISTEMA SANZIONATORIO:

Si rammenta che l'art. 25 octies.1 d.lgs. 231/2001 nel testo vigente annovera, al comma 1, quali reati presupposto, l'indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.), con sanzione amministrativa da 300 a 800 quote, la detenzione e diffusione di dispositivi diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.) e la frode informatica (art. 640-ter c.p.) aggravata dal trasferimento di denaro, con sanzione amministrativa fino a 500 quote. Il comma 2 contempla poi quale reato presupposto ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, salvo che il fatto costituisca più grave illecito amministrativo, con sanzioni amministrative graduate a seconda della pena edittale prevista dal codice penale.

La sanzione pecuniaria ora prevista per il trasferimento fraudolento di valori è invece da 250 a 600 quote. Inoltre, il comma 3 prevede che, nei casi di condanna per uno dei delitti di cui al medesimo art. 25.octies.1, e quindi da adesso anche per il reato di cui all' art. 512-bis c.p., si applichino all'Ente le sanzioni interdittive dell'interdizione dall'esercizio dell'attività; della sospensione o della revoca delle autorizzazioni, licenze o concessioni; del divieto di contrattare con la pubblica amministrazione, dell'esclusione da agevolazioni, finanziamenti, contributi o sussidi; del divieto di pubblicizzare beni o servizi (di cui al citato art. 9 comma 2, d.lgs. 231/2001).

DUNQUE, SI APPLICHERANNO LE SEGUENTI SANZIONI:

- Sanzioni pecuniarie da 250 a 600 quote.
- Sanzioni interdittive:
  - interdizione dall'esercizio dell'attività
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio.
  - Esclusione dalle agevolazioni, finanziamenti, contributi o sussidi ed eventuale revoca di quelli già concessi;
  - Divieto di pubblicizzare beni o servizi

7 ACQUISIZIONE DI NUOVI CESPITI E DISMISSIONE DEI CESPITI

In ordine ai cespiti, IDRAGEST definisce le regole e le procedure aziendali per l'approvazione dell'acquisizione o della cessione o dismissione dei cespiti, con la previsione di un processo approvativo che consiste:

▪ Il RATTR, o altra Funzione Aziendale all'uopo autorizzata, deve comunicare al Presidente e al RAM/RRU la possibilità di acquisire un nuovo cespite o l'esigenza di dismettere un cespite, caricando, nell'apposito archivio informatico della piattaforma digitale, una scheda del bene in questione e la relativa richiesta di autorizzazione, al fine di consentire la necessaria autorizzazione da parte del PRES che può sottoscrivere, con firma digitale o con firma olografa, la suddetta scheda. Ottenuta l'autorizzazione, il RATTR o la Funzione responsabile all'uopo autorizzata, procede con la dismissione del bene.

▪ la Funzione Aziendale competente prima di porre in essere l'atto di acquisizione o di dismissione del cespite, dovrà essere, previamente, autorizzata dal PRES, il quale apporrà la propria firma olografa o digitale nella citata autorizzazione;

▪ deve essere attuata la gestione contabile e fiscale della registrazione associata all'acquisizione e alla cessione o dismissione dei cespiti.

8 AGGIOTAGGIO (ART. 2637 C.C. MODIFICATO DA LEGGE N.32 DEL 23 SETTEMBRE 2025)

Il market abuse indica il comportamento di alcuni soggetti che, approfittando di informazioni confidenziali, diffondendo notizie non vere o falsando il meccanismo di determinazione del prezzo degli strumenti finanziari, cagionano conseguenze sfavorevoli per gli investitori.

La disciplina attuale del market abuse è stata introdotta dalla L. n. 62/2005, che ha recepito la direttiva 2003/6/Ce e ha sostituito l'originario capo IV (Abuso di informazioni privilegiate e aggiotaggio su strumenti finanziari) del Titolo I della Parte V del D.Lgs. 58/1998 (T.U.F.), introducendo il Titolo I-bis (Abuso di informazioni privilegiate e manipolazione del mercato).

Inoltre, la L. n. 62/2005 ha modificato l'art. 2637 c.c. (Aggiotaggio), eliminando il riferimento agli "strumenti finanziari quotati o non quotati" e introducendo l'espressione "strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato".

Successivamente, la L. 262/2005 ("sulla tutela del risparmio") è intervenuta sul trattamento sanzionatorio dei reati di abuso di informazioni privilegiate e di manipolazione del mercato, aggravando le pene dagli stessi previste.

Per comprendere il fenomeno del market abuse e la rilevanza penale delle relative fattispecie occorre, quindi, riferirsi alla figura dell'abuso di informazioni privilegiate, della manipolazione del mercato e dell'aggiotaggio.

Tali illeciti assumono rilevanza anche in relazione alla responsabilità amministrativa della società ex D.Lgs. n. 231/2001 che contempla, fra i reati-presupposto, l'abuso di informazioni privilegiate, la manipolazione del mercato (art. 25-sexies) e l'aggiotaggio (art. 25-ter, lett. r). Il presente contributo si propone, quindi, di offrire spunti di riflessione in ordine sia agli illeciti di market abuse, sia alle procedure finalizzate alla loro prevenzione, contenute nel modello organizzativo ex D.Lgs. n. 231/2001.

La Legge n. 147/2025 sull'intelligenza artificiale introduce specifiche circostanze aggravanti per i reati di aggiotaggio e di manipolazione del mercato quando i fatti sono commessi mediante l'impiego di sistemi di intelligenza artificiale.

Il reato di aggiotaggio si configura quando si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di società o gruppi

La pena prevista è da uno a cinque anni di reclusione

Con la Legge n.32 del 23 settembre 2025 la pena è della reclusione da due a sette anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale.

PROCEDURE PER PREVENIRE LA COMMISSIONE DEL REATO DI AGGIOTAGGIO

I Destinatari del Modello di Organizzazione Gestione e Controllo in occasione della divulgazione al pubblico di informazioni sono tenuti ad agire nel rispetto delle disposizioni di cui all'articolo 2637 c.c. e ad assicurare la veridicità, la completezza e la correttezza delle informazioni comunicate a terzi (quali ad esempio giornalisti e altri rappresentanti dei mezzi di comunicazione di massa o il pubblico in generale).

La Legge n. 147/2025 sull'intelligenza artificiale ha introdotto specifiche circostanze aggravanti per i reati di aggiotaggio e di manipolazione del mercato quando i fatti sono commessi mediante l'impiego di sistemi di intelligenza artificiale.

Con la Legge n.32 del 23 settembre 2025 la pena è stata portata alla reclusione da due a sette anni se il fatto è commesso mediante l'impiego di sistemi di intelligenza artificiale.

9 AREE A RISCHIO

In relazione ai reati e alle condotte criminose sopra esplicitate, le aree ritenute più specificatamente a rischio risultano essere le seguenti:

- predisposizione delle comunicazioni sociali riguardo alla situazione economica, finanziaria o patrimoniale, come per esempio bilancio e situazione semestrale;
- predisposizione di comunicazioni alle Autorità pubbliche di vigilanza;
- comunicazioni delle situazioni di conflitti d'interesse da parte dei componenti del Consiglio di Amministrazione;
- con specifico riguardo ai reati di corruzione tra privati le aree di attività che si espongono maggiormente al rischio di perpetrare condotte corruttive sono quelle dedite, di volta in volta, alla negoziazione per la stipula di contratti di fornitura di servizi ai clienti e alla relativa fase di erogazione.

10 PRINCIPI DI COMPORTAMENTO

La presente parte speciale prevede a carico dei destinatari, in considerazione delle diverse posizioni e obblighi che ciascuno assume nei confronti di IDRAGEST nell'ambito di espletamento delle attività considerate a rischio, l'obbligo di:

- evitare di porre in essere comportamenti tali da configurare i reati di cui all'art. 25-ter del D.Lgs. 231/01;
- evitare di porre in essere condotte che, se anche non costituenti reato, siano considerate ai margini di quanto previsto dalle fattispecie penali;
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e di regolamenti, nonché delle procedure interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche, al fine di fornire in generale un'informazione veritiera e appropriata sulla situazione economico e finanziaria di IDRAGEST;
- assicurare il regolare funzionamento di IDRAGEST e degli Organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione sociale;
- effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle autorità di controllo, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate.

PERCIÒ IN PARTICOLARE È FATTO DIVIETO DI:

- predisporre o comunicare dati falsi, o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, finanziaria e patrimoniale di IDRAGEST;
- omettere di comunicare dati ed informazioni richieste dalla normativa e dalle procedure in vigore riguardo alla situazione economica, finanziaria e patrimoniale di IDRAGEST;
- non attenersi ai principi e alle prescrizioni contenute nelle disposizioni legislative per la redazione dei bilanci di IDRAGEST;
- alterare o comunque non riportare in modo corretto i dati e le informazioni destinate alla stesura dei prospetti informativi;
- presentare i dati e le informazioni utilizzate in modo tale da fornire una rappresentazione non corretta e veritiera sulla situazione economica, finanziaria e patrimoniale di IDRAGEST nonché sull'evoluzione delle relative attività;
- tenere comportamenti che impediscano materialmente o siano comunque in grado di ostacolare lo svolgimento dell'attività di controllo della gestione sociale;

▪ porre in essere, in occasione dell'Assemblea, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione dell'attività assembleare;

▪ esporre nella documentazione trasmessa alle Autorità di vigilanza fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economico, finanziario e patrimoniale di IDRAGEST;

▪ porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità di pubblica vigilanza, anche in sede di ispezione come per esempio espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti;

▪ omettere di effettuare con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità in questione:

- le comunicazioni, periodiche e non, previste dalla legge e dalla normativa di settore;
- la trasmissione di dati e documenti previsti dalla normativa in vigore e/o specificatamente richieste dalle Autorità.

10.1 PRINCIPI PROCEDURALI SPECIFICI

Si indicano di seguito i principi procedurali che, in relazione ad ogni singola situazione delineata nelle Aree a rischio, i destinatari sono tenuti a rispettare e che, ove necessario, devono essere integrate da specifiche procedure interne oppure tempestivamente comunicate all'Organismo di Vigilanza:

▪ nell'attività di predisposizione delle comunicazioni ai soci e al pubblico in generale, contenente informazioni e dati sulla situazione economica, finanziaria o patrimoniale di IDRAGEST ed in particolare ai fini della formazione del bilancio, dovranno essere seguiti i principi dettati dalla normativa in vigore e con specifico riferimento ai presidi di antiriciclaggio e alle procedure di whistleblowing;

▪ nell'attività di predisposizione dei prospetti informativi relativi all'andamento di IDRAGEST dovranno essere svolti dei programmi formativi per tutti i soggetti coinvolti nell'attività, fornendo da un lato un adeguato supporto per svolgere l'attività richiesta e dall'altro lato rendendo gli stessi edotti relativamente alle fattispecie/ipotesi che siano in grado di integrare un illecito penale.

▪ nelle attività di trattamento, gestione e comunicazione verso l'esterno di notizie o dati riguardanti IDRAGEST, è fatto obbligo di attenersi a quanto previsto nelle procedure interne in materia di informazioni riservate o privilegiate e a quanto precisato in proposito dal Codice etico;

▪ nella predisposizione di comunicazioni alle Autorità di vigilanza occorrerà prestare particolare attenzione al rispetto:

- delle leggi e della normativa secondaria di settore concernenti le comunicazioni, periodiche e non, da inviare a tali Autorità;
- degli obblighi di trasmissione delle Autorità suddette di dati e di documenti previsti dalle norme in vigore ovvero richieste specificatamente dalle predette Autorità;
- degli obblighi di collaborazione da fornire nel corso di eventuali accertamenti ispettivi;

▪ con specifico riguardo all'obiettivo di scongiurare condotte corruttive è fatto divieto di:

- effettuare illecite elargizioni di denaro e comunque tali da influenzare l'indipendenza di giudizio o indurre ad assicurare un vantaggio per IDRAGEST;
- distribuire omaggi, regali o prestazioni di ogni natura, al di fuori di consolidate prassi aziendale (così come specificato nel Codice etico e nell'apposita procedura speciale);
- effettuare pagamenti in contanti o in natura, eccetto quelli relativi alla gestione della cassa interna e comunque entro i limiti previsti dalla presente procedura e dalla vigente normativa in materia di trasferimento di contanti. In particolare, dovrà comunque risultare da apposita documentazione la giustificazione della spesa e l'indicazione del destinatario.

11 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

Tutti i *Destinatari* coinvolti nella puntuale applicazione della presente procedura, dovranno segnare all'ODV:

- ogni situazione anomala;
- ogni situazione in contrasto con la presente procedura;
- ogni sospetto di riciclaggio o finanziamento del terrorismo, secondo le modalità definite nella sezione 5.6;
- ogni condotta posta in essere in violazione delle disposizioni del Modello e del Codice Etico.

LE FUNZIONI AZIENDALI ALL'UOPO PREPOSTE DOVRANNO COMUNICARE ALL'ODV:

- Mediante un report semestrale i pagamenti superiori ad euro 15.000,00;
- Mediante un report annuale, l'elenco dei conti correnti "*temporanei*" o inattivi da almeno 6 mesi, o comunque poco movimentati (ad es. ≤ 2 operazioni in un anno);

- tempestivamente, le operazioni effettuate per mezzo di strumenti di pagamento anomali e operazioni condotte in un Paese estero cosiddetto "*non collaborativo*", con espressa indicazione della motivazione economica per la quale è stata eseguita la predetta operazione;
- tempestivamente, qualsiasi condotta che possa integrare le fattispecie di cui al D.lgs.231/2001 e qualsivoglia condotta rilevante ai fini della presente procedura.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello. L'impedimento o l'ostacolo a tali attività di controllo può integrare una fattispecie di reato ai sensi dell'art. 2625 c.c.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda, adottata ai sensi del D.Lgs. 24/2023, la quale attua le previsioni di cui all'art. 6, co. 2-bis del D.Lgs. 231/2001.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

Sommario 2

1 OBIETTIVI E FUNZIONI DEL MODELLO 3

2 ACRONIMI AZIENDALI 3

3 RIFERIMENTI NORMATIVI 4

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA 5

5 LA DISCIPLINA DEL NUOVO CODICE DEGLI APPALTI PUBBLICI 5

5.1 CAUSE DI ESCLUSIONE AUTOMATICA 6

5.1.1 Cause di esclusione automatica 6

5.2 Cause di esclusione non automatica 6

5.3 ILLECITO PROFESSIONALE GRAVE 6

5.4 LE INTERAZIONI CON IL D.LGS. N. 231/2001 7

5.5 IL RUOLO DELLA RESTORATIVE COMPLIANCE 8

6 turbata liberta' degli incanti (ex art. 353 c.p.) e turbata liberta' del procedimento di scelta del contraente (ex art. 353 bis c.p.) 8

7 PRINCIPI GENERALI DI COMPORTAMENTO 10

7-BIS – USO DELL'IA NELLA PREDISPOSIZIONE DELL'OFFERTA E NELL'ESECUZIONE 11

7.1 VALUTAZIONE A PARTECIPARE ALLA GARA PUBBLICA 11

7.2 ESECUZIONE DEGLI APPALTI 12

7.3 FATTURAZIONE ATTIVA E CONTABILIZZAZIONE 13

8 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO 13

1 OBIETTIVI E FUNZIONI DEL MODELLO

Il presente Protocollo definisce i ruoli, le responsabilità operative, le attività di controllo e i principi di comportamento adottati da IDRAGEST S.r.l. in relazione alla scelta e gestione delle gare, nonché in relazione alla gestione dell'esecuzione degli appalti e dei contratti a favore degli enti pubblici e privati al fine di prevenire, nell'esecuzione di tale attività, la commissione degli illeciti previsti dal D.lgs. 231/2001, ed in particolare dagli artt. 24, 24-ter, 25 e 25-ter del medesimo Decreto.

Invero, lo scopo della presente procedura è quello di creare un "sistema di controllo" nella gestione dei rapporti con i clienti, definendo criteri che garantiscano una corretta e puntuale attività di riesame dei dati e documenti contrattuali, al fine di adeguare la struttura organizzativa dell'impresa al D.Lgs. 231/01, con particolare riferimento ai rischi connessi a: Corruzione e concussione, Truffa aggravata ai danni dello Stato e Reati in tema di erogazioni pubbliche.

Per tale ragione, in osservanza alla presente procedura, nonché alla procedura PMOG01 relativa alla prevenzione dei reati contro la P.A., le figure all'uopo preposte sono tenute, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, a fornire alla Pubblica Amministrazione informazioni veritiere o anche attraverso strumenti informatici o telematici idonee a non ostacolare la propria o altrui identificazione

LA PROCEDURA È DIRETTA, IN PARTICOLARE, A PREVENIRE:

1. reati contro la Pubblica Amministrazione;
2. reati in materia di turbata libertà degli incanti e del procedimento di scelta del contraente ai sensi degli artt. 353 e 353-bis c.p.;
3. reati informatici e condotte connesse all'uso improprio di strumenti digitali, sistemi IA, cloud e basi dati, in coordinamento con la PMOG 08;
4. delitti in materia di violazione del diritto d'autore, banche dati, scraping e uso illecito di opere o contenuti protetti, in coordinamento con la PMOG 11;
5. rischi connessi all'uso di sistemi di intelligenza artificiale nella predisposizione delle offerte e nell'esecuzione di prestazioni, in coordinamento con la PMOG 16 e la Policy IA;

La procedura persegue altresì finalità di tracciabilità, trasparenza, verificabilità delle decisioni, separazione dei ruoli, documentazione dei rapporti con le stazioni appaltanti e presidio dei flussi informativi verso l'Organismo di Vigilanza.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA

RSGQ	Responsabile Sistema di Gestione Qualità
RAM	Responsabile Amministrazione - Risorse Umane
RTEC	Responsabile Tecnico
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RFAM	Responsabile Facility Management
RPROG	Responsabile Progettazione
RSCM	Responsabile singola commessa
RATTR	Responsabile Attrezzature e Mezzi
PROG	Programmatori
REC	Responsabile Esterno Contabilità
RIA	Responsabile IA

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- D.Lgs. 8 giugno 2001 n. 231 e s.m.i.;
- D.Lgs. 31 marzo 2023 n. 36 e s.m.i.;
- Codice Etico e Modello di Organizzazione, Gestione e Controllo adottati dalla Società;
- Regolamento (UE) 2024/1689 (AI Act);
- Delibera ANAC n. 148 del 1° aprile 2026, recante aggiornamento del Bando tipo n. 1-2023 in materia di dichiarazioni sull'uso dell'intelligenza artificiale;
- Regolamento (UE) 2016/679 e D.Lgs. 196/2003, per i profili di trattamento dei dati personali;
- D.Lgs. 4 settembre 2024 n. 138 e Regolamento di esecuzione (UE) 2024/2690, per i profili di cybersicurezza e gestione del rischio digitale;
- Legge 22 aprile 1941 n. 633 e successive modificazioni, con particolare riguardo agli artt. 70-quater, 171 e seguenti;
- art. 25-novies D.Lgs. 231/2001;
- art. 612-quater c.p.;

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

La presente procedura deve essere osservata da tutte le Funzioni Aziendali all'uopo incaricate di scegliere e gestire le gare alle quali partecipare, nonché incaricate della gestione dell'esecuzione degli appalti e dei contratti a favore di enti pubblici e privati.

DUNQUE, LA PRESENTE PROCEDURA RIGUARDA:

- partecipazione a tutti i tipi di gare ed appalti pubblici;
- partecipazione a richieste d'offerta private;
- partecipazione ed esecuzione dell'appalto come operatore economico singolo , in A.T.I., tramite contratto di Rete, in consorzio, ovvero in subappalto (a titolo esemplificativo, per l'attività di controllo della progettazione dei documenti e dei dati; provvedere all'approvvigionamento; esecuzione delle prove, dei controlli e dei collaudi; controllo delle apparecchiature per prova, misurazione e collaudo; controllo del prodotto; controllo delle registrazioni della qualità; esecuzione di *audit*; gestione dei documenti di gara, dei contratti e conservazione della relativa documentazione);
- partecipazione ed esecuzione dei contratti a favore di enti privati.

Il principale responsabile della procedura è l'Organo amministrativo e, in via sussidiaria, il RCOM/APVG e il RTEC.

5 LA DISCIPLINA DEL NUOVO CODICE DEGLI APPALTI PUBBLICI

La partecipazione alle gare pubbliche e la successiva esecuzione del contratto devono avvenire nel rispetto del D.Lgs. 36/2023, dei principi di legalità, trasparenza, tracciabilità, correttezza professionale e affidabilità dell'operatore economico, nonché dei presidi previsti dal Modello 231 della Società.

NELLA VALUTAZIONE DELLA PARTECIPAZIONE ALLA GARA E NELLA PREDISPOSIZIONE DELLA DOCUMENTAZIONE, LA SOCIETÀ TIENE CONTO:

1. delle cause di esclusione automatica e non automatica;
2. dell'illecito professionale grave;
3. della necessità di garantire correttezza, completezza e veridicità delle dichiarazioni rese;
4. della documentazione relativa a eventuali misure correttive o di restorative compliance.

Per le gare aventi ad oggetto servizi intellettuali, la Società applica altresì le regole interne e dichiarative relative all'uso di sistemi di IA, assicurando la prevalenza del lavoro intellettuale umano, il controllo e la verifica dei risultati, la validazione umana degli output rilevanti e la conformità alla normativa su protezione dati, cybersicurezza e proprietà intellettuale.

5.1 CAUSE DI ESCLUSIONE AUTOMATICA

5.1.1 CAUSE DI ESCLUSIONE AUTOMATICA

La Società verifica preventivamente, con il supporto delle funzioni competenti, l'assenza di cause di esclusione automatica rilevanti ai sensi del D.Lgs. 36/2023, nonché la completezza e veridicità delle dichiarazioni da rendere in gara.

Le verifiche devono essere estese anche ai soggetti rilevanti ai fini della normativa di gara, ai partner di ATI/consorzi e, ove necessario, ai subappaltatori e soggetti ausiliari, con raccolta e conservazione della documentazione giustificativa nel fascicolo di gara.

5.2 CAUSE DI ESCLUSIONE NON AUTOMATICA

La Società valuta, prima della partecipazione, eventuali fatti o situazioni suscettibili di integrare cause di esclusione non automatica o gravi illeciti professionali, adottando, se del caso, misure correttive adeguate e documentate, idonee a dimostrare affidabilità e continuità dei presidi organizzativi.

TALE VALUTAZIONE DEVE CONSIDERARE ANCHE:

1. contestazioni significative relative all'esecuzione di precedenti contratti;
2. violazioni rilevanti del Modello 231 o del Codice Etico;
3. violazioni documentate in materia di sicurezza informatica, protezione dati, diritto d'autore, banche dati o uso dell'IA, quando incidenti sull'affidabilità professionale della Società.

5.3 ILLECITO PROFESSIONALE GRAVE

Nella valutazione dell'illecito professionale grave, la Società adotta un criterio prudenziale e documentato, verificando ogni fatto, contestazione, provvedimento o anomalia che possa incidere sull'integrità, affidabilità o correttezza professionale dell'operatore economico, ai fini della partecipazione alla gara o della prosecuzione del rapporto contrattuale.

AI FINI INTERNI, COSTITUISCONO ELEMENTI DA VALUTARE CON PARTICOLARE ATTENZIONE ANCHE:

1. condotte rilevanti ai sensi degli artt. 353 e 353-bis c.p.;
2. violazioni gravi in materia di tracciabilità, rapporti con la P.A. e veridicità delle dichiarazioni;
3. utilizzo improprio di strumenti informatici o sistemi IA nelle gare o nell'esecuzione;
4. violazioni accertate o significative in materia di diritto d'autore, licenze, banche dati, scraping o data extraction.

5.4 LE INTERAZIONI CON IL D.LGS. N. 231/2001

Le previsioni di cui sopra collegano espressamente l'esclusione degli operatori economici al sistema della responsabilità amministrativa degli enti.

IN PARTICOLARE:

• esclusione automatica nel caso di condanna dell'ente, ai sensi del D.Lgs. n. 231/2001, per uno dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti;

• esclusione automatica nel caso di condanna penale delle persone fisiche legate all'ente (art. 94, comma 3) per uno dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti;

• esclusione automatica degli enti già destinatari della sanzione interdittiva di cui all'art. 9, comma 2, lett. c) del D.Lgs. n. 231/2001 («il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio») o di altra sanzione che comporta il divieto di contrarre con la pubblica amministrazione (senza vincolo alcuno, in questo caso, all'elenco dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti);

• esclusione non automatica dell'ente di cui si accerti la commissione di un illecito professionale grave, desumibile – fra gli altri motivi – dalla commissione o dalla mera contestazione di un qualsiasi reato-presupposto di cui al D.Lgs. n. 231/2001.

Quest'ultima previsione (art. 98, comma 3, lett. h), in particolare, consente l'esclusione dell'operatore economico a vario titolo coinvolto in una indagine per un reato che fonda la responsabilità amministrativa degli enti, ancorché in fase di indagini ovvero riferibile alle persone fisiche collegate all'ente. Il comma 6 dell'articolo, infatti, stabilisce che costituiscono mezzi di prova adeguati alla dimostrazione dell'illecito professionale legato alle violazioni 231 le sentenze e i decreti penali di condanna, nonché i provvedimenti cautelari personali o reali.

Come già segnalato da diverse organizzazioni (in primis, l'Unione delle Camere Penali Italiane e l'Associazione dei Componenti degli Organismi di Vigilanza – AODV231), la nuova disciplina si pone in frizione con i principi fondamentali della materia penale (presunzione di non colpevolezza ex art. 27, comma 2°, Cost.), con la libertà di iniziativa economica privata (art. 41 Cost.) e con taluni degli stessi principi ispiratori del Codice degli appalti.

Si consideri, inoltre, che il riferimento all'intero decalogo dei reati contemplati dal Decreto 231 non tiene conto della incessante moltiplicazione delle fattispecie suscettibili di dar luogo alla responsabilità da reato delle società, molte delle quali non costituiscono nemmeno espressione della c.d. criminalità d'impresa,

men che meno della devianza "politico-amministrativa" cui si dovrebbero riferire le esclusioni dalle gare pubbliche.

5.5 IL RUOLO DELLA RESTORATIVE COMPLIANCE

Il comma 4 dell'art. 98 prevede che, ai fini della valutazione di gravità dell'illecito professionale, si tenga conto del bene giuridico e dell'entità della lesione inferta dalla condotta e del tempo trascorso dalla violazione, «*anche in relazione a modifiche intervenute nel frattempo nell'organizzazione dell'impresa*». Ciò significa che le stazioni appaltanti, pur in presenza degli elementi che integrano, sul piano oggettivo, un illecito professionale, potranno valutare – nell'esercizio della discrezionalità amministrativa – le azioni correttive intraprese dall'operatore economico in un tempo successivo alla contestazione o alla condanna per un illecito 231, al fine di stabilire se la riorganizzazione aziendale è tale da elidere la gravità dell'illecito e/o da riabilitare l'affidabilità dell'ente.

Il riferimento, anche se non espresso, è, dunque, alla *restorative compliance*, ossia alla riorganizzazione intrapresa dall'ente successivamente alla commissione dell'illecito. L'adozione, l'effettiva attuazione e la "correzione" di un Modello di organizzazione, gestione e controllo, già rilevanti sul fronte "premiale" delle condotte riparatorie ex D.Lgs. n. 231/2001, divengono dunque strumenti di riabilitazione dell'ente, anche ai fini della partecipazione alle gare pubbliche, ovvero per rimediare alla sua potenziale esclusione.

La previsione conferma, in definitiva, il ruolo sempre più centrale della *compliance* (non solo *ex ante,* ma anche *ex post*) nel sistema in senso lato sanzionatorio delle persone giuridiche, nell'ambito del quale spiccano le previsioni del D.Lgs. n. 231/2001 e le misure interdittive e di prevenzione di cui D.Lgs. n. 159/2011 (c.d. codice antimafia), in ispecie per le ripercussioni che determinano sulla "vita" pubblica e sociale dell'ente e nei rapporti con la p.a.

6 TURBATA LIBERTA' DEGLI INCANTI (EX ART. 353 C.P.) E TURBATA LIBERTA' DEL PROCEDIMENTO DI SCELTA DEL CONTRAENTE (EX ART. 353 BIS C.P.)

Il 9 ottobre del 2023 è stata pubblicata in Gazzetta Ufficiale la Legge n. 137/2023 che ha convertito in legge, con modificazioni, il D.L. 10 agosto 2023 n. 105 (cd. Decreto Giustizia).

La citata Legge di conversione ha introdotto importanti modifiche al testo originario del Decreto Giustizia e le principali novità riguardano proprio l'introduzione di nuovi delitti nel catalogo dei reati presupposto ex D.Lgs. n. 231/2001 intervenendo sugli artt. 24 e 25-octies.

In particolare, La Legge di conversione ha introdotto all'art. 24 le fattispecie di reato di turbata libertà degli incanti (art. 353 c.p.) e turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.).

L'art. 353 c.p. punisce chiunque, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, impedisca o turbi una gara nei pubblici incanti o nelle licitazioni private per conto della Pubblica Amministrazione, ovvero ne allontani gli offerenti.

La disposizione si applica anche nel caso di licitazioni private per conto di privati, dirette da un pubblico ufficiale o da persona legalmente autorizzata.

L'art. 353-bis c.p. sanziona, invece, chiunque, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, turbi il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della Pubblica Amministrazione.

Entrambe le fattispecie, quindi, sono volte a tutelare il buon andamento della P.A. rispetto a condotte fraudolente che impediscano o alterino la regolare procedura di una gara (art. 353 c.p.), o, ancor prima, il procedimento che porta alla realizzazione di un bando (art. 353-bis c.p.).

PERTANTO, TITOLO ESEMPLIFICATIVO, I DESTINATARI DELLA PRESENTE PROCEDURA SI DEVONO ASTENERE:

- ✓ dal promettere ad un proprio concorrente lavori futuri, al fine di impedirne la partecipazione a una gara di appalto, poiché ciò configurerebbe il reato di cui all'art. 353-bis c.p.;
- ✓ dal firmare un accordo clandestino con un pubblico ufficiale finalizzato a redigere un bando di gara con requisiti talmente stringenti da predeterminare l'aggiudicazione poiché ciò integrerebbe il reato di cui all'art. 353 c.p.;
- ✓ dal porre in essere qualsiasi atto idoneo ad influenzare l'andamento della gara. Sul punto si rileva che la recentissima Cass., VI, ord. n. 41379/2023, ha rimesso alle SS.UU. la questione se sia configurabile, oltre al reato di cui all'art. 353 c.p., anche quello di estorsione nella condotta di chi, con violenza o minaccia, allontani gli offerenti da una gara nei pubblici incanti o nelle licitazioni private. Con la citata sentenza la Corte di Cassazione ha precisato che "*il delitto di turbata libertà della gara si configura sia nel caso di danno effettivo sia nel caso di danno mediato e potenziale, non occorrendo l'effettivo conseguimento del risultato, perseguito dagli autori dell'illecito, ma la semplice idoneità degli atti ad influenzare l'andamento della gara (…) Si è precisato che, ai fini dell'integrazione del reato di cui all'art. 353 cod. pen., occorre che tale idoneità si sia in qualche modo manifestata, nel senso che le condotte dell'agente devono essersi tradotte in una concreta minaccia, ossia che abbiano in qualche modo cagionato la verificazione del citato evento di pericolo, determinando un rischio di alterazione di quello che, diversamente, sarebbe stato il corso degli incanti.*

L'Ente nel cui interesse e/o a cui vantaggio risulti commesso uno dei reati appena descritti potrà essere condannato a pagare una sanzione amministrativa pecuniaria fino a 500 quote (da un minimo di 25.800 euro ad un massimo di 774.500 euro).

L'art. 24, comma 2, D.Lgs. n. 231/2001 prevede inoltre la sanzione pecuniaria da 200 a 600 quote (da 51.600 a 929.400 euro) nel caso in cui l'ente abbia conseguito un profitto di rilevante entità o sia derivato un danno di particolare gravità.

In aggiunta alle sanzioni pecuniarie, troveranno applicazione le seguenti sanzioni interdittive (art. 9, comma 2, lett. c), d) ed e), D.Lgs. n. 231/2001):

- divieto di contrattare con la Pubblica Amministrazione;
- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- divieto di pubblicizzare beni o servizi;
- in generale, al fine di evitare la configurazione del reato di cui all'art. 353 bis c.p. è vietata la commissione di comportamenti fraudolenti volti a falsare il risultato di una procedura ad evidenza pubblica; tali comportamenti possono realizzarsi mediante l'uso di violenza, minaccia, doni, promesse, collusione od altri mezzi fraudolenti, impedendo o turbando la gara espletata da Pubbliche Amministrazioni o allontanando gli offerenti.

dunque, sia il reato di "Turbata libertà degli incanti" (art. 353 c.p.) sia il reato di "Turbata libertà del procedimento di scelta del contraente" (art. 353 bis c.p) sono volti a tutelare il corretto espletamento delle procedure ad evidenza pubblica, nelle varie fasi, i procedurali (dalla predisposizione del bando fino allo svolgimento della procedura ad evidenza pubblica).

7 PRINCIPI GENERALI DI COMPORTAMENTO

Tutti i destinatari della presente procedura sono tenuti a operare secondo principi di legalità, correttezza, buona fede, trasparenza, tracciabilità, segregazione dei compiti, documentazione delle attività e rispetto delle competenze autorizzative interne.

NELLA GESTIONE DELLE GARE E DEI CONTRATTI È FATTO DIVIETO DI:

1. promettere, offrire o corrispondere utilità indebite;

2. intrattenere rapporti non autorizzati o non tracciati con stazioni appaltanti, funzionari pubblici o soggetti privati coinvolti;

3. produrre o utilizzare documenti incompleti, non veritieri, non verificati o non autorizzati;

4. utilizzare sistemi IA diversi da quelli autorizzati dalla Società o usare output IA senza validazione umana quando rilevanti ai fini dell'offerta o dell'esecuzione;

5. inserire nei prompt dati riservati, personali non anonimizzati, documentazione di gara riservata, credenziali, segreti commerciali o dati tecnici dei clienti in violazione delle regole aziendali;

6. usare software, banche dati, cartografie, testi, codice o altri materiali privi di adeguato titolo di utilizzo o in violazione delle licenze applicabili.

7-BIS – USO DELL'IA NELLA PREDISPOSIZIONE DELL'OFFERTA E NELL'ESECUZIONE

L'utilizzo di sistemi di IA nella predisposizione dell'offerta o nell'esecuzione del contratto è consentito esclusivamente nel rispetto della PMOG 16 e della Policy IA aziendale.

Per i servizi di natura intellettuale, la Società assicura, in conformità alla Delibera ANAC n. 148/2026, la prevalenza del lavoro intellettuale umano, il controllo e la verifica dei risultati ottenuti e la corretta dichiarazione, in sede di domanda, dell'eventuale uso di sistemi di IA nella predisposizione dell'offerta tecnica e nell'esecuzione della prestazione.

È VIETATO:

1. utilizzare output IA come elaborati finali senza preventiva validazione umana;

2. impiegare IA per generare automaticamente dichiarazioni, certificazioni o documenti giuridicamente rilevanti senza verifica e assunzione di responsabilità da parte del soggetto competente;

3. utilizzare sistemi non autorizzati o non tracciati;

4. omettere o rendere in modo non veritiero le dichiarazioni richieste in gara in ordine all'uso dell'IA.

La documentazione relativa all'uso dell'IA in gara o in esecuzione deve essere inserita nel fascicolo digitale di gara/commessa, comprensiva di dichiarazioni, checklist, log rilevanti e attestazioni di validazione.

7.1 VALUTAZIONE A PARTECIPARE ALLA GARA PUBBLICA

IDRAGEST viene a conoscenza di gare d'appalto a cui partecipare o attraverso specifici inviti da parte di organismi committenti (di regola operanti con sistemi di qualifica – albo fornitori) ovvero tramite segnalazioni di siti specializzati.

La partecipazione di IDRAGEST a gare di appalto pubblico viene in prima istanza valutata dal RAM, dal RCOM/APVG e/o dal Consiglio di Amministrazione, previa verifica dei requisiti necessari e della documentazione (capitolati, specifiche tecniche, ecc.) inerente la partecipazione alla gara, anche valutando la possibilità di concorrere in ATI o con le imprese facenti parte del contratto di rete cui appartiene

IDRAGEST, nonché valutando la possibilità di partecipare attraverso eventuali associazioni temporanee di imprese o altre forse di partecipazione consentite dalle disposizioni di legge in materia.

La preparazione alla gara comporta, preliminarmente, la puntuale osservanza del disciplinare di gara, nonchè la predisposizione della documentazione richiesta dal bando di gara.

In caso di esito di aggiudicazione, occorrerà provvedere alla preparazione di tutti i documenti richiesti dall'amministrazione per la firma del contratto, comprese polizze (fidejussorie definitive e la polizza per la responsabilità civile verso i terzi RCT, ecc.).

Una volta firmato e riesaminato il contratto predisposto dalle stazioni appaltanti, si provvederà all'apertura della commessa.

7.2 ESECUZIONE DEGLI APPALTI

Ai fini della prevenzione dei reati di cui al D.lgs. 231/2001 ed indipendentemente dalla forma di partecipazione (ad es. operatore economico singolo, o partecipazione in A.T.I., contratto di Rete, consorzio, subappalto, con enti privati ecc.) IDRAGEST assicura il rispetto delle seguenti prescrizioni:

- eseguire la fornitura a regola d'arte, secondo l'ordinaria diligenza, astenendosi da condotte illecite o lesive dell'interesse del committente lecito e contrattualmente pattuito;
- approntare e mantenere, per ogni commessa, un fascicolo digitale caricato nell'apposito archivio informatico all'uopo predisposto nell'apposita piattaforma digitale di condivisione, contenente una "scheda di apertura commessa", l'indicazione del responsabile della commessa, il contratto, la documentazione inerente l'acquisto dei materiali, il piano di fornitura, la documentazione concernente la costituzione dell'A.T.I., o la partecipazione tramite contratto di Rete o consorzio, ovvero gli eventuali documenti relativi al subappalto diversi dal contratto, con le rispettive competenze delle partecipanti, la documentazione concernente le comunicazioni tra le aziende partecipanti all'A.T.I. o al consorzio o al contratto di Rete, ovvero con l'appaltatore principale;
- i contatti con funzionari di enti pubblici potranno avvenire solo per motivi inerenti alle gare cui la società partecipa o intende partecipare e solo attraverso il PRES, o il soggetto da quest'ultimo incaricato: dovrà essere predisposto un elenco con indicazione di data, motivazione del contatto e soggetto interlocutore; il suddetto elenco, relativo ai contatti intercorsi con i funzionari degli enti pubblici, verrà caricato e tenuto nell'archivio informatico all'uopo predisposto nella piattaforma digitale di condivisione.

Lotta alla corruzione

i) NEI RAPPORTI CON LA P.A. IDRAGEST:

- vieta qualsivoglia forma di corruzione, sia attiva, sia passiva;
- vieta ai soggetti che agiscono per conto della Società, di autorizzare, sollecitare, offrire, promettere di concedere, offrire, direttamente o indirettamente, pagamenti o oggetti di valore a funzionari pubblici con l'intento di persuadere o influenzare detti funzionari ad agire secondo modalità che possano agevolare la Società ad ottenere, promuovere, mantenere le proprie attività o ad assicurarsi vantaggi illegittimi o indebiti nello svolgimento delle stesse;

ii) NEI RAPPORTI CON I PRIVATI IDRAGEST:

- Vieta di offrire, promettere, concedere, sollecitare o accettare, sia direttamente che indirettamente, qualsivoglia vantaggio indebito monetario o di altra natura, a/da qualsiasi soggetto che dirige o lavora, indipendentemente dalla posizione ricoperta, per un altro ente privato, al fine di indurlo ad agire o ad astenersi dall'agire in violazione dei suoi doveri;
- Vieta ai soggetti che agiscono per conto e nell'interesse della società, di offrire o corrispondere a soggetti terzi, omaggi, trattamenti di favore e/o regalie di valore più che simbolico e, comunque, estranei alle normali relazioni di cortesia, nell'intento di favorire in modo illecito la Società; i medesimi soggetti non possono accettare da terzi omaggi, trattamenti di favore e/o regalie di valore più che simbolico.

7.3 FATTURAZIONE ATTIVA E CONTABILIZZAZIONE

Il monitoraggio relativo allo stato di avanzamento della commessa è a cura del responsabile di commessa all'uopo incaricato, il quale - nei momenti stabiliti contrattualmente - deve verificare che l'importo complessivamente fatturato corrisponda a quanto stabilito nel contratto, segnalando eventuali differenze al PRES e trasmettendone copia alla Funzione preposta alla contabilizzazione.

La Funzione preposta alla contabilizzazione registrerà in contabilità gli incassi e mensilmente effettuerà la riconciliazione bancaria dei conti correnti attestando l'effettività di incassi e pagamenti.

L'emissione di note di credito dovrà essere autorizzata dal PRES o da altro soggetto all'uopo incaricato.

8 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

OGNI FUNZIONE AZIENDALE INTERESSATA DEVE INFORMARE L'ORGANISMO DI VIGILANZA, PERIODICAMENTE, E COMUNQUE CON FREQUENZA ALMENO ANNUALE, ATTRAVERSO UNO SPECIFICO REPORT, SUGLI ASPETTI SIGNIFICATIVI AFFERENTI LE EVENTUALI DIVERSE ATTIVITÀ DEL PROCESSO DI PROPRIA COMPETENZA, IN PARTICOLARE PER QUANTO ATTIENE A:

• l'eventuale partecipazione a procedure ad evidenza pubblica;

• l'andamento generale dei prezzi ed eventuali ribassi di rilievo praticati dall'azienda rispetto alla concorrenza, al di fuori della normale griglia prezzi e condizioni;

• comunicare all'Organismo di Vigilanza ogni eventuale deroga alle procedure, adottata in caso di emergenza o di impossibilità temporanea di attuazione, indicando la motivazione, e ogni anomalia significativa riscontrata;

• qualunque evento e/o comportamento anomalo rilevato nell'esecuzione degli appalti;

• qualsiasi violazione della presente procedura;

• qualunque altra anomalia riscontrata in fase di contrattualizzazione ed esecuzione degli appalti;

• la violazione dei divieti di cui al punto 5.2 della presente procedura;

• qualunque violazione del Modello e del Codice Etico.

DEVONO ESSERE COMUNICATI TEMPESTIVAMENTE ALL'ODV, OLTRE AL REPORT PERIODICO PREVISTO DALLA PROCEDURA, ALMENO I SEGUENTI EVENTI:

1. anomalie o criticità nella partecipazione a gare pubbliche o private;
2. contestazioni rilevanti da parte della stazione appaltante o del cliente;
3. sospetti o accertate violazioni degli artt. 353 e 353-bis c.p.;
4. utilizzo non conforme di sistemi IA nella predisposizione dell'offerta o nell'esecuzione del contratto;
5. omissioni o irregolarità nelle dichiarazioni ANAC sull'uso dell'IA;
6. incidenti informatici, accessi abusivi, fughe di dati, anomalie nei log o violazioni delle misure cyber con impatto su gara o commessa;
7. violazioni in materia di diritto d'autore, licenze, scraping, data extraction, deepfake o uso di contenuti non leciti;
8. ogni ulteriore fatto suscettibile di incidere sull'affidabilità professionale della Società o sull'efficacia del Modello 231.

La documentazione rilevante deve essere conservata nel fascicolo digitale di gara o commessa e resa accessibile all'OdV.

I Destinatari devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto su apposita piattaforma informatica – tutta la documentazione necessaria.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV, IN PARTICOLARE, PUÒ:

- visionare tutta la documentazione;
- verificare il puntuale rispetto delle disposizioni previste dalla presente procedura, dal Codice Etico, dal Modello e da tutte le disposizioni in materia.

Tutte le Funzioni Aziendali coinvolte hanno la responsabilità di osservare e far osservare il contenuto della presente procedura.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

Sommario

1 OBIETTIVI E FUNZIONE DEL MODELLO 3
2 ACRONIMI AZIENDALI 4
3 RIFERIMENTI NORMATIVI 4
4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA 4
5 PRINCIPI DI COMPORTAMENTO 4
Le Funzioni Aziendali interessate sono tenute a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo 7
5.1 L'ASSUNZIONE 7
5.2 IL PAGAMENTO DEL SALARIO MENSILE E LA GESTIONE DI RIMBORSI SPESE 7
5.3 L'ADOZIONE DEL MODELLO E IL SISTEMA SANZIONATORIO 8
5.4. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE 8
5.4.1 Digitalizzazione delle procedure di ingresso e assunzione 9
5.4.2. Presidi di Controllo Preventivo e Verifica preventiva del titolo di soggiorno 10
5.4.3 Controlli Operativi e Tracciabilità 10
5.5 PERMESSO DI SOGGIORNO PER GLI STRANIERI VITTIME DI INTERMEDIAZIONE ILLECITA E SFRUTTAMENTO DEL LAVORO 11
5.6 LE ATTIVITÀ SENSIBILI RELATIVE AI REATI DI IMPIEGO IRREGOLARE DI LAVORATORI STRANIERI PRIVI DEL PERMESSO DI SOGGIORNO 13
5.7 LA TRACCIABILITÀ DELLE PRESENZE 14
5.8 FORMAZIONE 14
6 GESTIONE DEI TRATTAMENTI PREVIDENZIALI E ASSISTENZIALI DEL PERSONALE 15
7 LA GESTIONE DEGLI OMAGGI 15
8 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO 15

1 OBIETTIVI E FUNZIONE DEL MODELLO

Il presente protocollo si applica a tutte le Funzioni Aziendali di IDRAGEST coinvolte nella gestione del processo di selezione e assunzione del personale.

Il processo potrebbe costituire una delle modalità strumentali attraverso cui commettere i reati di "Corruzione contro la Pubblica Amministrazione" nelle loro varie tipologie, "Induzione indebita a dare o promettere utilità", "Traffico di influenze illecite", nonché dei reati di "Corruzione tra privati" e "Istigazione alla corruzione tra privati".

Una gestione non trasparente del processo di selezione ed assunzione del personale, potrebbe, infatti, consentire la commissione di tali reati attraverso la promessa di assunzione verso rappresentanti della Pubblica Amministrazione, e/o esponenti apicali, e/o persone loro subordinate di società o enti controparti o in relazione con la Società, o soggetti da questi indicati, concessa al fine di influenzarne l'indipendenza di giudizio o di assicurare un qualsivoglia vantaggio per IDRAGEST.

Nell'ipotesi di assunzione di soggetti facenti parti di Paesi Terzi, IDRAGEST con la presente procedura ha fissato i principi finalizzati a prevenire il rischio della commissione del reato di "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

DESCRIZIONE DEL PROCESSO

Il processo di selezione e assunzione si articola nelle seguenti fasi:

• SELEZIONE DEL PERSONALE:

1) analisi e richiesta di nuove assunzioni;

2) definizione del profilo del candidato;

3) reclutamento dei candidati;

4) effettuazione del processo selettivo;

5) individuazione dei candidati.

• FORMALIZZAZIONE DELL'ASSUNZIONE.

Resta nelle competenze delle Funzioni Aziendali l'istruttoria relativa alla selezione ed assunzione di personale specialistico altamente qualificato per l'espletamento delle attività aziendali, ovvero di personale assunto in somministrazione per l'espletamento di specifiche commesse.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RSGQ	Responsabile Sistema di Gestione Qualità
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RTEC	Responsabile Tecnico
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RFAM	Responsabile Facility Management
RPROG	Progettazione
RSCM	Responsabile singola commessa
RATTR	Responsabile Attrezzature e Mezzi
PROG	Programmatori
CDL	Consulente del lavoro
REC	Responsabile Esterno Contabilità

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di IDRAGEST S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

Come su esposto al punto 1), la presente procedura si applica a tutte le Funzioni Aziendali coinvolte nella selezione, assunzione e gestione del personale, le quali dovranno verificare le competenze professionali richieste dalla Società.

Rientrano, dunque, nel campo di applicazione della procedura di selezione del personale dipendente il RAM/RRU e il PRES.

5 PRINCIPI DI COMPORTAMENTO

Le Funzioni Aziendali, a qualsiasi titolo coinvolte nella gestione del processo di selezione e assunzione del personale, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di

legge esistenti in materia, la normativa interna, nonché eventualmente le eventuali previsioni del Codice Etico e del Codice Disciplinare.

IN PARTICOLARE:

- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta al PRES e all'Organismo di Vigilanza;
- competenza, professionalità ed esperienza in relazione al ruolo per il quale avviene l'assunzione.

Le Funzioni Aziendali che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella selezione, assunzione e gestione del personale (anche in somministrazione ed anche straniero non comunitario) devono:

- operare nel rispetto del criterio di meritocrazia in relazione alle reali esigenze della società;
- garantire l'esistenza della documentazione attestante il corretto svolgimento delle procedure di selezione e assunzione;
- assicurare che la definizione delle condizioni economiche sia coerente con la posizione ricoperta dal candidato e le responsabilità/compiti assegnati;
- garantire che l'assunzione del personale avvenga sulla base di regolari contratti di lavoro, non essendo ammessa alcuna forma di rapporto lavorativo non conforme o comunque elusiva delle disposizioni normative vigenti;
- dimostrare l'impiego di lavoratori stranieri con valido permesso di soggiorno e monitorarne l'effettivo rinnovo, secondo i termini di legge;
- curare l'archiviazione di tutta la documentazione prodotta/ricevuta con riferimento alle attività propedeutiche e conseguenti alla presentazione della domanda di nulla osta, all'assunzione di lavoratori stranieri residenti all'estero;
- richiedere a ciascun dipendente, prima dell'assunzione, di produrre il casellario giudiziario ed il certificato dei carichi pendenti in corso di validità.

Le Funzioni Aziendali che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella selezione, assunzione e gestione del personale (anche straniero non comunitario) non possono:

- operare secondo logiche di favoritismo e/o pratiche discriminatorie;
- rendere promesse di assunzione e/o di avanzamento di carriera a risorse vicine a funzionari pubblici e a soggetti privati, qualora non venga rispettato il principio della meritocrazia;
- assumere personale, anche per contratti temporanei, senza il rispetto delle normative vigenti (ad esempio in termini di contributi previdenziali ed assistenziali, permessi di soggiorno, etc.);

- assumere o promettere l'assunzione nella società di impiegati della Pubblica Amministrazione (o loro parenti, affini, amici, etc.) o soggetti privati, che abbiano partecipato personalmente e attivamente ad una trattativa d'affari pubblica o privata, ovvero che abbiano partecipato, anche individualmente, a processi autorizzativi della Pubblica Amministrazione o ad atti ispettivi, nei confronti della Società, qualora non venga rispettato il principio della meritocrazia;
- impiegare lavoratori stranieri del tutto privi di permesso di soggiorno o con un permesso annullato, revocato o scaduto, per il quale non sia stata presentata domanda di rinnovo, documentata dalla relativa ricevuta postale;
- assumere un cittadino straniero non comunitario in Italia per motivi di turismo, anche se regolarmente munito della prescritta dichiarazione di presenza;
- fare ricorso, in qualsiasi forma, al lavoro minorile;
- assumere o promettere l'assunzione di soggetti, al fine di favorire o recare vantaggio ad organizzazioni criminali, ed in particolare ad associazioni di tipo mafioso e/o ad associazioni con finalità di terrorismo.

QUALORA IL PROCESSO DI ASSUNZIONE RIGUARDI:

1) personale diversamente abile, il reclutamento dei candidati avverrà nell'ambito delle liste di soggetti appartenenti alle categorie protette, da richiedere al competente Ufficio del Lavoro;

2) lavoratori stranieri, il processo dovrà garantire il rispetto delle leggi sull'immigrazione del Paese ove è sita l'unità organizzativa di destinazione e la verifica del possesso, per tutta la durata del rapporto di lavoro, dei permessi di soggiorno, ove prescritti;

3) ex dipendenti pubblici, il processo dovrà garantire il rispetto dei divieti di legge.

- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo di selezione e assunzione del personale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- la corresponsione di onorari o compensi a collaboratori o consulenti esterni eventualmente coinvolti è soggetta ad un preventivo che dovrà essere sottoposto al CDA per valutare la qualità della prestazione e la conseguente congruità del corrispettivo richiesto; in ogni caso non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- promettere o dare seguito – anche a mezzo di intermediari - a richieste di assunzione in favore di rappresentanti/esponenti della Pubblica Amministrazione ovvero di soggetti da questi indicati, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio a IDRAGEST;
- promettere o dare seguito a richieste di assunzioni di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con IDRAGEST, ovvero di soggetti da questi indicati, al fine di favorire indebitamente il perseguimento di interessi della Società.

Le Funzioni Aziendali interessate sono tenute a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

5.1 L'ASSUNZIONE

Se le valutazioni sui candidati avranno esito positivo, sarà possibile procedere all'assunzione.

Il PRES o un componente del CDA munito del potere di rappresentanza, sottoscrive il contratto di assunzione.

5.2 IL PAGAMENTO DEL SALARIO MENSILE E LA GESTIONE DI RIMBORSI SPESE

Il CDL, elabora, mensilmente, un elenco con i pagamenti da effettuare in favore dei dipendenti; il suddetto elenco viene sottoposto al controllo del PRES.

I rimborsi spese a ciascun dipendente devono essere eseguiti sulla base di evidenze documentali, di cui dovrà predisporsi apposito report.

In caso di concessione di *"fringe benefits"*, essi devono risultare dalla busta paga.

Gli avanzamenti di carriera sono stabiliti sulla base di valutazioni oggettive, in relazione alle competenze possedute ed a quelle potenzialmente esprimibili, in ragione della funzione da ricoprire.

Le retribuzioni eccedenti le misure fissate dai contratti collettivi, sulla base delle responsabilità e dei compiti della mansione attribuita al dipendente e, comunque, in riferimento ai valori medi di mercato, dovranno essere motivate dal CDL e, all'uopo, autorizzate per iscritto o digitalmente dal PRES.

INOLTRE, PER L'UTILIZZO DI RISORSE FINANZIARIE COLLEGATE AL PAGAMENTO DEGLI STIPENDI:

1. il pagamento deve essere effettuato, esclusivamente, sul conto corrente comunicato dal dipendente;
2. il pagamento deve corrispondere a quanto risultante dalla busta paga mensile; si precisa che, i rimborsi spese devono anch'essi risultare dalla busta paga, supportati dalle evidenze di spesa.

   E', tuttavia, possibile, laddove richiesto dal dipendente interessato, eseguire il pagamento di un anticipo sullo stipendio, purchè lo stesso venga annotato sull'apposito archivio informatico – all'uopo predisposto nella piattaforma digitale di condivisione – e successivamente, procedere al pagamento del saldo dovuto, dopo l'emissione della relativa busta paga;

3. vige il divieto di effettuare pagamenti su conti cifrati e di pagamento in favore di un soggetto diverso dalla controparte contrattuale;
4. il pagamento non può essere effettuato in un Paese terzo rispetto a quello delle parti contraenti o di esecuzione del contratto;
5. il pagamento effettuato su conti correnti di banche appartenenti od operanti in paesi elencati tra i c.d. "paradisi fiscali", o in favore di società "*off shore*", deve avvenire nel rispetto delle leggi in materia;
6. al momento dell'addebito del bonifico e al fine di garantire la tracciabilità del pagamento, conservare, nell'apposito archivio informatico - all'uopo predisposto nella piattaforma digitale di condivisione -, la contabile di pagamento.

5.3 L'ADOZIONE DEL MODELLO E IL SISTEMA SANZIONATORIO

Ai nuovi assunti verrà consegnata copia cartacea (o digitale) del Modello 231 e del Codice Etico, a seguito della quale la risorsa, con la sottoscrizione del contratto di assunzione, si impegna: ***i)*** al rispetto dei principi e delle regole negli stessi contenuti; ***ii)*** a prendere, periodicamente, visione del Modello sul sito aziendale, al fine di verificare possibili revisioni che verranno apportate al medesimo in ragione di possibili aggiornamenti normativi.

La risorsa dovrà, inoltre, essere informata del fatto che la società ha adottato un sistema sanzionatorio, in aderenza a quanto previsto dal CCNL di riferimento, per cui eventuali violazioni del Modello e del Codice Etico potranno essere sanzionate e, i comportamenti più gravi, potranno sfociare nel licenziamento per giusta causa.

5.4.IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE

La presente sezione disciplina i principi di comportamento e i presidi operativi che IDRAGEST S.r.l. è tenuta ad adottare al fine di prevenire la commissione del reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, così come configurato dall'art. 22, comma 12 e comma 12-bis, del D.Lgs. n. 286/1998 ("Testo Unico sull'Immigrazione"), nel testo risultante a seguito delle modifiche introdotte dal D.L. 11 ottobre 2024, n. 145 ("Decreto Flussi"), convertito con modificazioni dalla Legge 9 dicembre 2024, n. 187.

Il quadro normativo di riferimento ha subìto un significativo aggiornamento per effetto dei citati provvedimenti, che hanno ridisegnato in senso digitale le procedure amministrative di assunzione di lavoratori stranieri e hanno rimodulato alcune fattispecie penali connesse, lasciando tuttavia sostanzialmente invariata la struttura delle condotte-presupposto rilevanti ai fini della responsabilità degli enti ai sensi del D.Lgs. 231/2001.

REATO-PRESUPPOSTO E RESPONSABILITÀ DEGLI ENTI

Il reato di impiego di lavoratori stranieri privi di regolare permesso di soggiorno è richiamato quale reato-presupposto dall'art. 25-duodecies del D.Lgs. n. 231/2001, il quale prevede la responsabilità amministrativa dell'ente esclusivamente nelle ipotesi aggravate di cui al comma 12-bis dell'art. 22 D.Lgs. 286/1998, nei termini di seguito analizzati.

Per le ipotesi di reato non circostanziate di cui al comma 12, la responsabilità rimane di carattere esclusivamente penale personale in capo all'autore materiale della condotta e agli eventuali concorrenti, senza comportare la responsabilità amministrativa dell'ente. Ciò non esime IDRAGEST dall'adottare presidi preventivi anche con riguardo al comma 12, in coerenza con i principi generali del Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D.Lgs. 231/2001.

5.4.1 Digitalizzazione delle procedure di ingresso e assunzione

Il D.L. 145/2024, modificando l'art. 22 D.Lgs. 286/1998 , ha introdotto un'articolata riforma delle procedure amministrative di assunzione di lavoratori stranieri, improntata alla digitalizzazione integrale del processo. I principali adempimenti a carico del datore di lavoro sono i seguenti:

Trasmissione telematica della domanda allo Sportello Unico per l'Immigrazione (SUI): La domanda di nulla osta al lavoro, comprensiva di tutta la documentazione richiesta, deve essere trasmessa in via telematica. È fatto divieto di presentazione cartolarea.

Documentazione da allegare in forma digitale: Contestualmente alla domanda, il Responsabile delle Risorse Umane (RAM/RRU) di IDRAGEST è tenuto a trasmettere allo Sportello Unico per l'Immigrazione:

1. il certificato di idoneità alloggiativa, sottoscritto con firma digitale o altro tipo di firma elettronica qualificata (è ammessa autocertificazione per dormitori stabili di cantiere nel rispetto dell'allegato XIII del D.Lgs. 81/2008; per strutture alberghiere è sufficiente l'indicazione della struttura ospitante);
2. l'asseverazione di cui all'art. 24-bis, comma 2, D.Lgs. 286/1998, in originale digitale, sottoscritta con firma digitale o firma elettronica qualificata;
3. il domicilio digitale (PEC) del datore di lavoro, inserito in uno degli indici nazionali di cui agli artt. 6-bis e 6-quater del D.Lgs. 82/2005 (Codice dell'Amministrazione Digitale).

Sottoscrizione digitale del contratto di soggiorno: A seguito del rilascio del nulla osta, il datore di lavoro e il lavoratore straniero sono tenuti a sottoscrivere il contratto di soggiorno di cui all'art. 5-bis D.Lgs. 286/1998 entro quindici giorni dalla data di ingresso del lavoratore nel territorio nazionale, non più presso lo Sportello Unico per l'Immigrazione, bensì:

1. mediante firma digitale o firma elettronica qualificata da parte del datore di lavoro;
2. ovvero, in alternativa per il lavoratore, mediante firma autografa, con successiva apposizione della firma digitale del datore di lavoro sulla copia informatica del contratto, che costituisce dichiarazione ai sensi dell'art. 47 D.P.R. 445/2000 in ordine alla sottoscrizione autografa del lavoratore.

Il contratto così sottoscritto deve essere trasmesso telematicamente dallo stesso datore di lavoro allo Sportello Unico per l'Immigrazione per gli adempimenti concernenti la richiesta di rilascio del permesso di soggiorno

Conferma del nulla osta: Il datore di lavoro è tenuto a confermare la richiesta di nulla osta allo Sportello Unico per l'Immigrazione entro quindici giorni dalla comunicazione di avvenuta conclusione degli accertamenti di rito sulla domanda di visto di ingresso presentata dal lavoratore. In assenza di conferma entro tale termine, la richiesta si intende rifiutata e il nulla osta, ove già rilasciato, è revocato.

5.4.2. Presidi di Controllo Preventivo e Verifica preventiva del titolo di soggiorno

Prima dell'instaurazione di qualsiasi rapporto di lavoro con un cittadino di Paese terzo già presente nel territorio nazionale, il RAM/RRU di IDRAGEST è tenuto a:

1. verificare la validità del permesso di soggiorno, accertando che lo stesso non sia scaduto, revocato o annullato;
2. verificare la compatibilità del titolo di soggiorno con l'esercizio di attività lavorativa subordinata (non è consentita, ad esempio, l'assunzione di cittadini extracomunitari presenti in Italia per soli motivi di turismo);
3. acquisire e conservare copia del documento di soggiorno prima della stipulazione del contratto di lavoro.

È FATTO DIVIETO ASSOLUTO DI INSTAURARE RAPPORTI DI LAVORO CON CITTADINI STRANIERI:

1. privi di permesso di soggiorno;
2. il cui permesso sia scaduto senza che ne sia stato chiesto il rinnovo nei termini di legge;
3. il cui permesso sia stato revocato o annullato.
4. È altresì vietato il ricorso al lavoro minorile in qualsiasi forma.

5.4.3 Controlli Operativi e Tracciabilità

La gestione operativa degli adempimenti di cui alla presente sezione è affidata al Responsabile Amministrativo/Responsabile delle Risorse Umane (RAM/RRU), il quale:

1. è il soggetto referente per tutti i rapporti con lo Sportello Unico per l'Immigrazione;
2. coordina il monitoraggio delle scadenze dei permessi di soggiorno dei dipendenti stranieri;
3. garantisce la corretta formazione e aggiornamento del personale coinvolto nelle attività di selezione e assunzione;
4. riferisce tempestivamente al CDA in caso di irregolarità emerse o potenziali, con proposta di misura cautelativa;
5. può delegare specifici compiti di monitoraggio operativo al Responsabile di Funzione competente, mantenendo la responsabilità di supervisione.

5.5 PERMESSO DI SOGGIORNO PER GLI STRANIERI VITTIME DI INTERMEDIAZIONE ILLECITA E SFRUTTAMENTO DEL LAVORO

La presente sezione disciplina i principi di comportamento, i controlli operativi e i flussi informativi relativi alla gestione dei casi in cui un lavoratore straniero sia vittima di violenza, abuso o sfruttamento lavorativo rilevante ai sensi dell'art. 18-ter del D.Lgs. 286/1998, introdotto dal D.L. 145/2024, nel quadro dei presidi di prevenzione dei reati richiamati dall'art. 25-duodecies del D.Lgs. 231/2001 e del delitto di cui all'art. 603-bis c.p.

.Quando, nel corso di operazioni di polizia, di indagini o di un procedimento per il delitto previsto dall'art. 603-bis c.p. commesso in danno di un lavoratore straniero sul territorio nazionale, siano accertate situazioni di violenza, abuso o comunque di sfruttamento del lavoro, e il lavoratore contribuisca utilmente all'emersione dei fatti e all'individuazione dei responsabili, il Questore, su proposta dell'autorità giudiziaria procedente, rilascia con immediatezza un permesso di soggiorno finalizzato a consentire alla vittima e ai membri del suo nucleo familiare di sottrarsi alla violenza o allo sfruttamento D.Lgs. 286/1998 Qualora le situazioni di violenza, abuso o sfruttamento siano segnalate all'autorità giudiziaria o al Questore dall'Ispettorato nazionale del lavoro, quest'ultimo esprime contestualmente il proprio parere anche in merito all'eventuale rilascio del permesso.

Il permesso rilasciato ai sensi dell'art. 18-ter reca la dicitura "casi speciali", ha durata di sei mesi, è rinnovabile per un anno o per il maggior periodo occorrente per motivi di giustizia, consente l'accesso ai servizi assistenziali e allo studio, l'iscrizione anagrafica e lo svolgimento di lavoro subordinato o autonomo, fermi i requisiti minimi di età, ed è convertibile, alla scadenza, in permesso per lavoro subordinato, autonomo o studio nei casi previsti dalla legge.

Il permesso è revocato in caso di condotta incompatibile con le finalità dello stesso, segnalata dal procuratore della Repubblica o, per quanto di competenza, dal Ministero del lavoro e delle politiche

sociali, ovvero accertata dal Questore, nonché quando vengano meno le condizioni che ne hanno giustificato il rilascio.

Nei confronti dello straniero condannato, anche con sentenza non definitiva o a seguito di applicazione della pena su richiesta, per il delitto di cui all'art. 603-bis c.p., possono inoltre essere disposte la revoca del permesso di soggiorno e l'espulsione ai sensi dell'art. 13 del D.Lgs. 286/1998.

Ai fini del presente Modello, la Società vieta in modo assoluto qualsiasi condotta che possa anche indirettamente favorire l'impiego di lavoratori stranieri in condizioni di irregolarità, abuso o sfruttamento, nonché qualunque comportamento idoneo a ostacolare l'emersione di fatti rilevanti ai sensi dell'art. 603-bis c.p. o del rilascio del permesso di soggiorno per casi speciali previsto dall'art. 18-ter del D.Lgs. 286/1998. È fatto divieto a tutti i destinatari del Modello di porre in essere o tollerare condizioni lavorative riconducibili agli indici di sfruttamento richiamati dall'art. 603-bis c.p., nonché di utilizzare personale privo di titolo di soggiorno valido o di documentazione idonea a consentire legittimamente il soggiorno e l'attività lavorativa nei casi previsti dalla legge.

In coerenza con l'art. 22, commi 12 e 12-bis, del D.Lgs. 286/1998, la Società vieta altresì l'occupazione di lavoratori stranieri privi di permesso di soggiorno, con permesso scaduto senza richiesta di rinnovo nei termini di legge, revocato o annullato, con particolare attenzione ai casi aggravati rilevanti ai fini dell'art. 25-duodecies del D.Lgs. 231/2001.

Sotto il profilo operativo, la funzione competente alla gestione del personale deve acquisire, verificare e conservare in modo tracciato la documentazione relativa al titolo di soggiorno, all'eventuale ricevuta attestante la presentazione della richiesta di rilascio del permesso ex art. 18-ter, agli eventuali provvedimenti o comunicazioni dell'autorità, nonché ogni altro documento utile a dimostrare la legittima prosecuzione del rapporto di lavoro.

In attesa del rilascio del permesso di soggiorno, il lavoratore straniero cui sia stata rilasciata la ricevuta attestante l'avvenuta presentazione della richiesta può soggiornare legittimamente nel territorio dello Stato e svolgere temporaneamente l'attività lavorativa fino a eventuale comunicazione dell'autorità di pubblica sicurezza relativa a motivi ostativi; pertanto la Società può consentire l'avvio o la prosecuzione dell'attività solo previa acquisizione della predetta ricevuta e previa verifica della sua coerenza con il caso concreto.

La funzione competente deve inoltre censire tali posizioni nell'anagrafica del personale, monitorare le scadenze dei titoli e dei rinnovi, richiedere in tempo utile la documentazione aggiornata, sospendere l'attivazione o la prosecuzione del rapporto in caso di documentazione mancante, incoerente o negativa, e attivare senza ritardo i flussi interni di escalation previsti dalla procedura.

In presenza di segnalazioni, ispezioni, indizi di sfruttamento, anomalie retributive, utilizzo irregolare di intermediari o provvedimenti dell'autorità che facciano emergere possibili situazioni riconducibili all'art. 603-bis c.p., la funzione competente deve assicurare immediata informazione agli organi aziendali competenti e all'Organismo di Vigilanza, con piena tracciabilità delle verifiche svolte e delle decisioni adottate.

5.6 LE ATTIVITÀ SENSIBILI RELATIVE AI REATI DI IMPIEGO IRREGOLARE DI LAVORATORI STRANIERI PRIVI DEL PERMESSO DI SOGGIORNO

L'Art. 6, comma 2, lett. a) del D.Lgs.n.231/2001 indica, come uno degli elementi essenziali dei modelli di organizzazione e di gestione previsti dal decreto, l'individuazione delle cosiddette attività "sensibili" o "a rischio", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D.Lgs.n.231/2001.

L'analisi svolta nel corso del Progetto ha permesso di individuare le attività della Società che potrebbero essere considerate "sensibili" con riferimento al rischio di commissione dei reati richiamati dall'Art.25-duodecies del D.Lgs.n.231/2001.

In particolare, costituiscono attività sensibili:

1. assunzione diretta di personale extra-UE;
2. utilizzo di personale somministrato;
3. affidamento di attività operative a fornitori o subfornitori con impiego di manodopera;
4. accesso di tecnici esterni presso clienti o siti operativi;
5. gestione delle scadenze dei titoli di soggiorno;
6. verifiche documentali in sede di onboarding e in costanza di rapporto.

Per ciascuna attività sensibile è obbligatoria una check-list di controllo comprendente almeno:

1. identificazione del lavoratore;
2. acquisizione del titolo di soggiorno;
3. verifica della sua validità e compatibilità con l'attività; registrazione della scadenza;
4. alert preventivo;
5. esito del controllo;
6. eventuali azioni sospensive.

RAM/RRU monitora con periodicità almeno mensile le scadenze dei titoli e segnala senza ritardo anomalie, omissioni documentali, mancati rinnovi, impiego di personale esterno non verificato o situazioni a rischio di sfruttamento.

5.7 LA TRACCIABILITÀ DELLE PRESENZE

Il RAM/RRU, consegna il *file* presenze dipendenti al Consulente del lavoro per l'elaborazione delle buste paga, e dovrà conservarlo nell'apposito archivio informatico – all'uopo predisposto nella piattaforma digitale di condivisione - per eventuali verifiche.

5.8 FORMAZIONE

L'attività di formazione, promossa dallo stesso ODV, è finalizzata a promuovere la conoscenza della normativa di cui al decreto legislativo 231/2001 e a fornire un quadro esaustivo della stessa, dei risvolti pratici che da essa discendono, nonché dei contenuti e principi su cui si basa il Modello Organizzativo e il relativo Codice Etico fra tutti i dipendenti che, pertanto, sono tenuti a conoscerli, osservarli e rispettarli, contribuendo alla loro attuazione.

L'attività di formazione, eventualmente anche tramite corsi on line, è differenziata, nei contenuti e nelle modalità di erogazione, in ragione del ruolo ricoperto dai destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno i destinatari funzioni di rappresentanza della Società.

Per i soggetti maggiormente coinvolti nelle attività considerate sensibili ai fini del decreto legislativo 231/2001, la Società organizza corsi di formazione ad hoc in aula.

In particolare, in osservanza agli obblighi imposti dalla L. n. 90/2024 - che ha previsto l'estensione della sicurezza informatica per difendersi dai cyber-attacchi, aumentando le sanzioni previste per i c.d. "computer crimes" - IDRAGEST SRL si impegna a:

- adottare un programma di sensibilizzazione sulla sicurezza delle informazioni con l'obiettivo di rendere i dipendenti – ed in particolare il responsabile della sicurezza informatica - consapevoli delle loro responsabilità per la sicurezza delle informazioni e dei mezzi con cui tali responsabilità vengono assolte. Invero, la società dovrà, con cadenza annuale, eseguire un apposito programma di formazione, in modo da rimanere in linea con le politiche e le procedure organizzative all'uopo previste.

- organizzare programmi di formazione per sensibilizzare i dipendenti in materia di responsabilità amministrativa degli enti con l'intento di evitare che l'azione illecita di un dipendente comporti l'apertura di un procedimento ex Decreto 231 a carico della società.

- promuovere ed assicurare il puntuale rispetto da parte di tutti i Destinatari della presente procedura del regolamento informatico adottato da IDRAGEST e delle relative procedure aventi ad oggetto il corretto utilizzo delle risorse informatiche aziendali, la sicurezza informatica/telematica, la protezione dei dati sensibili.

- Tracciatura e registrazione delle attività eseguite su sistemi, applicazioni e reti, potenzialmente lesive per la sicurezza.

- Verifica periodica delle modalità di accesso ai sistemi, dei log di registrazione delle attività sui sistemi, delle eccezioni e degli eventi concernenti la sicurezza.
- Definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi.
- Adozione di meccanismi di protezione da software pericolosi e procedure di controllo della installazione di software sui sistemi operativi.

La partecipazione ai corsi di formazione ha carattere obbligatorio e deve riguardare non solo il personale HR, ma anche i responsabili di commessa, i referenti che autorizzano l'accesso di personale esterno presso i clienti e i soggetti che gestiscono appalti, outsourcing tecnico o somministrazione di personale, con focus su verifiche documentali, indicatori di rischio, divieti di impiego indiretto di lavoratori irregolari e obblighi di tracciabilità.

6 GESTIONE DEI TRATTAMENTI PREVIDENZIALI E ASSISTENZIALI DEL PERSONALE

Qualsiasi contatto con esponenti della Pubblica Amministrazione per questioni inerenti il personale, deve essere annotato su apposito registro.

Qualsiasi documento diretto alla P.A. relativo alla gestione del personale, deve essere sottoposto al CDL via *mail* o *brevi manu*.

7 LA GESTIONE DEGLI OMAGGI

Il Codice Etico stabilisce la politica di IDRAGEST in merito alla ricezione e all'offerta di omaggi, ospitalità ed intrattenimenti (ossia erogazioni gratuite di beni e servizi, a fini promozionali o di pubbliche relazioni), delineando le relative responsabilità dei soggetti coinvolti nel processo.

Nell'ambito dei suddetti comportamenti e come disciplinato dal protocollo relativo alla gestione degli omaggi, è fatto divieto alla Società, ai suoi dipendenti e/o ai soggetti terzi in particolare, di concedere altri vantaggi di qualsiasi natura (es.: promesse di assunzione, *etc.*) in favore dei rappresentanti della Pubblica Amministrazione e/o soggetti privati, ovvero farsi concedere altri vantaggi.

8 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutte le Funzioni Aziendali coinvolte nella selezione e assunzione del personale informano, tempestivamente, l'Organismo di Vigilanza delle situazioni anomale e/o in contrasto con la presente procedura, nonchè di qualsivoglia comportamento non conforme alle disposizioni previste dal Codice Etico.

Inoltre, i soggetti a vario titolo coinvolti, sono tenuti a trasmettere all'Organismo di Vigilanza, con periodicità annuale:

- le assunzioni / avanzamenti di carriera e variazioni remunerative, relative a personale che abbia ricoperto cariche pubbliche e/o che abbia avuto esperienze lavorative in un ente pubblico;
- copia dei procedimenti disciplinari svolti e le eventuali sanzioni comminate, i provvedimenti assunti ovvero i provvedimenti motivati di archiviazione di procedimenti disciplinari a carico del personale aziendale.

I destinatari devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio ordinato – tutta la documentazione all'uopo necessaria.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari;

• con periodicità annuale, effettua dei controlli, anche documentali, tramite interviste al personale o al RAM/RRU, al fine di verificare gli orari dei lavoratori, controllare l'adeguatezza dei turni e del termine dell'orario di lavoro, del riposo settimanale, delle ferie, dell'aspettativa obbligatoria, delle agevolazioni previste dalla legge in materia di disabilità, maternità, paternità, malattia.

Tutto ciò posto, sono trasmessi all'OdV, con periodicità almeno semestrale e comunque immediatamente nei casi gravi, i dati relativi a: lavoratori extra-UE in forza; scadenze dei titoli di soggiorno; anomalie documentali; sospensioni cautelative dell'operatività; utilizzo di personale di terzi non ancora validato; verifiche ispettive e contestazioni ricevute. L'OdV può richiedere accesso ai fascicoli documentali e svolgere controlli a campione.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E,

PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

Sommario....2

1 OBIETTIVI E FUNZIONI DEL MODELLO....3

2 ACRONIMI AZIENDALI....3

3 RIFERIMENTI NORMATIVI....3

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA....4

5 PRINCIPI GENERALI DI COMPORTAMENTO E DESCRIZIONE DEL PROCESSO....4

6 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO....6

1 OBIETTIVI E FUNZIONI DEL MODELLO

Ai sensi del D. Lgs. 231/2001, il processo relativo alla gestione dei contenziosi giudiziali e stragiudiziali, nonchè delle dichiarazioni da rendere all'Autorità Giudiziaria, potrebbe presentare occasioni per la commissione dei reati di "*Corruzione contro la Pubblica Amministrazione*", "*Induzione indebita a dare o promettere utilità*", "*Traffico di influenze illecite*", e "*Truffa ai danni dello Stato o di altro Ente pubblico*" nonché del reato di "In*duzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*".

Inoltre, sussiste, altresì, il rischio della commissione dei reati di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte di IDRAGEST, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC	Responsabile Tecnico
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RPROG	Responsabile Progettazione
REC	Responsabile Esterno Contabilità

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di IDRAGEST S.r.l.;

-Decreto Legislativo 10 marzo 2023, n. 24 (Attuazione della direttiva (UE) 2019/1937 - "Whistleblowing");
- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

Il presente protocollo si applica a tutte le Funzioni Aziendali e/o ad eventuali consulenti esterni coinvolti nella gestione dei contenziosi giudiziali e stragiudiziali (ad es. amministrativo, civile, penale, fiscale, giuslavoristico e previdenziale) e degli accordi transattivi con enti pubblici o con soggetti privati, nonché a tutti i *Destinatari* (compresi i Collaboratori ed i Consulenti esterni all'uopo incaricati) che, in occasione di procedimenti penali, entrino in contatto con l'Autorità Giudiziaria e che ricoprano la qualità di imputati o coimputati in un procedimento connesso o collegato.
Il Responsabile della procedura è il Presidente.

5 PRINCIPI GENERALI DI COMPORTAMENTO E DESCRIZIONE DEL PROCESSO

Il processo di gestione del contenzioso e degli accordi transattivi deve essere improntato ai principi di massima trasparenza, tracciabilità documentale e segregazione delle funzioni. Le Funzioni Aziendali competenti per materia operano in coordinamento con gli eventuali professionisti esterni incaricati, garantendo che ogni fase sia autorizzata e verificabile.

IL PROCESSO DI GESTIONE DEL CONTENZIOSO SI ARTICOLA NELLE SEGUENTI FASI:

APERTURA DEL CONTENZIOSO:

1. raccolta e formalizzazione delle informazioni e della documentazione;
2. analisi, valutazione e produzione degli elementi probatori, con parere formale della funzione competente;
3. predisposizione degli scritti difensivi, approvati dalla funzione responsabile prima del deposito.

GESTIONE DELLA VERTENZA:

1. ricezione, analisi e valutazione degli atti, con protocollazione e archiviazione digitale;
2. partecipazione alle udienze, con redazione di report sintetici per la Direzione;
3. mantenimento di rapporti costanti e formalizzati (es. via email, verbali) con i professionisti esterni.

CHIUSURA DELLA VERTENZA.

IL PROCESSO DI GESTIONE DEGLI ACCORDI TRANSATTIVI SI ARTICOLA NELLE SEGUENTI FASI:

1. analisi dell'evento e verifica dei presupposti per la transazione, con redazione di una relazione che ne attesti la convenienza economica e la congruità per la Società, al fine di escludere che l'accordo possa mascherare dazioni o promesse illecite;
2. gestione delle trattative, condotte da personale autorizzato e tracciate tramite comunicazioni formali;

redazione, stipula ed esecuzione dell'accordo, previa autorizzazione del CDA o di un suo delegato in base ai poteri conferiti.

NEL CASO IN CUI UN DESTINATARIO DEL MODELLO SIA CHIAMATO A RENDERE DICHIARAZIONI INNANZI ALL'AUTORITÀ GIUDIZIARIA, DEVE OSSERVARE I SEGUENTI PRINCIPI:

1. garantire massima collaborazione con l'Autorità Giudiziaria, nel rispetto delle indicazioni formulate dalla stessa e dei principi del Modello e del Codice Etico;
2. riferire con veridicità le notizie in proprio possesso;
3. segnalare immediatamente all'Organismo di Vigilanza e, se del caso, all'Autorità Giudiziaria, ogni eventuale pressione, minaccia o offerta ricevuta per indurlo a non rendere dichiarazioni o a renderle mendaci, utilizzando i canali previsti dalla procedura di whistleblowing.

PER QUANTO CONCERNE GLI ASPETTI OPERATIVI:

1. i legali esterni devono essere nominati con apposita procura e scelti da un albo fornitori qualificato. Solo i legali esterni formalmente incaricati possono interfacciarsi con le controparti e le autorità;
2. tutta la documentazione da trasmettere all'Autorità Giudiziaria deve essere preventivamente verificata dalla funzione interna competente e dai legali incaricati, e formalmente approvata dal Responsabile della procedura prima dell'invio;
3. la Società garantisce la conservazione e la tracciabilità di tutta la documentazione prodotta e ricevuta.

6 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutte le Funzioni Aziendali, i dipendenti, i collaboratori e i consulenti esterni coinvolti nei processi descritti devono comunicare tempestivamente all'Organismo di Vigilanza, attraverso i canali di segnalazione istituiti ai sensi del D.Lgs. 24/2023:

1. qualsiasi situazione anomala, violazione o presunta violazione della presente procedura;
2. qualsiasi comportamento non conforme al Codice Etico e al Modello;
3. notizie di procedimenti giudiziari a carico di soggetti che operano per IDRAGEST S.r.l., se rilevanti per le attività a rischio.

In conformità con il D.Lgs. 24/2023, la Società garantisce la massima riservatezza sull'identità del segnalante e vieta e sanziona qualsiasi atto di ritorsione, diretta o indiretta, nei suoi confronti.

I Destinatari devono garantire la completa tracciabilità del processo, mettendo a disposizione dell'OdV, in un archivio digitale dedicato, tutta la documentazione necessaria per le verifiche.

All'Organismo di Vigilanza sono garantiti pieni e autonomi poteri di iniziativa e controllo, libero accesso a tutta la documentazione aziendale e adeguate risorse per lo svolgimento delle sue funzioni, a presidio della sua indipendenza ed efficacia.

L'ODV DOVRÀ, IN PARTICOLARE, EFFETTUARE:

1. il monitoraggio costante sull'efficacia delle procedure;
2. l'esame delle segnalazioni ricevute, disponendo gli accertamenti necessari;
3. La verifica periodica della corretta applicazione dei principi di segregazione funzionale e tracciabilità.

I dettagli sulle modalità di segnalazione sono precisati nella "Procedura di gestione del whistleblowing", redatta in conformità al D.Lgs. 24/2023.

La violazione della presente procedura, inclusi gli obblighi di comunicazione e il divieto di ritorsione, integra una violazione del Modello 231 e costituisce un illecito disciplinare, perseguibile ai sensi del sistema sanzionatorio definito nel Modello stesso, in conformità alla legge e al CCNL applicato.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI E FUNZIONE DEL MODELLO 3

2 ACRONIMI AZIENDALI 3

3 RIFERIMENTI NORMATIVI 4

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA 4

5 PRINCIPI GENERALI DI COMPORTAMENTO 4

5.1 PRINCIPIO DI CAUTELA NELL'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE (AI) 6

5.2 DESCRIZIONE DEL PROCESSO 6

6 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO 7

1 OBIETTIVI E FUNZIONE DEL MODELLO

Con il presente protocollo, IDRAGEST S.r.l. ("Società") definisce la procedura per la gestione e la divulgazione delle informazioni e delle comunicazioni esterne.

LO SCOPO È DI ASSICURARE LA CORRETTEZZA, TRASPARENZA E VERIDICITÀ DELLE INFORMAZIONI DIFFUSE, AL FINE DI PREVENIRE LA COMMISSIONE DEI REATI PRESUPPOSTO DI CUI AL D.LGS. 231/2001, CON PARTICOLARE RIFERIMENTO AI:

1. Reati societari, quali le false comunicazioni sociali (artt. 2621 e 2622 c.c.);
2. Reati contro la Pubblica Amministrazione, in considerazione dei rapporti di consulenza e fornitura che la Società intrattiene con enti pubblici o gestori di pubblici servizi;
3. Reati di frode (art. 640 c.p.) e frode informatica (art. 640-ter c.p.);
4. Reati di manipolazione del mercato (art. 185 TUF), per quanto applicabili e con specifico riferimento ai rischi derivanti dall'uso di nuove tecnologie.

Tutti coloro che, per ragioni del proprio incarico, sono coinvolti nella gestione del processo in oggetto, devono garantire la tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte. La presente procedura costituisce, inoltre, uno strumento essenziale per l'adempimento del dovere, in capo all'organo amministrativo, di istituire un assetto organizzativo, amministrativo e contabile adeguato, ai sensi dell'art. 2086 del Codice Civile

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RSPP	Responsabile Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC	Responsabile Tecnico
RPROG	Responsabile Progettazione
RFAM	Responsabile Facility Management
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RATTR	Responsabile Attrezzature e Mezzi
RAM/RRU	Responsabile Amministrazione - Risorse Umane
GRPROG	Gruppo Progettisti

PROG Programmatori

RSCM Responsabile singola commessa

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii.;
- Codice Civile, con particolare riferimento agli artt. 2086, 2621 e 2625;
- Testo Unico della Finanza (D.Lgs. 58/1998), con particolare riferimento all'art. 185 come modificato dalla L. 238/2021 e dalla L. 147/2025 in materia di intelligenza artificiale;
- Regolamento (UE) 2024/2187 sull'Intelligenza Artificiale (AI Act), per i principi di trasparenza e controllo sui sistemi di IA;
- Decreto Legislativo 10 marzo 2023, n. 24 (Decreto Whistleblowing);

Codice Etico di IDRAGEST S.r.l..

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

Il presente protocollo si applica all'Organo Amministrativo, ai dipendenti e ai collaboratori di IDRAGEST che abbiano accesso ad informazioni privilegiate, nell'accezione di cui alla vigente normativa di legge e regolamentare, ovvero che gestiscano le comunicazioni della Società all'esterno, intendendosi con tale espressione la distribuzione di ricerche e raccomandazioni nonché qualsiasi diffusione di notizie, dati o informazioni nell'ambito dei rapporti di business, delle attività di marketing o promozionali, dei rapporti con i mezzi di informazione, oltre che le comunicazioni di carattere obbligatorio *c.d. price sensitive*.

Il principale responsabile della seguente procedura è il PRES.

5 PRINCIPI GENERALI DI COMPORTAMENTO

Il processo di comunicazione esterna, se non adeguatamente presidiato, espone la Società al rischio di commissione di reati quali false comunicazioni sociali, frodi e illeciti nei rapporti con la Pubblica

Amministrazione. È pertanto fondamentale garantire la massima correttezza, veridicità e trasparenza di ogni informazione comunicata all'esterno.

OBIETTIVO DELLE REGOLE SANCITE DAL PRESENTE DOCUMENTO, IN OTTEMPERANZA AI DETTAMI DELLA NORMATIVA VIGENTE, È QUELLO DI GARANTIRE CHE:

• la circolazione delle informazioni nel contesto aziendale possa svolgersi senza pregiudizio del carattere privilegiato o confidenziale delle informazioni stesse ed evitare che dette informazioni siano condivise con soggetti non autorizzati, nonché di assicurare che la divulgazione all'esterno delle informazioni privilegiate avvenga in modo tempestivo, in forma completa e comunque in modo tale da evitare asimmetrie informative;

• le informazioni privilegiate non vengano comunicate, anche in modo involontario, a terzi per ragioni diverse da quelle di ufficio;

• tutti i Destinatari ed i collaboratori non abusino delle informazioni privilegiate, di cui sono in possesso in virtù del ruolo ricoperto e / o delle funzioni svolte in ambito aziendale;

• le comunicazioni di IDRAGEST all'esterno trovano adeguata disciplina e una precisa individuazione dei soggetti abilitati ad effettuarle, affinché le stesse siano tali da evitare la divulgazione di informazioni o notizie false o fuorvianti, sia con riferimento alla Società, sia con riferimento a società terze;

• più in generale è vietato a chiunque lavori o collabori con la Società di effettuare qualsivoglia comunicazione e/o divulgare informazioni, per conto della Società, senza l'autorizzazione scritta e/o senza la preventiva approvazione del PRES; è, altresì, vietato comunicare e/o divulgare informazioni relative alla Società se riservate e/o coperte da segreto industriale.

In particolare, le misure organizzative, di gestione e controllo delle informazioni privilegiate attuate da IDRAGEST sono dirette ad assicurare condizioni di correttezza, efficienza e tempestività nella trasparenza informativa della Società.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte di IDRAGEST, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Eventuali eccezioni a questi protocolli devono essere autorizzate dal PRES o da altra funzione all'uopo preposta.

5.1 PRINCIPIO DI CAUTELA NELL'USO DI SISTEMI DI INTELLIGENZA ARTIFICIALE (AI)

In linea con le più recenti evoluzioni normative (Legge n. 147/2025 e AI Act), è richiesto un elevato livello di cautela nell'utilizzo di sistemi di Intelligenza Artificiale per la generazione o la diffusione di comunicazioni esterne.

IN PARTICOLARE, È FATTO OBBLIGO DI:

1. Verificare sempre l'accuratezza e la veridicità delle informazioni generate da sistemi di AI prima della loro diffusione.
2. Assicurare la trasparenza sull'utilizzo di tali sistemi, ove richiesto dalla natura della comunicazione o dalla normativa.
3. Evitare l'impiego di sistemi di AI per creare o diffondere notizie false o porre in essere "altri artifizi" idonei a ingannare terzi o alterare la corretta formazione della volontà negoziale, tenuto conto che l'impiego di tali sistemi può costituire un'aggravante di reato .

5.2 DESCRIZIONE DEL PROCESSO

LE FUNZIONI AZIENDALI, I DIPENDENTI E I COLLABORATORI SONO TENUTI A OSSERVARE LE SEGUENTI MODALITÀ:

1. È fatto obbligo di mantenere riservate tutte le informazioni e i documenti acquisiti, sia aventi ad oggetto la Società, sia riguardanti clienti o fornitori, utilizzandoli esclusivamente per l'espletamento dei propri compiti lavorativi;
2. Particolare rigore deve essere osservato nelle comunicazioni e nella documentazione prodotta nell'ambito di rapporti con la Pubblica Amministrazione. Tali comunicazioni devono essere sempre veritiere, complete e trasparenti, in aderenza ai principi del Codice Etico;
3. È vietato trasmettere a terzi informazioni riservate su clienti, fornitori, progetti o strategie aziendali, se non previa autorizzazione e sottoscrizione di accordi di confidenzialità;
4. La comunicazione selettiva di informazioni riservate è consentita solo per comprovate esigenze di servizio e nel rispetto delle cautele atte ad evitarne un'impropria circolazione;

Tutta la documentazione – comprese le autorizzazioni – relativa alla gestione della comunicazione a terzi, deve essere archiviata digitalmente e resa accessibile per le attività di controllo.

6 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

I Destinatari devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto su apposita piattaforma informatica – tutta la documentazione necessaria.

Ciascun soggetto coinvolto nella procedura informa tempestivamente l'Organismo di Vigilanza di:

- ✓ situazioni anomale e/o poste in essere in deroga alla presente procedura;
- ✓ di comportamenti non conformi a quanto previsto nel Modello e nel Codice Etico;
- ✓ Qualsiasi pressione, interna o esterna, volta a diffondere informazioni non veritiere, fuorvianti o a omettere informazioni rilevanti, specialmente nei rapporti con la P.A., istituti di credito o altri stakeholder significativi;
- ✓ Eventuali utilizzi non autorizzati o anomali di sistemi di Intelligenza Artificiale per la comunicazione esterna.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

L'ostacolo a tali attività di controllo può integrare una violazione sanzionabile ai sensi dell'art. 2625 c.c

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda, quest'ultima adottata ai sensi del D.Lgs. 24/2023 per dare attuazione a quanto previsto dall'art. 6, comma 2-bis, del D.Lgs. 231/2001. Tali canali garantiscono la riservatezza dell'identità del segnalante e la sua protezione da qualsiasi atto ritorsivo .

La violazione della presente procedura e dei suoi obblighi di comunicazione, integra una violazione del presente Modello di Organizzazione Gestione e Controllo e, pertanto, costituisce un illecito disciplinare passibile di sanzione ai sensi della legge vigente in materia, dello stesso Modello 231, nonché del contratto collettivo nazionale di lavoro applicato.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI E FUNZIONE DEL MODELLO 3

2 ACRONIMI AZIENDALI 6

3 RIFERIMENTI NORMATIVI 7

4 CAMPO DI APPLICAZIONE E RESPONSABILI DELLA PROCEDURA 7

5 I REATI INFORMATICI E DI INDEBITO UTILIZZO DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI 8

5.1 ART. 615 TER C.P. - Accesso abusivo ad un sistema telematico o informatico 8

5.2 art. 635 bis c.p. - Danneggiamento di informazioni, dati e programmi informatici (Modificato dalla Legge n.90 del 28 giugno 2024) 10

5.3 art. 635 ter c.p. - Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (modificato sia nella rubrica che nel testo dalla Legge n.90 del 28 giugno 2024) 10

5.4 art. 635 quater c.p. - Danneggiamento di sistemi informatici o telematici E art. 635 quinquies c.p. - Danneggiamento di sistemi informatici o telematici di pubblica utilità 12

5.5 ART. 491 BIS C.P. - Falsità nei documenti informatici 13

5.6 art. 640 quinquies c.p. - Frode informatica del soggetto che presta servizi di certificazione di firma elettronica ... 13

5.7 ART. 629, 3° COMMA, C.P. ESTORSIONE (INTRODOTTO DALLA LEGGE N.90 DEL 28 GIUGNO 2024) 14

6 REATI PRESUPPOSTO strumenti di pagamento diversi dai contanti 14

7 GOVERNANCE E GESTIONE DEL RISCHIO DI CIBERSICUREZZA (IN ATTUAZIONE DEL D.LGS. 138/2024) 16

8 ATTIVITA AZIENDALI SENSIBILI E PRINCIPI GENERALI DI COMPORTAMENTO 17

9 I REATI INFORMATICI di gestione ed utilizzo dei sistemi informatici del patrimonio informativo di idragest 18

10 ATTIVITA AZIENDALI SENSIBILI E PRINCIPI GENERALI DI COMPORTAMENTO 20

10.1 L'ACCESSO AI SISTEMI INFORMATICI, ACQUISTO E CONTROLLO DI *SOFTWARE - HARDWARE* 23

10. 2 L'ACCESSO A SITI DI ENTI PUBBLICI O PRIVATI 23

10. 3 I DISPOSITIVI ASSEGNATI A DIPENDENTI O FUNZIONI AZIENDALI 24

10.4 USO DELLA RETE INTERNET 24

10. 5 LE *PASSWORD* DI ACCESSO AI DISPOSITIVI 24

10. 6 LA GESTIONE DELLA POSTA ELETTRONICA 25

10. 7 L'UTILIZZO DI SUPPORTI MAGNETICI RIMOVIBILI 25

10. 8 IL LICENZIAMENTO O LE DIMISSIONI DI UN DIPENDENTE 25

10.9 LA VARIAZIONE DI DATI NEL SISTEMA INFORMATICO 26

10.10 INSTALLAZIONE DI *SOFTWARE* DI TERZE PARTI PER LA FATTURAZIONE 26

10.11 L'UTILIZZO DI SISTEMI *CLOUD COMPUTING* 26

10.12 FALSITÀ DI UN DOCUMENTO INFORMATICO O TELEMATICO E UTILIZZO DI *SMARTCARD* 26

10.13 DATA BREACH 26

10. 14 PREVISIONE DI UNA PROCEDURA DI *DISASTER RECOVERY* 27

11 I DIVIETI 27

12 LEGGE N. 90 DEL 2024 – CYBERSICUREZZA 29

12.1 I CONTROLLI PER LA PREVENZIONE DEI REATI INFORMATICI 31

12.2 PRESIDI DI CONTROLLO 33

12.3 Principi procedurali specifici 34

13 UTILIZZO DI SISTEMI DI INTELLIGENZA ARTIFICIALE E IA GENERATIVA 36

12 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO 38

1 OBIETTIVI E FUNZIONE DEL MODELLO

La Legge 18.3.2008 n. 48 ha ratificato la Convenzione del Consiglio d'Europa, stipulata a Budapest il 23.11.2001, avente quale obiettivo la promozione della cooperazione internazionale tra gli Stati firmatari, al fine di contrastare il proliferare di reati a danno della riservatezza, dell'integrità e della disponibilità di sistemi, reti e dati informatici, specie in considerazione della natura di tali illeciti, che spesso, nelle modalità della loro preparazione o realizzazione, coinvolgono Paesi diversi.

La riforma della disciplina della criminalità informatica è stata realizzata sia introducendo nel codice penale nuove fattispecie di reato, sia riformulando alcune norme incriminatrici già esistenti. L'art. 7 della legge ha inoltre aggiunto al D. Lgs. 231/2001 l'art. 24 bis, che elenca la serie dei reati informatici che possono dar luogo alla responsabilità amministrativa degli Enti.

La citata legge ha modificato anche il codice di procedura penale e le disposizioni in tema di protezione dei dati personali, essenzialmente al fine di agevolare le indagini sui dati informatici e consentire per determinati periodi la conservazione dei dati relativi al traffico telematico.

Non sono invece state recepite nell'ordinamento italiano le definizioni di "sistema informatico" e di "dato informatico" contenute nella Convenzione di Budapest; tali definizioni, che si riportano qui di seguito, potranno essere prese come riferimento dalla giurisprudenza in materia:

• "SISTEMA INFORMATICO": si intende qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica dei dati;

• "DATO INFORMATICO": si intende qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.

La presente procedura è redatta in conformità e in attuazione del nuovo quadro normativo in materia di cibersicurezza, introdotto con il Decreto Legislativo 4 settembre 2024, n. 138 (di recepimento della Direttiva NIS 2) e del relativo Regolamento di Esecuzione (UE) 2024/2690. In considerazione della natura dei servizi offerti da IDRAGEST, in particolare a supporto di infrastrutture critiche come le reti idriche, la Società si impegna ad adottare un approccio alla gestione del rischio cyber in linea con i più elevati standard richiesti per i "soggetti essenziali e importanti".

In tale ottica, questa procedura non solo mira a prevenire i reati presupposto 231, ma istituisce un sistema di gestione del rischio cyber che attribuisce specifiche responsabilità all'Organo Amministrativo, come previsto dall'art. 23 del D.Lgs. 138/2024.

Infine, la procedura costituisce uno strumento essenziale per l'adempimento del dovere, in capo all'organo amministrativo, di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa, ai sensi dell'art. 2086 del Codice Civile.

Ancora, non può non rilevarsi che l'attenzione rivolta al settore cyber è imposta da un contesto storico in cui la criminalità informatica continua ad evolversi rapidamente, adottando tecniche intrusive difficili da contrastare.

Per tali ragioni, l'esigenza di riformare la materia in esame, attuata con la L. n. 90/2024 che ha previsto l'estensione della sicurezza informatica per difendersi dai cyber-attacchi, aumentando le sanzioni previste per i c.d. "computer crimes". In attesa del recepimento nazionale della cosiddetta "NIS2"- che estende la responsabilità della cybersicurezza a tutta la filiera dei fornitori, con particolare riguardo alle infrastrutture critiche tra cui gli acquedotti - legge mira ad aumentare la sicurezza informatica per difendersi dai cyberattacchi, innalzando le sanzioni previste per alcuni tipi di reati informatici.

Invero, il Consiglio dei Ministri del 10 giugno ha approvato il decreto legislativo di recepimento della direttiva NIS2, che ha l'obiettivo di accrescere il livello di sicurezza delle reti e dei sistemi informativi, attraverso l'obbligo per le imprese di adottare un modello organizzativo di gestione del rischio aziendale relativo alla sicurezza informatica.

Infatti, i soggetti destinatari della normativa devono completare l'iter di adeguamento al nuovo impianto normativo che impone ai soggetti che, come IDRAGEST, erogano servizi o producono beni definiti essenziali e importanti, l'adozione di misure tecniche e organizzative adeguate e proporzionate rispetto alla gestione dei rischi che potrebbero esporre i propri sistemi informatici e di rete ad attacchi esterni e mettere in serio pericolo la fornitura dei propri servizi e l'intera infrastruttura.

SI ILLUSTRANO QUI DI SEGUITO I REATI PRESUPPOSTO ELENCATI DALL'ART. 24 BIS, 25 QUINQUIES, 25 NOVIES E 25 QUINQUIESDECIES DEL D. LGS. 231/2001.

La presente procedura definisce l'adeguamento alla riforma delle norme penali:

A) in materia di contrasto alle frodi e alle falsificazioni di mezzi di pagamento diversi dai contanti, attuata con il D.Lgs. 8 novembre 2021 n. 184 e della Legge n. 238 del 23.12.2021, nonché alle modifiche sostanziali apportate dalla L. n. 90/2024, recante "disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", fissando i ruoli, le responsabilità operative, le attività di controllo e i principi di comportamento adottati da IDRAGEST S.r.l. nell'ambito del processo di gestione ed utilizzo di sistemi informatici, per le attività a rischio, connesse con le fattispecie di reato previste dall'artt. 493 ter c.p., 493 quater e 640 ter c.p., art. 615 quater c.p., 615 quinquies c.p. (abrogato dalla L. 90/2024), 617 quater c.p., 617 quinquies c.p., art. 600 quater c.p. e art.609 undecies c.p., nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché di tracciabilità delle attività.

B) nella gestione e nell'utilizzo dei sistemi informatici e del Patrimonio Informativo della Società, poiché ai sensi del D. Lgs. 231/2001, i relativi processi potrebbero presentare occasioni per la commissione dei delitti informatici contemplati dall'art. 24 bis, nonché dei reati di "Frode informatica" previsto dall'art. 640 ter del codice penale e richiamato dagli art. 24 e 25 octies.1 del Decreto e "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti". Inoltre, mediante l'accesso alle reti informatiche potrebbero essere integrate le condotte illecite aventi ad oggetto le opere dell'ingegno protette.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Dunque, le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Modello e nel Codice Etico e la documentazione adottata in materia di protezione dei dati personali delle persone fisiche, in linea con la vigente normativa in tema di *privacy*.

Ancora, la presente procedura si applica altresì all'utilizzo, da parte dei soggetti aziendali autorizzati, di sistemi di intelligenza artificiale e di intelligenza artificiale generativa, inclusi gli strumenti messi a disposizione da fornitori terzi quali ChatGPT, nei limiti e secondo le modalità stabilite dalla policy IA aziendale.

L'utilizzo dell'intelligenza artificiale in ambito lavorativo deve avvenire in modo sicuro, affidabile, trasparente e nel rispetto della riservatezza dei dati personali e delle informazioni aziendali.

La Società, quale utilizzatore dei sistemi di IA nell'ambito della propria organizzazione, disciplina tali impieghi con misure tecniche, organizzative e formative idonee a garantirne il controllo, la tracciabilità e la supervisione umana, in coerenza con i principi di adeguatezza organizzativa ex art. 2086 c.c. [4], con le esigenze del modello ex art. 6 D.Lgs. 231/2001 e con la governance dei rischi cyber.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RSPP	Responsabile Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC	Responsabile Tecnico
RPROG	Responsabile Progettazione
RFAM	Responsabile Facility Management
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RATTR	Responsabile Attrezzature e Mezzi
RAM/RRU	Responsabile Amministrazione - Risorse Umane
GRPROG	Gruppo Progettisti
PROG	Programmatori

RSCM Responsabile singola commessa

CDL Consulente del Lavoro

REC Responsabile Esterno Contabilità

RIA Responsabile IA

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di IDRAGEST S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l.;
- Decreto Legislativo 4 settembre 2024, n. 138 (Recepimento Direttiva NIS 2);
- Regolamento di Esecuzione (UE) 2024/2690 (Requisiti tecnici e metodologici NIS 2);
- Decreto Legislativo 10 marzo 2023, n. 24 (Decreto Whistleblowing);
- Codice Penale (artt. 491-bis, 615-ter, 617-quater, 629, 635-bis, etc.).
- Decreto Legislativo 4 settembre 2024, n. 138, art. 23;
- Regolamento di esecuzione (UE) 2024/2690;
- Legge 23 settembre 2025, n. 132, art. 11.

4 CAMPO DI APPLICAZIONE E RESPONSABILI DELLA PROCEDURA

Il presente protocollo deve essere osservato da tutte le Funzioni Aziendali coinvolte nella gestione e nell'utilizzo dei sistemi informatici della società.

Sono responsabili della procedura le funzioni aziendali coinvolte per ragioni del proprio incarico nella gestione e nell'utilizzo delle rete informatiche e, dunque, il PRES, il RSPP, il RSGQ, il RTEC, il RPROG, il RFAM, ed il RAM/RUU e tutti i dipendenti che utilizzano ed hanno accesso ai sistemi informatici della Società.

Rientrano nel campo di applicazione della presente procedura anche i dipendenti, collaboratori e funzioni aziendali espressamente autorizzati all'utilizzo di sistemi di intelligenza artificiale secondo quanto previsto dalla policy IA adottata da IDRAGEST.

5 I REATI INFORMATICI E DI INDEBITO UTILIZZO DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

I REATI PRESUPPOSTO ELENCATI DALL'ART. 24 BIS DEL D. LGS. 231/2001 SONO:

IL PROCESSO DI GESTIONE E UTILIZZO DEGLI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI SI ARTICOLA NEI SEGUENTI PROCESSI:

• Carte di pagamento (carte di debito e di servizio, carte di credito, carte prepagate);

• Incassi e pagamenti (es. assegni, bonifici, addebiti diretti, RIBA – MAV – effetti);

• Servizi di Accesso ai Canali Digitali (accesso ed identificazione a distanza destinati a persone fisiche e persone giuridiche, altri servizi);

• Prevenzione delle frodi (Security Fraud Management);

• Gestione Reclami lamentele e disconoscimenti (Customer Relationship Management)

• Gestione risorse Umane con riferimento alle carte di credito aziendali e se rilasciate ai Dipendenti anche i buoni pasto e le carte di servizio per le autovetture (carta carburante, telepass).

5.1 ART. 615 TER C.P. - ACCESSO ABUSIVO AD UN SISTEMA TELEMATICO O INFORMATICO

La L. n. 90/2024 ha modificato il testo dell'art. 615 -ter c.p. che disponeva "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o

comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede si procede d'ufficio."

Il reato è commesso da chi abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo.

Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema; può pertanto realizzarsi anche qualora lo scopo sia quello di dimostrare la propria abilità e la vulnerabilità dei sistemi altrui, anche se più frequentemente l'accesso abusivo avviene al fine di danneggiamento o è propedeutico alla commissione di frodi o di altri reati informatici.

Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali: verificarsi della distruzione o del danneggiamento dei dati, dei programmi o del sistema, o dell'interruzione totale o parziale del suo funzionamento; o quando si tratti di sistemi di interesse pubblico o di fatti compiuti con abuso della qualità di operatore del sistema.

Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati della Società, mediante l'utilizzo delle credenziali di altri colleghi abilitati.

Orbene, è evidente come le modifiche introdotte dalla citata disposizione sono volte ad ampliare l'ambito di applicazione della fattispecie e a inasprire il trattamento sanzionatorio elevando le pene previste.

Infatti, "il primo profilo: - l'aggravante di cui al secondo comma, n. 2, è prevista non soltanto se il colpevole per commettere il fatto usa violenza sulle cose o sulle persone, ma anche se usa minaccia (n. 1, 1.2); l'aggravante di cui al secondo comma, n. 3, è prevista anche se dal fatto deriva la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare, dei dati (n. 1, 1.3)".

Invece, sotto "il profilo dell'inasprimento delle pene: .- nella fattispecie aggravata ai sensi del secondo comma è prevista la pena della reclusione da 2 a 10 anni (attualmente è da 1 a 5 anni) (n. 1, 1.1); - nella fattispecie aggravata ai sensi del terzo comma è prevista la pena della reclusione da 3 a 10 anni (attualmente è da 1 a 5 anni) (n. 2); - nella fattispecie pluriaggravata in cui ricorrano l'aggravante di cui al terzo comma nonché taluna delle aggravanti di cui al secondo comma è prevista la pena della reclusione da 4 a 12 anni (attualmente è da 3 a 8 anni) (n. 2)".

5.2 ART. 635 BIS C.P. - DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (MODIFICATO DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

L'art. 635 bis c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime, informazioni, dati o programmi informatici altrui.
Secondo un'interpretazione rigorosa, nel concetto di "programmi altrui" potrebbero ricomprendersi anche i programmi utilizzati dal soggetto agente in quanto a lui concessi in licenza dai legittimi titolari.
Dunque, tale fattispecie reato si realizza quando un soggetto "*distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui*".
Con la Legge n.90 del 28 giugno 2024 si è avuto un inasprimento della pena, in due casi:
1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato

Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.
Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore.

5.3 ART. 635 TER C.P. - DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI PUBBLICI O DI INTERESSE PUBBLICO (MODIFICATO SIA NELLA RUBRICA CHE NEL TESTO DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

L'art. 635 bis c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera, sopprime, informazioni, dati o programmi informatici altrui.
Secondo un'interpretazione rigorosa, nel concetto di "programmi altrui" potrebbero ricomprendersi anche i programmi utilizzati dal soggetto agente in quanto a lui concessi in licenza dai legittimi titolari.
L'art. 635 ter c.p., salvo che il fatto costituisca più grave reato, punisce le condotte anche solo dirette a produrre gli eventi lesivi descritti dall'articolo che precede, a prescindere dal prodursi in concreto del

risultato del danneggiamento, che se si verifica costituisce circostanza aggravante della pena. Deve però trattarsi di condotte dirette a colpire informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti, o comunque di pubblica utilità. Rientrano pertanto in tale fattispecie anche le condotte riguardanti dati, informazioni e programmi utilizzati da Enti privati, purché siano destinati a soddisfare un interesse di pubblica necessità.

Entrambe le fattispecie sono aggravate se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema. Il primo reato è perseguibile a querela della persona offesa o d'ufficio, se ricorre una delle circostanze aggravanti previste; il secondo reato è sempre perseguibile d'ufficio.

Si riporta integralmente il testo sostituito dalla Legge n.90 del 28 giugno 2024:

"*Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni. La pena è della reclusione da tre a otto anni:*

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)"

Tale reato si realizza quando un soggetto commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici pubblici o di interesse pubblico.

Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato.

5.4 ART. 635 QUATER C.P. - DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI E ART. 635 QUINQUIES C.P. - DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ

L'art. 635 quater c.p. che prevedeva "*Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.*

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata." è stato modificato dalla L. n 90/2024 e precisamente 1) al primo comma, le parole: «da uno a cinque anni» sono sostituite dalle seguenti: «da due a sei anni»; 2) il secondo comma è sostituito dal seguente: "La pena e' della reclusione da tre a otto anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato".

L' art. 635 quater c.p. punisce, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'art. 635 bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. Per dirsi consumato il reato in oggetto, il sistema su cui si è perpetrata la condotta criminosa deve risultare danneggiato o reso, anche in parte, inservibile o ne deve venire ostacolato il funzionamento.

L'art. 635 quinquies c.p. punisce le medesime condotte descritte nell'articolo che precede anche se gli eventi lesivi non si realizzino in concreto; il loro verificarsi costituisce circostanza aggravante della pena (va però osservato che il concreto ostacolo al funzionamento del sistema non rientra espressamente fra gli "eventi" aggravanti). Deve però trattarsi di condotte che mettono in pericolo sistemi informatici o telematici di pubblica utilità.

In questa previsione, a differenza di quanto previsto all'art. 635 ter, non vi è più alcun riferimento all'utilizzo da parte di Enti pubblici: per la configurazione del reato in oggetto, parrebbe quindi che i sistemi aggrediti debbano essere semplicemente "di pubblica utilità"; non sarebbe cioè, da un lato,

sufficiente l'utilizzo da parte di Enti pubblici e sarebbe, per altro verso, ipotizzabile che la norma possa applicarsi anche al caso di sistemi utilizzati da privati per finalità di pubblica utilità.

Entrambe le fattispecie sono perseguibili d'ufficio e prevedono aggravanti di pena se i fatti sono commessi con violenza alle persone o minaccia, o con abuso della qualità di operatore di sistema.

Le novità introdotte dalla citata normativa in relazione a tale norma incriminatrice, prevedono l'innalzamento della pena per la fattispecie semplice, con la reclusione da 2 a 6 anni (anziché da 1 a 5 anni); l'ampliamento della fattispecie aggravata; la ridefinizione della pena per la fattispecie aggravata, con la reclusione da 3 a 8 anni (anziché l'aumento fino a un terzo previsto dal testo previgente).

5.5 ART. 491 BIS C.P. - FALSITÀ NEI DOCUMENTI INFORMATICI

L'art. 491 bis c.p. dispone che ai documenti informatici pubblici aventi efficacia probatoria si applichi la medesima disciplina penale prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, previste e punite dagli articoli da 476 a 493 del codice penale. Si citano in particolare i reati di falsità materiale o ideologica commessa da pubblico ufficiale o da privato, falsità in registri e notificazioni, falsità ideologica in certificati commessa da persone esercenti servizi di pubblica necessità, uso di atto falso.

Il concetto di documento informatico è nell'attuale legislazione svincolato dal relativo supporto materiale che lo contiene, in quanto l'elemento penalmente determinante ai fini dell'individuazione

5.6 ART. 640 QUINQUIES C.P. - FRODE INFORMATICA DEL SOGGETTO CHE PRESTA SERVIZI DI CERTIFICAZIONE DI FIRMA ELETTRONICA

Tale reato è commesso dal soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato. Il soggetto attivo del reato può essere soltanto un soggetto "certificatore qualificato", che esercita particolari funzioni di certificazione per la firma elettronica qualificata.

Si tenga comunque presente che – per assumere rilevanza penale – la violazione degli obblighi per il rilascio di un certificato qualificato deve essere assistita dal dolo specifico sopra evidenziato (perseguimento di un ingiusto profitto / danno altrui).

5.7 ART. 629, 3° COMMA, C.P. ESTORSIONE (INTRODOTTO DALLA LEGGE N.90 DEL 28 GIUGNO 2024)

La Legge n. 90 del 2024 ha introdotto l'art. 629, 3°comma, c.p. il quale dispone che "*Chiunque, mediante le condotte di cui agli articoli 615 ter, 617 quater, 617 sexies, 635 bis, 635 quater e 635 quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità*".

Il reato si configura quando qualcuno, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies, minaccia o costringe taluno a compierle o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno.

Il recente provvedimento, dunque, costruisce una nuova fattispecie criminosa, sanzionandola più aspramente dell'estorsione semplice (che è punita oggi con una pena massima di dieci anni di reclusione). Una cornice edittale che si inasprisce in maniera significativa nel caso in cui sussistano talune circostanze aggravanti. Basti pensare che, sulla scorta delle nuove prescrizioni dettate dalla Legge, nell'ipotesi in cui la condotta penalmente rilevante venga posta in essere a danno di una persona incapace per età o per infermità, il reato è punito con la reclusione fino a ventidue anni di reclusione.

6 REATI PRESUPPOSTO STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

Il Decreto legislativo 184/2021 ha introdotto nel catalogo dei reati presupposto della responsabilità dell'ente i delitti in materia di strumenti di pagamento diversi dai contanti inserendo: **1)** l'aggravante di cui all'art. 640 ter, comma 2, c.p.; **2)** le modifiche all'art. 493 ter c.p.; **3)** ed, ex novo, l'art. 493 quater c.p. Caratteristiche e contesto di detti reati fanno sì che gli stessi possano essere ricondotti nell'Area sensibile dei reati informatici fermo che, anche in questo caso, le attività sensibili previste in quest'area, ricomprendente reati che possono generare proventi illeciti, si devono intendere predisposte anche al fine della prevenzione dei reati di riciclaggio in senso lato.

SI ILLUSTRANO DI SEGUITO I REATI INTRODOTTI DALL'ART. 25.OCTIES.1:

FRODE INFORMATICA CHE PRODUCE TRASFERIMENTO DI DENARO, DI VALORE MONETARIO O DI VALUTA VIRTUALE (ART. 640 TER, COMMA 2).

La fattispecie consiste nell'alterare il funzionamento di un sistema informatico o telematico o nell'intervenire senza diritto sui dati, informazioni o programmi in essi contenuti, ottenendo un ingiusto profitto. La circostanza aggravante che il fatto produca un trasferimento di denaro, di valore monetario o di valuta virtuale determina anche la responsabilità dell'Ente senza bisogno che il soggetto passivo sia lo Stato, la Pubblica Amministrazione o l'UE

INDEBITO UTILIZZO E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (493 TER C.P.)

La fattispecie punisce la condotta di chi, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque ogni altro strumento di pagamento diverso dai contanti.

Viene punita anche la condotta di chi, al fine di trarne profitto per sé o per altri, falsifica o altera gli strumenti o i documenti di cui al primo periodo, ovvero possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

Il rischio di commissione di tale reato può in teoria configurarsi in tutte le realtà aziendali ed in particolare in tutti i processi aziendali interessati dalla movimentazione di flussi finanziari, in relazione alle differenti tipologie di strumenti di pagamento diverse dai contanti.

In particolare, sono sensibili tutte le attività che rendono possibile l'accesso a dati identificativi, credenziali, etc., funzionali all'eventuale utilizzo indebito di strumenti di pagamento (diversi dai contanti) di titolarità di terzi, quali ad esempio le carte di credito.

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.)

Salvo che il fatto costituisca più grave reato, la fattispecie punisce chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a se' o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo.

La condotta descritta potrebbe riscontrarsi nell'ambito di quelle attività che comportano la gestione e/o la diffusione di strumenti di pagamento diversi dai contanti e negli ambienti tecnologici a supporto di dette attività.

L'articolo 25 octies.1 del D.Lgs. 231/2001, ha inoltre esteso il catalogo dei reati presupposto a "*ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale*" a condizione che ne siano oggetto materiale "*strumenti di pagamento diversi dai contanti*".

7 GOVERNANCE E GESTIONE DEL RISCHIO DI CIBERSICUREZZA (IN ATTUAZIONE DEL D.LGS. 138/2024)

In linea con il quadro normativo NIS 2, la gestione della cibersicurezza è un'attività di governance strategica, fondata sui seguenti pilastri:

7.1 RESPONSABILITÀ E SUPERVISIONE DELL'ORGANO AMMINISTRATIVO

Ai sensi dell'art. 23 del D.Lgs. 138/2024, l'Organo Amministrativo (CDA) di IDRAGEST:

Approva formalmente le misure di gestione dei rischi per la sicurezza informatica definite nella presente procedura e ne sorveglia la corretta e costante implementazione.

È direttamente responsabile per le violazioni degli obblighi in materia di cibersicurezza.

È tenuto a seguire una formazione specifica e periodica in materia di sicurezza informatica, per acquisire le conoscenze necessarie a individuare i rischi e valutarne l'impatto sui servizi offerti.

Promuove l'offerta di analoga formazione a tutti i dipendenti.

Nomina almeno una persona che riferisca direttamente all'organo stesso sulle questioni di cibersicurezza.

7.2 APPROCCIO BASATO SUL RISCHIO E MISURE MINIME DI SICUREZZA

La Società adotta un approccio basato su un'analisi "multirischio", considerando non solo le minacce dolose ma anche i rischi operativi (es. errore umano, guasto tecnico). Le misure di sicurezza sono adeguate e proporzionate al rischio identificato e, ai sensi dell'art. 24 del D.Lgs. 138/2024, devono includere come minimo:

1. Politiche di analisi dei rischi e di sicurezza dei sistemi informativi.
2. Procedure per la gestione degli incidenti.

3. Piani di continuità operativa (Business Continuity), quali la gestione dei backup e il ripristino in caso di disastro (Disaster Recovery).
4. Sicurezza della catena di approvvigionamento (supply chain), includendo la valutazione dei rischi derivanti dai rapporti con fornitori e prestatori di servizi.
5. Procedure per la gestione e la divulgazione delle vulnerabilità.
6. Politiche e procedure per valutare l'efficacia delle misure adottate.
7. Pratiche di "igiene informatica" di base e formazione continua del personale.
8. Politiche sull'uso della crittografia e, ove opportuno, della cifratura.
9. Sicurezza del personale, politiche di controllo dell'accesso e gestione degli asset informatici.

8 ATTIVITA AZIENDALI SENSIBILI E PRINCIPI GENERALI DI COMPORTAMENTO

PREVENZIONE REATI INFORMATICI RIGUARDANTI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI:

Le attività aziendali sensibili di IDRAGEST, nelle quali possono essere commessi i reati informatici (ivi compresi i reati di "Frode informatica che produce trasferimento di denaro, di valore monetario o di valuta virtuale" e "Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti") e trattati in modo illecito i dati aziendali informatici, sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione.

All'uopo, IDRAGEST ha predisposto appositi presidi organizzativi e si è dotata di adeguate soluzioni di sicurezza, in conformità alla normativa europea e nazionale in materia di protezione dei dati personali, per prevenire e controllare i rischi in tema di tecnologia dell'informazione (IT) e di Cybersecurity, a tutela del proprio patrimonio informativo, della clientela e dei terzi.

Invero, per Patrimonio Informativo Aziendale s'intende un coacervo di categorie di informazioni assolutamente eterogenee, concernenti non solo i dati espliciti, ovvero le informazioni strutturate (ad esempio, in database) o quelle formalizzate (in documenti e nei sistemi informativi: procedure, policy, contratti, piani, progetti), ma anche le informazioni nella posta elettronica, nonché i software e tutte le informazioni facilmente individuabili perché contenute in un supporto, fisico o digitale.

Ancora, per quanto attiene il reato di Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti ed ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende

il patrimonio previsto dal Codice penale, a condizione che ne siano oggetto materiale strumenti di pagamento diversi dai contanti, le attività aziendali sensibili della Società nelle quali può essere commessa questa tipologia di reato, riguardano tutti i processi aziendali che comportano la movimentazione di flussi finanziari sia di IDRAGEST, che per conto della propria clientela, attraverso le differenti tipologie di strumenti di pagamento diverse dai contanti e dei relativi applicativi.

Orbene, tutte le Funzioni Aziendali che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione e utilizzo dei sistemi informatici aziendali, devono rispettare le prescrizioni sopra individuate e, in particolare:

- ✓ intercettare, impedire e/o interrompere l'utilizzo di ogni dispositivo, oggetto o record protetto, materiale o immateriale, o una loro combinazione, diverso dalla moneta a corso legale, che da solo o unitamente a una procedura o ad una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario anche attraverso mezzi di scambio digitale;
- ✓ intercettare, impedire e/o interrompere l'utilizzo di apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere reati riguardanti gli strumenti di pagamento diversi dai contanti o sono specificamente adattati al medesimo scopo;
- ✓ intercettare, impedire e/o interrompere l'utilizzo dispositivi finalizzati al trasferimento di denaro, di valore monetario o di valuta virtuale;
- ✓ intercettare trasferimenti illeciti di mezzi di pagamento diversi dal contante;
- ✓ vietare ed ostacolare la diffusione e l'installazione abusiva di apparecchiature ed altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche, nonché le condotte atte a danneggiare o interrompere un sistema informatico o telematico.

9 I REATI INFORMATICI DI GESTIONE ED UTILIZZO DEI SISTEMI INFORMATICI DEL PATRIMONIO INFORMATIVO DI IDRAGEST

L'utilizzo e la gestione di sistemi informatici e del Patrimonio Informativo sono attività imprescindibili per l'espletamento del business aziendale e contraddistinguono la maggior parte dei processi della IDRAGEST.

Si rendono quindi necessarie una efficace e stringente definizione di norme e misure di sicurezza organizzative, comportamentali e tecnologiche e la realizzazione di attività di controllo, peculiari del

presidio a tutela di una gestione e di un utilizzo dei sistemi informatici e del Patrimonio Informativo di IDRAGEST in coerenza con la normativa vigente.

Alla luce delle considerazioni che precedono, di seguito si declinano i processi sui quali si basa il presidio posto in essere sulla gestione e sull'utilizzo dei sistemi informatici e del Patrimonio Informativo di IDRAGEST.

IL PROCESSO DI GESTIONE DELLA SICUREZZA INFORMATICA SI ARTICOLA NELLE SEGUENTI FASI:

• analisi del rischio IT e definizione dei requisiti di sicurezza informatica;

• gestione Accessi Risorse Informatiche e Servizi di Sicurezza ICT;

• monitoraggio eventi sicurezza informatica e gestione eventi critici di sicurezza informatica;

• sicurezza delle terze parti;

• diffusione della cultura di sicurezza informatica;

• progettazione e realizzazione soluzioni di sicurezza informatica.

IL PROCESSO DI PREVENZIONE FRODI SI ARTICOLA NELLE SEGUENTI FASI:

• identificazione delle misure atte al rafforzamento della prevenzione;

• monitoraggio dell'evoluzione delle frodi informatiche;

• gestione delle comunicazioni con le Autorità Competenti.

IL PROCESSO DI GESTIONE DELLA SICUREZZA FISICA SI ARTICOLA NELLE SEGUENTI FASI:

• gestione protezione di aree e locali ove si svolge l'attività;

• gestione sicurezza fisica dei sistemi periferici.

IL PROCESSO DI GESTIONE E SUPPORTO ICT (*INFORMATION AND COMUNICATION TECHNOLOGIES*) SI ARTICOLA NELLE SEGUENTI FASI:

• erogazione dei servizi ICT;

• monitoraggio del funzionamento dei servizi ICT e gestione delle anomalie;

• assistenza agli utenti attraverso attività di Help desk e problem solving.

Il processo di gestione delle comunicazioni alle Autorità Preposte per la definizione, gestione e controllo del "Perimetro di sicurezza nazionale cibernetica" si articola, nel rispetto degli attesi provvedimenti attuativi del Governo nelle seguenti fasi:

• individuazione delle informazioni ed eventi che devono essere oggetto di comunicazione/segnalazione;

• trasmissione, a seconda delle Autorità Preposte, della comunicazione/segnalazione a cura delle funzioni compenti.

10 ATTIVITA AZIENDALI SENSIBILI E PRINCIPI GENERALI DI COMPORTAMENTO

PREVENZIONE REATI INFORMATICI SULLA GESTIONE ED UTILIZZO DEI SISTEMI INFORMATICI

Le Funzioni Aziendali, a qualsiasi titolo coinvolte nelle attività di gestione ed utilizzo di sistemi informatici e del Patrimonio Informativo della Società, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa intern,a nonché le eventuali previsioni del Codice Etico e del Codice Interno di Comportamento di IDRAGEST.

IN PARTICOLARE:

• le Funzioni Aziendali coinvolte nei processi devono predisporre e mantenere il censimento degli applicativi che si interconnettono con la Pubblica Amministrazione o con le Autorità di Vigilanza e/o dei loro specifici software in uso;

• i soggetti coinvolti nel processo devono essere appositamente incaricati;

• ogni dipendente/amministratore del sistema è tenuto alla segnalazione al proprio preposto di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente ed attivando l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi ed alle comunicazioni alle Autorità Preposte;

• ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (es. personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la Società dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;

• qualora sia previsto il coinvolgimento di soggetti terzi/outsourcer nella gestione dei sistemi informatici e del Patrimonio Informativo di IDRAGEST, nonché nell'interconnessione/utilizzo dei software della Pubblica Amministrazione o delle Autorità di Vigilanza, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001 e, più in particolare, a titolo meramente esemplificativo e non esaustivo:

• introdursi abusivamente, direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate o di utilizzare indebitamente, falsificare o alterare strumenti di pagamento diversi dai contanti;

• accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati di IDRAGEST, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;

• intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;

• utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, worm, troian, spyware, dialer, keylogger, rootkit, ecc.) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;

• distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;

• introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;

• detenere, procurarsi, riprodurre o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;

• produrre, importare, esportare, vendere, trasportare, distribuire, mettere a disposizione o in qualsiasi modo procurare a sé o ad altri apparecchiature, dispositivi o programmi informatici progettati principalmente per commettere reati riguardanti strumenti di pagamento diversi dai contanti o adattati a tale scopo;

• procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;

• alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;

• produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;

• porre in essere mediante l'accesso alle reti informatiche condotte illecite costituenti violazioni di diritti sulle opere dell'ingegno protette, quali, a titolo esemplificativo:

o diffondere in qualsiasi forma opere dell'ingegno non destinate alla pubblicazione o usurparne la paternità;

o detenere qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione dei programmi di elaborazione;

o rimuovere o alterare informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti;

• omettere di comunicare entro i termini prescritti dalla normativa vigente in materia di "sicurezza nazionale cibernetica" dati, informazioni o elementi di fatto rilevanti;

• esibire documenti e dati incompleti e/o comunicare dati falsi o alterati nell'ambito delle comunicazioni in materia di "sicurezza nazionale cibernetica".

I Responsabili sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

Le Funzioni Aziendali che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione e utilizzo dei sistemi informatici aziendali, devono rispettare le prescrizioni sopra individuate e,

IN PARTICOLARE:

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- effettuare verifiche periodiche delle credenziali utente al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi;
- applicare, nell'utilizzo dei sistemi informatici aziendali, regole atte ad assicurare l'aggiornamento delle *password* dei singoli utenti;
- garantire che la sicurezza fisica dell'infrastruttura tecnologica della Società sia utilizzata nel rispetto delle regole interne ed in modo da consentire un monitoraggio delle attività di gestione e manutenzione sulla stessa;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso ai sistemi informatici altrui, con l'obiettivo di acquisire abusivamente informazioni e/o distruggere dati contenuti nei suddetti sistemi informatici, utilizzare abusivamente codici d'accesso a sistemi informatici e telematici, nonché procedere alla diffusione degli stessi;

- porre in essere condotte miranti alla distruzione e/o all'alterazione dei documenti informatici aventi finalità probatoria in assenza di una specifica autorizzazione;
- utilizzare e/o installare programmi diversi da quelli autorizzati;
- aggirare e/o tentare di aggirare i meccanismi di sicurezza aziendali (*antivirus*, *firewall*, *proxy server*, *etc.*);
- rivelare a terzi le proprie credenziali di autenticazione (nome utente e *password*) alla rete aziendale e/o ad altri siti e/o sistemi comunque connessi all'attività della Società;
- detenere e/o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- intercettare, impedire e/o interrompere comunicazioni informatiche o telematiche illecite;
- accedere a pagine *web* con contenuti pedopornografici.

Tuttavia, a seguito dell'introduzione della Legge 90/2024, che mira ad aumentare la sicurezza informatica per difendersi dai cyber-attacchi, aumentando le sanzioni previste per i c.d. "computer crimes", IDRAGEST ha aggiunto ulteriori precisazioni e norme di comportamento a quelle dià sopra dettagliatamente indicate.

10.1 L'ACCESSO AI SISTEMI INFORMATICI, ACQUISTO E CONTROLLO DI *SOFTWARE - HARDWARE*

L'eventuale acquisto da parte della Società di nuovi *software* deve essere debitamente approvato dall'Organo amministrativo, previa acquisizione della dichiarazione della casa madre di conformità del *software* al Regolamento Europeo n. 679/2016 (*privacy by design* e *by default*).

È obbligatorio l'utilizzo di *software antivirus* e *firewall* costantemente aggiornati automaticamente per protezione contro potenziali attacchi verso l'esterno originati da tutti i server o le *workstations* della Società (postazioni fisse e portatili).

10. 2 L'ACCESSO A SITI DI ENTI PUBBLICI O PRIVATI

L'accesso a siti di enti pubblici o privati che richiede apposita autenticazione da parte della Società è consentito solo a personale specifico e all'uopo autorizzato (tramite *user-id* e *password*, *Token* di autenticazione).

I soggetti che in azienda – il PRES ed il soggetto all'uopo eventualmente incaricato – siano a conoscenza delle credenziali per l'accesso ai sistemi informatici della P.A. o di enti privati sono obbligati a tenere segrete le credenziali di accesso ai sistemi e a conservarle in modo adeguato.

10. 3 I DISPOSITIVI ASSEGNATI A DIPENDENTI O FUNZIONI AZIENDALI

La Società può mettere a disposizione dei dipendenti e/o delle funzioni aziendali appositi dispositivi elettronici, da utilizzare unicamente ai fini dell'espletamento dell'attività aziendale, nel pieno rispetto delle normative in materia di utilizzo e gestione dei sistemi informatici e delle procedure aziendali definite.

In particolare, qualora siano assegnati ai dipendenti dispositivi informatici personali, deve essere redatto verbale di consegna e, all'atto dell'interruzione del rapporto lavorativo (eventuale licenziamento e/o dimissioni) ovvero in caso di guasti o sostituzioni dei predetti dispositivi, il relativo verbale di restituzione.

In caso di smarrimento o furto, dovrà essere data immediata informazione al superiore gerarchico e/o al PRES, che dovrà occuparsi di effettuare la relativa denunzia alle competenti autorità.

È vietato prestare o cedere a terzi qualsiasi apparecchiatura informatica messa a disposizione dalla Società.

I Dipendenti e le Funzioni Aziendali devono, una volta terminata la lavorazione assegnata, salvare i dati nell'archivio Cloud preposto per l'archiviazione e condivisione dei dati.

10.4 USO DELLA RETE INTERNET

La rete *internet* deve essere utilizzata solo per scopi prettamente attinenti all'attività lavorativa e devono essere implementati i meccanismi di protezione della rete. È espressamente vietato utilizzare la rete aziendale per navigare in siti illeciti, ed in particolare pornografici e pedopornografici, nonché dedicati al gioco d'azzardo o altri tipi di giochi *online*.

10. 5 LE *PASSWORD* DI ACCESSO AI DISPOSITIVI

A ciascun dipendente o funzione aziendale, che utilizzi dispositivi aziendali, dovrà essere creata un'utenza personale o *account* corredato da apposita *password*. La *password* del dispositivo potrà essere modificata dal singolo utente, che dovrà avere cura di custodirla.

Le utenze che non verranno utilizzate per più di tre mesi devono essere disabilitate: il PRES o la Funzione eventualmente incaricata dal primo per iscritto, si occuperà della disabilitazione delle utenze.

Il dipendente che venga munito di un dispositivo elettronico mobile o fisso, dovrà accedervi tramite apposita *password* – composta da almeno 8 caratteri, contenente numeri e almeno una lettera composta

da almeno da 8 caratteri, che non dovrà essere riportata su carta o cellulari e dispositivi elettronici in genere.

10. 6 LA GESTIONE DELLA POSTA ELETTRONICA

La gestione della posta elettronica certificata e le *password* di accesso non possono essere diffuse ad altro soggetto diverso dall'Organo amministrativo.

Le P.E.C. in entrata devono essere regolarmente archiviate dal PRES – o da altro componente del CDA, all'uopo incaricato – ed inserite in un registro digitale e/o cartaceo.

L'invio di P.E.C. in uscita deve unicamente avvenire a cura dei componenti del CDA, nonché, previa autorizzazione, da parte del RPROG o di altra funzione aziendale all'uopo autorizzata.

Per quanto riguarda la posta elettronica ordinaria le caselle di posta assegnate ai dipendenti devono riportare il riferimento al nome della Società.

La gestione della posta elettronica aziendale e, pertanto, il trattamento dei dati connesso al suo utilizzo da parte dei soggetti autorizzati, dovrà essere svolta nel pieno rispetto della normativa *privacy* vigente (anche al livello comunitario), nonché di quelle all'uopo previste in relazione ai rapporti di lavoro.

10. 7 L'UTILIZZO DI SUPPORTI MAGNETICI RIMOVIBILI

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, *etc.*), contenenti dati particolari/sensibili, nonché informazioni costituenti *know-how* aziendale, devono essere trattati con particolare cautela al fine di evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

10. 8 IL LICENZIAMENTO O LE DIMISSIONI DI UN DIPENDENTE

Qualora un dipendente interrompa il rapporto di lavoro con l'azienda, per qualsivoglia ragione, è necessario modificare le *password* di cui lo stesso era a conoscenza e/o disabilitare le utenze.

IDRAGEST S.r.l. si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio, la necessità di mantenere attiva in ricezione le utenze – es. la casella postale – per un congruo periodo di tempo, al fine di garantire la funzionalità aziendale.

10.9 LA VARIAZIONE DI DATI NEL SISTEMA INFORMATICO

Eventuali variazioni dei dati inseriti nel sistema informatico e concernenti l'anagrafica Clienti e/o Dipendenti (ad esempio l'IBAN fornitore e/o dipendente, *password, etc.)*, devono essere autorizzate dal Responsabile di funzione e, comunque, comunicate per iscritto al CDA.

10.10 INSTALLAZIONE DI *SOFTWARE* DI TERZE PARTI PER LA FATTURAZIONE

È FATTO DIVIETO AD OGNI FUNZIONE AZIENDALE AUTORIZZATA ALL'UTILIZZO DEI SISTEMI INFORMATICI DI:

- Modificare contenuti e settaggi dei programmi ivi installati;
- procurarsi, riprodurre, diffondere, comunicare e/o consegnare codici, parole chiave e/o altri mezzi idonei al superamento delle misure di sicurezza poste a protezione dei *software.*

Devono essere tempestivamente comunicati all'OdV eventuali aggiornamenti relativi al sistema informatico aziendale (*software*), ad esempio: modifiche e/o integrazioni dei profili autorizzativi, delle funzioni, delle modalità di inserimento dati, del rilevamento accessi, etc.

10.11 L'UTILIZZO DI SISTEMI *CLOUD COMPUTING*

L'utilizzo di sistemi di cd. *cloud computing* è ammesso solo se l'applicativo è conforme al GDPR *compliance.*

10.12 FALSITÀ DI UN DOCUMENTO INFORMATICO O TELEMATICO E UTILIZZO DI *SMARTCARD*

L'utilizzo di *smartcard* per la firma "digitale" di documenti, è consentito solo ed esclusivamente al CDA.
Le credenziali per la firma possono essere detenute anche da altre funzioni o dipendenti, in azienda, ad esempio dal RPROG; tuttavia, ai fini dell'utilizzo è necessario acquisire apposita autorizzazione scritta da parte del PRES.

10.13 DATA BREACH

Ogni dipendente o collaboratore che nell'utilizzo dei dispositivi informatici aziendali in dotazione sospetti o constati l'avvenuta perdita, modifica, comunicazione non autorizzata, diffusione non autorizzata o accesso non autorizzato dei dati personali trattati dall'azienda (quali, a titolo di esempio: furto, smarrimento di supporti, *virus*, *e mail* sospette aperte per errore, *etc.*) è tenuto a informare immediatamente e, comunque, non oltre 24 ore dalla conoscenza di tale evento, il superiore gerarchico e/o il PRES.

L'Organo amministrativo, valutata l'entità e la gravità del *data breach*, effettuerà, entro le 72 ore seguenti, tutti gli adempimenti richiesti dalla legge, notificando la violazione al *Garante Privacy* e agli interessati, ove richiesto. L'Amministratore, inoltre, provvederà ad adottare, immediatamente, tutte le misure di sicurezza idonee ad evitare ulteriori conseguenze dannose, originate dal *data breach* all'Azienda e/o a terzi eventualmente interessati, nonché a prevenire ulteriori *data breach*.

DIVIETO DI PAGAMENTI IN CASO DI DATA BREACH PER RIAVERE I DATI

Nel caso di infezione del sistema informatico della Società causato da *crypto virus* o analoghi *virus* che bloccano, carpiscono, oscurano, sottraggono i dati, oltre ad attivare la procedura di *data breach* prescritta dalla legge, qualora esse siano corredate da richieste di riscatto di denaro o altra utilità per rientrare in possesso dei dati o per evitare altre conseguenze dannose derivanti dall'utilizzo o la perdita dei dati personali e non, della Società, il PRES dovrà denunciare il fatto alle competenti autorità. È fatto divieto di corrispondere denaro, *bitcoin* o altre utilità a titolo di riscatto e, comunque, per rientrare in possesso dei dati o per evitare altre azioni dannose per la società.

10. 14 PREVISIONE DI UNA PROCEDURA DI *DISASTER RECOVERY*

Al fine di evitare possibili violazioni dei dati personali e/o aziendali, è obbligatorio che, su tutti i pc aziendali fissi o mobili, venga effettuato settimanalmente un *backup* dei dati. Inoltre, verrà effettuato un *backup* delle macchine virtuali, contenti i *database* aziendali.

11 I DIVIETI

Le predette attività di controllo costituiscono valido presidio, anche a garanzia della tracciabilità delle modifiche apportate alle procedure informatiche, della rilevazione degli utenti che hanno effettuato tali modifiche e di coloro che hanno effettuato i controlli sulle modifiche apportate.

In ogni caso, le attività di gestione ed utilizzo dei sistemi informatici aziendali devono essere assoggettate ad una costante attività di controllo, attraverso l'utilizzo di adeguate misure per la protezione delle informazioni, salvaguardandone la riservatezza, l'integrità e la disponibilità, con particolare riferimento al trattamento dei dati personali.

IN OGNI CASO, È FATTO DIVIETO DI:

- Installare, nella rete aziendale di IDRAGEST S.r.l., programmi/*software* privi di licenza che non rientrino nello scopo per cui il sistema informatico è stato assegnato all'utente;

- distruggere e/o alterare documenti informatici, aventi finalità probatoria in assenza di una specifica autorizzazione dell'amministratore;
- per ciascun dipendente, di rivelare le proprie credenziali di autenticazione (nome utente e *password*) alla rete aziendale o anche ad altri siti/sistemi;
- copiare documenti e materiali protetti da *copyright,* senza l'autorizzazione espressa del detentore, salvi i casi in cui tali attività rientrino nel normale svolgimento delle funzioni affidate;
- effettuare l'*upload* e il *download* di *software* gratuiti (*freeware* e *shareware*), nonché l'utilizzo di documenti provenienti da siti *web* o *http*, se non strettamente attinenti all'attività lavorativa e previa verifica dell'attendibilità dei siti in questione;
- installare autonomamente programmi provenienti dall'esterno sui *computer* di IDRAGEST, tali da agevolare il rischio di introduzione di *virus* informatici e/o di alterazione della funzionalità delle applicazioni *software* esistenti;
- effettuare collegamenti alla rete con modalità difformi dall'architettura informatica prevista;
- utilizzare la casella di posta elettronica "personale" per trasmettere documenti e allegati vari al di fuori della rete informatica aziendale, ciò al fine di garantire la sicurezza e la *privacy* delle informazioni trattate;
- prendere parte a *blog*, dibattiti non attinenti al lavoro con la propria postazione aziendale di accesso alla rete;
- manomettere, in qualunque modo, il funzionamento di un sistema informatico; in particolare aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (*antivirus*, *firewall*, *proxy*, *server*);
- entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- modificare la configurazione aziendale del personal computer in dotazione ed utilizzare software diversi o aggiuntivi rispetto a quelli coperti da licenza d'uso o, comunque, installati dalla Società, salvo espressa autorizzazione del Responsabile della Funzione Aziendale all'uopo preposta e purchè si tratti di software necessari allo svolgimento dell'attività lavorativa;
- installare e/o utilizzare programmi, dispositivi, software o qualsiasi altro strumento informatico che permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali;
- detenere, diffondere ed installare abusivamente apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici;

- detenere, diffondere ed installare abusivamente apparecchiature ed altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- detenere, diffondere ed installare abusivamente apparecchiature, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema telematico protetto da misure di sicurezza, al fine di procurare a sé o ad altri un profitto o arrecare un danno ad altri;
- detenere, diffondere ed installare abusivamente apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- danneggiare un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, detenendo, producendo, riproducendo, importando, diffondendo, comunicando, consegnando o mettendo a disposizione di terzi o installando apparecchiature, dispositivi o programmi informatici;
- intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrente tra più sistemi, impedendole o interrompendole;
- detenere, diffondere ed installare abusivamente apparecchiature e altri mezzi atti ad intercettare, impedire ed interrompere comunicazioni informatiche o telematiche;
- detenere materiale pornografico realizzato utilizzando minori degli anni diciotto;
- utilizzare sistemi informatici o appositi siti internet per l'adescamento di minori;
- diffondere notizie false o porre in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione di strumenti finanziari (art. 185 TUF).

12 LEGGE N. 90 DEL 2024 – CYBERSICUREZZA

La Legge n. 90 del 2024, c.d. "legge sulla Cybersicurezza" interviene anche sul catalogo dei reati presupposto in materia di responsabilità amministrativa degli enti, contemplati nel decreto legislativo n. 231 del 2001. In particolare, il legislatore:

1. Ritocca il contenuto dell' articolo 24-bis, relativo ai reati informatici, aumentando le sanzioni previste all'interno del suo comma 1, le quali passano da una cornice edittale ricompresa tra cento e cinquecento quote, ad una ricompresa tra duecento e settecento quote.
2. Aggiunge all'articolo 24-bis il nuovo comma 1-bis, ai sensi del quale si applica all'ente la sanzione pecuniaria da trecento a ottocento quote a seguito della commissione della nuova fattispecie di reato –introdotta sempre dalla Legge sulla Cybersicurezza – legata all'estorsione informatica di cui all'

articolo 629, comma 3, del codice penale. Nei casi di condanna, inoltre, è prevista anche l'applicazione delle sanzioni interdittive previste dall' articolo 9, comma 2, del decreto legislativo n. 231/2001, per una durata non inferiore a due anni.

Invero, è evidente come il legislatore, attraverso il combinato disposto del comma 3 dell' articolo 629 del codice penale e del comma 1-bis dell' articolo 24-bis del decreto legislativo n. 231/2001, tenti di limitare la piaga estorsiva discendente, anzitutto, dagli attacchi informatici di tipo ransomware, provando a creare anche un argine al dilagare dei pagamenti dei riscatti richiesti dalle organizzazioni criminali.

Tuttavia, l'introduzione nel nostro ordinamento del reato di estorsione informatica, teso a punire con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000 "*chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno*", difficilmente potrà modificare da sola lo scenario criminale legato agli attacchi ransomware nei confronti dell'Italia, che vede agire – nella quasi totalità dei casi – soprattutto soggetti al di fuori dei nostri confini nazionali.

Il medesimo ragionamento vale anche per quanto previsto al comma 1-bis dell' articolo 24-bis del decreto legislativo n. 231/2001, il quale, nei fatti, introduce correttamente la responsabilità amministrativa dell'ente, unitamente alle discendenti sanzioni interdittive personali, ma solo nel caso in cui, semplificando, il reato di estorsione informatica sia commesso da un soggetto appartenente all'ente stesso. Un'ipotesi, questa, certamente possibile e, quindi, senz'altro da regolamentare, ma che nella quotidianità dei reati informatici appare forse come un "caso limite" e che, purtroppo, potrebbe avere poco impatto sul dilagare – soprattutto nel mondo privato – dei pagamenti di riscatti a seguito di attività estorsive condotte, ad esempio, attraverso attacchi ransomware.

3. Modifica il comma 2 dell'articolo 24-bis, relativo alla commissione dei delitti di cui agli articoli 615-quater ("Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici e telematici") e 615-quinquies ("Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico") del codice penale, innalzando la sanzione pecuniaria ivi prevista sino a quattrocento quote.

4. Sostituisce tra i reati presupposto per i quali è prevista l'applicazione all'ente della sanzione pecuniaria di cui al precede al punto 3., il riferimento all'articolo 615-quinquies c.p., abrogato proprio dalla Legge sulla Cybersicurezza, con il richiamo al nuovo delitto di detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico di cui all'articolo 635-quater.1.

12.1 I CONTROLLI PER LA PREVENZIONE DEI REATI INFORMATICI

È fatto obbligo alla Società di attivarsi, con cadenza semestrale, per porre in essere le azioni necessarie all'adeguato e corretto funzionamento del sistema informatico aziendale. Tali adempimenti dovranno essere realizzati da un esperto informatico (anche interno alla Società) all'uopo autorizzato dal PRES.

IL TECNICO INCARICATO DOVRÀ, IN PARTICOLARE:

- verificare la sicurezza della rete e dei sistemi informativi aziendali ed identificare le potenziali vulnerabilità nel sistema dei controlli IT;
- effettuare le attività di verifica dell'esistenza dei *backup*. Di tale attività deve essere conservata un'evidenza documentale; in caso di intervento di soggetto interno alla Società, quest'ultimo dovrà redigere apposito verbale inerente l'attività svolta, sottoscritto anche dal PRES;
- verificare e vietare le condotte aventi ad oggetto mezzi di pagamento digitali attraverso cui viene scambiata moneta elettronica avente corso legale, ma anche le c.d. criptovalute, prive di valore legale ma socialmente sempre più accettate come mezzi di pagamento;
- verificare la sicurezza della rete e dei sistemi informativi aziendali ed identificare le potenziali vulnerabilità nel sistema dei controlli IT attraverso test periodici (es. vulnerability assessment);
- Effettuare una valutazione dei rischi specifici e della qualità delle pratiche di cybersecurity dei propri fornitori e prestatori di servizi diretti, integrando clausole di sicurezza specifiche nei relativi contratti.

Nel caso in cui l'attività di gestione del sistema informatico dovesse essere svolta da un terzo esterno alla Società – fermo restando l'obbligo di regolamentare il trattamento dei dati ai sensi dell'art. 28 del Regolamento Europeo n. 679/2016 – il responsabile di Funzione coinvolto dovrà predisporre un *report* di intervento completo di data, ora, nominativo del soggetto che ha effettuato l'intervento, la tipologia delle operazioni effettuate e lo scopo. Il *report* sarà sottoscritto dal responsabile di Funzione e dal soggetto che ha effettuato l'intervento, e trasmesso al PRES, il quale provvederà ad apporre apposito visto.

I collegamenti da remoto per manutenzione e/o riparazioni al sistema informatico possono essere effettuati solo previa autorizzazione dell'utente utilizzatore del dispositivo informatico interessato.

Ancora, in ottemperanza agli obblighi imposti dalla Legge n. 90 del 2024, IDRAGEST si impegna a:

- stabilire ed applicare procedure interne per assicurare la sicurezza dei sistemi informatici prevedendo rigide misure di segregazione degli accessi logici, al fine di impedire a soggetti non autorizzati di accedere e manomettere strumentazione informatica;

- implementare sistemi di monitoraggio continuo per identificare tempestivamente eventuali minacce o violazioni;
- valutare la valorizzazione della crittografia come strumento di cybersicurezza, nonché di ogni iniziativa utile al rafforzamento dell'autonomia industriale e tecnologica, valorizzando lo sviluppo di algoritmi proprietari. In tal caso, la Società potrà: **i)** sviluppare e diffondere standard, linee guida e raccomandazioni al fine di rafforzare la cybersicurezza dei sistemi informatici; **ii)** valutare la sicurezza dei sistemi crittografici; **iii)** organizzare e gestire attività di divulgazione finalizzate a promuovere l'utilizzo della crittografia come strumento di cybersicurezza;
- Adozione e implementazione di procedure per la classificazione ed il trattamento delle informazioni, per l'utilizzo di sistemi crittografici in relazione alla trasmissione in rete di documenti informatici, per i controlli tesi a rintracciare eventuali falle o debolezze dei sistemi (es. vulnerability assessment e penetration test, finalizzati a valutare la tenuta del sistema a fronte di eventuali attacchi esterni).
- Predisposizione e aggiornamento, con cadenza almeno annuale, di un elenco delle reti, dei sistemi informativi e dei servizi informatici (che comprenda la relativa architettura e componentistica interna);
- adottare un programma di sensibilizzazione sulla sicurezza delle informazioni con l'obiettivo di rendere i dipendenti – ed in particolare il responsabile della sicurezza informatica - consapevoli delle loro responsabilità per la sicurezza delle informazioni e dei mezzi con cui tali responsabilità vengono assolte. Invero, la società dovrà, con cadenza annuale, eseguire un apposito programma di formazione, in modo da rimanere in linea con le politiche e le procedure organizzative all'uopo previste.
- organizzare programmi di formazione per sensibilizzare i dipendenti in materia di responsabilità amministrativa degli enti con l'intento di evitare che l'azione illecita di un dipendente comporti l'apertura di un procedimento ex Decreto 231 a carico della società.
- promuovere ed assicurare il puntuale rispetto da parte di tutti i Destinatari della presente procedura del regolamento informatico adottato da IDRAGEST e delle relative procedure aventi ad oggetto il corretto utilizzo delle risorse informatiche aziendali, la sicurezza informatica/telematica, la protezione dei dati sensibili.
- Tracciatura e registrazione delle attività eseguite su sistemi, applicazioni e reti, potenzialmente lesive per la sicurezza.
- Verifica periodica delle modalità di accesso ai sistemi, dei log di registrazione delle attività sui sistemi, delle eccezioni e degli eventi concernenti la sicurezza.
- Definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi.

- Adozione di meccanismi di protezione da software pericolosi e procedure di controllo della installazione di software sui sistemi operativi.

12.2 PRESIDI DI CONTROLLO

Gli Organi Sociali, gli Amministratori, i dipendenti, nonché i collaboratori e tutte le altre controparti contrattuali coinvolti nello svolgimento delle attività a rischio hanno l'espresso obbligo di perseguire i seguenti principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi di controllo specifici:

- **Segregazione delle attività**

si richiede l'applicazione del principio di separazione delle attività e dei ruoli che intervengono nelle attività chiave dei processi operativi esposti a rischio, tra chi autorizza, chi esegue e chi controlla; in particolare, deve sussistere separazione dei ruoli di gestione di un processo e di controllo dello stesso; ad esempio: progettazione ed esercizio, acquisto di beni e risorse e relativa contabilizzazione

- **Esistenza di procedure**

devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire i principi di comportamento e le modalità operative per lo svolgimento delle attività sensibili. Le procedure devono definire formalmente le responsabilità e i ruoli all'interno del processo e le disposizioni operative e relativi controlli posti a presidio nelle attività

- **Poteri autorizzativi e di firma**

definire livelli autorizzativi da associarsi alle attività critiche dei processi operativi esposti a rischio

- **Tracciabilità**

tracciabilità degli accessi e delle attività svolte sui sistemi informatici che supportano i processi esposti a rischio; ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione distruzione delle registrazioni effettuate

- **Gestione delle segnalazioni**

raccolta, analisi e gestione delle segnalazioni di fattispecie a rischio per i reati informatici rilevati da soggetti interni e esterni all'ente

- **Riporto all'OdV**

riferire prontamente all'OdV eventuali situazioni di irregolarità

12.3 PRINCIPI PROCEDURALI SPECIFICI

In particolare, si elencano qui di seguito le regole che devono essere rispettate dalla società e dai dipendenti e dagli altri soggetti eventualmente autorizzati nell'ambito delle Attività Sensibili:

- I dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come riservati
- È vietato introdurre in azienda computer, periferiche, altre apparecchiature o software senza preventiva autorizzazione del soggetto responsabile individuato
- È vietato in qualunque modo modificare la configurazione di postazioni di lavoro fisse o mobili effettuata dal servizio infrastrutture
- È vietato acquisire, possedere o utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, etc.)
- È vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla società
- È vietato divulgare, cedere o condividere con personale interno o esterno all'azienda le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti
- È vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti
- È vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi
- È vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici aziendali, a meno che non sia esplicitamente previsto nei propri compiti lavorativi
- È vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi
- È vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici aziendali, di clienti 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
- È vietato comunicare a persone non autorizzate, interne o esterne alla società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati

- È proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati
- È vietato lo spamming come pure ogni azione di risposta allo spam
- È obbligatorio segnalare all'organismo di vigilanza qualsiasi situazione in cui si abbia il sospetto che uno dei reati oggetto della presente parte speciale sia stato commesso o possa essere commesso.

IDRAGEST si impegna a porre in essere i seguenti adempimenti:

 Informare adeguatamente i dipendenti e gli altri soggetti eventualmente autorizzati dell'importanza di mantenere i propri codici di accesso (username e password) confidenziali e di non divulgare gli stessi a soggetti terzi (cfr. Manuale utilizzo user id e password)

 Fare sottoscrivere ai dipendenti e agli altri soggetti eventualmente autorizzati uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche aziendali

 Informare i dipendenti e agli altri soggetti eventualmente autorizzati della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di bloccare l'accesso al pc "lock computer", qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso (cfr. Manuale utilizzo user id e password)

 Impostare i sistemi informatici in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente

 Fornire un accesso da e verso l'esterno (connessione alla rete internet) esclusivamente ai sistemi informatici dei dipendenti o di eventuali soggetti terzi che ne abbiano la necessità ai fini lavorativi o connessi all'amministrazione societaria

 Limitare gli accessi alla stanza server unicamente al personale autorizzato

 Proteggere, per quanto possibile, ogni sistema informatico societario 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

Fornire ogni sistema informatico 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 dalla società e non correlati con l'attività espletata per la stessa

 Limitare l'accesso alle aree ed ai siti internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "virus") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti (ad esempio, siti di posta elettronica o siti di diffusione di informazioni e file)

 Impedire l'installazione e l'utilizzo, sui sistemi informatici della società, di software (c.d. "p2p", di files sharing o di istant messaging) mediante i quali è possibile scambiare con altri soggetti

all'interno della rete internet ogni tipologia di file (quali filmati, documenti, canzoni, virus, ecc.) Senza alcuna possibilità di controllo da parte della società

 Qualora per la connessione alla rete internet si utilizzino collegamenti wireless (ossia senza fili, mediante routers dotati di antenna wi-fi), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni all'azienda, possano illecitamente collegarsi alla rete Internet tramite i routers della stessa e compiere illeciti ascrivibili ai dipendenti

 Prevedere un procedimento di autenticazione mediante username e password al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei dipendenti e degli altri soggetti eventualmente autorizzati;

 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 e degli altri soggetti eventualmente autorizzati (i.e. Connessione tramite VPN o RAS)

Effettuare periodicamente, in presenza di accordi sindacali che autorizzino in tale senso e ove possibile, controlli ex ante ed ex post sulle attività effettuate dal personale sulle reti nonché, quando verrà completato il progetto di anomaly detection, rielaborare con regolare cadenza i log dei dati al fine di evidenziare eventuali comportamenti anomali.

13 UTILIZZO DI SISTEMI DI INTELLIGENZA ARTIFICIALE E IA GENERATIVA

IDRAGEST consente l'utilizzo di sistemi di intelligenza artificiale e di IA generativa esclusivamente ai soggetti previamente autorizzati e nei limiti stabiliti dalla policy IA aziendale e dalla procedura speciale del MOG231.

L'autorizzazione deve essere nominativa, coerente con le mansioni svolte e accompagnata da adeguata formazione sui rischi informatici, organizzativi, reputazionali, privacy e 231 connessi all'utilizzo dello strumento.

13.1 PRINCIPI GENERALI

L'uso dei sistemi di IA è consentito solo come strumento di supporto all'attività lavorativa e non può sostituire la valutazione, il controllo e la responsabilità della persona fisica incaricata.

Ogni output generato dall'IA che incida su attività aziendali rilevanti, documentazione tecnica, progettuale, commerciale, contrattuale, amministrativa o comunicazioni verso l'esterno deve essere verificato, validato e, se del caso, corretto da un soggetto umano competente prima del suo utilizzo o invio.

12.2 USI CONSENTITI

L'uso dell'IA può essere consentito, nei limiti autorizzati, per attività preparatorie, organizzative o di supporto, quali: ricerche preliminari, sintesi non definitive, supporto alla redazione di testi interni, supporto allo sviluppo software, organizzazione di informazioni, generazione di bozze non vincolanti, analisi preliminari di dati non riservati o previamente anonimizzati.

12.2 USI VIETATI

È vietato utilizzare strumenti di IA:

- per inserire credenziali, password, chiavi di accesso, token, configurazioni di sicurezza o altre informazioni idonee a compromettere i sistemi informatici aziendali o di terzi;
- per inserire codice sorgente, database, documentazione tecnica, specifiche di progetto, dati di clienti, informazioni di commessa, rilievi, dati infrastrutturali o altri contenuti riservati, salvo espressa autorizzazione e in conformità alla policy IA e alle regole aziendali di sicurezza;
- per trattare dati personali, specie se particolari o giudiziari, in assenza di preventiva verifica di conformità alle regole interne in materia di privacy e sicurezza;
- per generare automaticamente elaborati tecnici, offerte, contratti, pareri, relazioni, comunicazioni esterne o documenti destinati a clienti, fornitori, Pubbliche Amministrazioni o Autorità senza preventiva verifica e validazione umana;
- per assumere o supportare in via esclusiva decisioni che producano effetti rilevanti su lavoratori, clienti, fornitori o terzi;
- in modo difforme dalla policy IA adottata dalla Società.

13.4 OBBLIGHI DELL'UTENTE AUTORIZZATO

L'utente autorizzato all'uso dell'IA deve:

1. utilizzare esclusivamente gli strumenti approvati dalla Società;
2. operare entro il perimetro delle autorizzazioni ricevute;
3. astenersi dall'inserire dati e informazioni non consentiti;
4. verificare l'accuratezza, la coerenza, la liceità e l'affidabilità dell'output generato;
5. mantenere evidenza dell'utilizzo dell'IA nei processi sensibili o nei casi stabiliti dalla policy interna;
6. segnalare tempestivamente al proprio responsabile e all'OdV eventuali anomalie, utilizzi impropri, fughe di dati, output manifestamente errati o criticità di sicurezza.

13.5 TRACCIABILITÀ E CONTROLLI

L'utilizzo dei sistemi di IA autorizzati deve essere assoggettato, ove tecnicamente possibile e in misura proporzionata al rischio, a meccanismi di tracciabilità, registrazione degli accessi, monitoraggio degli utilizzi e verifiche periodiche di conformità alla policy IA, alla presente procedura e alle regole di sicurezza informatica.

13.6 COORDINAMENTO CON LA POLICY IA

La presente procedura si coordina con la policy IA aziendale, che ne costituisce allegato tecnico-operativo per la disciplina di dettaglio dei casi d'uso consentiti, dei livelli autorizzativi, delle misure di sicurezza, dei modelli di supervisione umana e delle istruzioni operative per il personale autorizzato.

14 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutti i Destinatari coinvolti nelle attività di gestione ed utilizzo dei Sistemi Informatici aziendali sono tenuti a comunicare tempestivamente all'Organismo di Vigilanza:

- ✓ qualsiasi violazione ai principi di comportamento;
- ✓ qualsiasi violazione del Modello di Organizzazione e del Codice Etico, con l' indicazione delle ragioni delle difformità e dando atto del processo autorizzativo seguito;
- ✓ report su violazioni da cui si evincono accessi non autorizzati ai sistemi interni o di terzi;
- ✓ Anomalie, criticità riscontrate, etc;
- ✓ Qualsiasi incidente di sicurezza significativo, anche se non ha comportato un data breach, per permettere la valutazione dell'efficacia delle misure in atto;
- ✓ Gli esiti delle verifiche periodiche di vulnerabilità (vulnerability assessment) e dei penetration test;
- ✓ Eventuali criticità rilevate nella sicurezza della catena di approvvigionamento (fornitori IT).

I Destinatari devono, ognuno per le parti di rispettiva competenza, verificare la tracciabilità del processo eseguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposta su apposita piattaforma informatica -tutta la documentazione necessaria.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

Alla luce della complessità dell'esecuzione di tali controlli, l'OdV ha la facoltà di essere coadiuvato da:

• le funzioni aziendali coinvolte nelle verifiche sulle attività sensibili e/o nella gestione dell'infrastruttura informatica (i.e. la funzione Internal Audit, la funzione IT/ICT ovvero l'eventuale outsourcer incaricato);

• eventuali consulenti ad hoc, specializzati nelle investigazioni informatiche e nell'analisi forense informatica.

In particolare, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui all'Art. 24-bis del Decreto, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

In particolare, l'ODV potrà:

 proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei delitti informatici di cui alla presente Parte Speciale, anche in considerazione del progresso e dell'evoluzione delle tecnologie informatiche ed alla luce dei nuovi reati presupposto;

 proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Parte Speciale;

 monitorare il rispetto delle procedure e la documentazione interna per la prevenzione dei Delitti Informatici in costante coordinamento con le funzioni Sicurezza Informatica, Compliance ed Internal Audit;

 consultarsi con il responsabile della Sicurezza Informatica ed invitare periodicamente lo stesso a relazionare alle riunioni dell'OdV;

 esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;

 conservare traccia dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda, quest'ultima adottata ai sensi del D.Lgs. 24/2023 per dare attuazione a quanto previsto dall'art. 6, comma 2-bis, del D.Lgs. 231/2001, garantendo la riservatezza del segnalante e la protezione da ritorsioni.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

Sommario 1

1 OBIETTIVI E FUNZIONI DEL MODELLO 2

1.1 PROCESSO DI GESTIONE OMAGGI, SPESE DI RAPPRESENTANZA E SPONSORIZZAZIONE 2

1.2. PROCESSO DI GESTIONE E SELEZIONE DEI PARTENER COMMERCIALI 3

2 ACRONIMI AZIENDALI 5

3 RIFERIMENTI NORMATIVI 5

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA 6

5 PRINCIPI GENERALI DI COMPORTAMENTO E DESCRIZIONE DEL PROCESSO 6

5.2 PRINCIPI DI CONTROLLO 9

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori: 9

• LIVELLI AUTORIZZATIVI DEFINITI: 9

o per quanto attiene ai beni destinati ad omaggi ed alle spese di rappresentanza, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe e/o apposite autorizzazioni in essere, che stabiliscano le facoltà di autonomia gestionale per natura di spesa e impegno. 9

6 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO 10

La violazione della presente procedura e dei suoi obblighi di comunicazione, integra una violazione del presente Modello di Organizzazione Gestione e Controllo e, pertanto, costituisce un illecito disciplinare passibile di sanzione ai sensi della legge vigente in materia, dello stesso Modello 231, nonché del contratto collettivo nazionale di lavoro applicato. 11

1 OBIETTIVI E FUNZIONI DEL MODELLO

In relazione alla gestione della c.d. omaggistica e delle spese di rappresentanza, sono state analizzate le fattispecie di illeciti presupposto per le quali si applica il Decreto, poiché ai sensi del D. Lgs. 231/2001, poiché i relativi processi, potrebbero costituire una delle modalità strumentali attraverso cui commettere i reati di "Corruzione contro la Pubblica Amministrazione" nelle loro varie tipologie, "Induzione indebita a dare o promettere utilità", e "Traffico di influenze illecite".

Invero, si ritiene che possano essere individuate quali misure di prevenzione efficaci e sufficienti l'osservanza dei principi e delle disposizioni adottate dal Codice Etico, la stretta osservanza delle regole dettate dalle Procedure aziendali applicabili, unitamente ad una rigorosa applicazione da parte di IDRAGEST del sistema disciplinare.

1.1 PROCESSO DI GESTIONE OMAGGI, SPESE DI RAPPRESENTANZA E SPONSORIZZAZIONE

Si precisa che, ai fini del presente protocollo, valgono le seguenti definizioni:

• **PER OMAGGI** si intendono le elargizioni di beni di modico valore offerte, nell'ambito delle ordinarie relazioni di affari, al fine di promuovere l'immagine di IDRAGEST;

• **PER SPESE DI RAPPRESENTANZA** si intendono le spese sostenute da IDRAGEST nell'espletamento delle relazioni commerciali, destinate a promuovere e migliorare l'immagine della Società (ad es. spese per rinfreschi, per forme di accoglienza ed ospitalità, ecc.);

• **PER INIZIATIVE DI BENEFICENZA** si intendono le elargizioni in denaro che IDRAGEST destina esclusivamente ad Enti senza fini di lucro;

• **PER SPONSORIZZAZIONI** si intendono la promozione, la valorizzazione ed il potenziamento dell'immagine della IDRAGEST attraverso la stipula di contratti atipici (in forma libera, di natura patrimoniale, a prestazioni corrispettive) con Enti esterni (ad es.: Enti senza fini di lucro, Enti territoriali ed organismi locali, ecc.).

Una gestione non trasparente dei processi relativi a omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni potrebbe, infatti, consentire la commissione di tali reati, ad esempio attraverso il riconoscimento/concessione di vantaggi ad esponenti della Pubblica Amministrazione e/o ad esponenti apicali, e/o a persone loro subordinate, di società o enti controparti o in relazione con la Società, al fine di favorire interessi di IDRAGEST, ovvero la creazione di disponibilità utilizzabili per la realizzazione dei reati in questione.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte di IDRAGEST, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

1.2. PROCESSO DI GESTIONE E SELEZIONE DEI PARTENER COMMERCIALI

Il presente protocollo definisce, altresì, i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento che tutte le Funzioni Aziendali coinvolte devono adottare nell'ambito del processo di gestione e di selezione dei fornitori di beni, servizi ed incarichi professionali.

Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Modello e nel Codice Etico.

Tutti coloro che, in ragione del proprio incarico o della propria funzione, sono coinvolti nella gestione del processo relativo alla scelta dei partner commerciali devono:

- garantire la completa tracciabilità dell'*iter* decisionale, autorizzativo e delle attività di controllo svolte;

- garantire che la scelta dei fornitori di beni e sevizi o e dei consulenti sia aderente rispetto alle reali esigenze aziendali, evitando la configurazione di ogni possibile situazione di conflitto di interessi;
- informare i fornitori di beni e servizi, le società committenti/appaltatrici ed i professionisti esterni, che IDRAGEST S.r.l. ha adottato il Modello di Organizzazione Gestione e Controllo previsto dal D.Lgs 231/2001 ed un Codice Etico, e richiedere l'impegno a rispettare le leggi e i regolamenti applicabili in Italia, nonché, ove ritenuto necessario, il rispetto dei principi di comportamento e di controllo previsti dal predetto Modello e dal Codice Etico, compresa tutta la vigente normativa antiriciclaggio, il rispetto delle norme contributive, fiscali, previdenziali ed assicurative in favore dei propri dipendenti e collaboratori, degli obblighi di tracciabilità finanziaria, nonché l'assenza di provvedimenti a carico dei fornitori, dei professionisti e degli enti e/o dei suoi apicali, per i reati di cui al D.Lgs n. 231/2001;
- privilegiare, ove possibile, i fornitori dotati rispettivamente di un Sistema per la Gestione della Qualità, di un Sistema di Gestione Ambientale, di un Sistema di Gestione della Salute e Sicurezza certificato, nonché fornitori che si siano conformati al rispetto delle regole di prevenzione dei reati di cui al D.Lgs. 231/2001 e degli standard sociali minimi;
- scegliere i partner commerciali solo dopo aver svolto idonee verifiche sulla reputazione e sulla affidabilità sul mercato degli stessi.

I CRITERI DA ADOTTARE PER LA SCELTA DEI PARTENER COMMERCIALI SONO I SEGUENTI:

- conformità dei prodotti/servizi alle disposizioni di legge;
- rapporto qualità/prezzo materiale/prestazione puntualità e precisione nelle consegne merce/fine lavori;
- servizio di assistenza;
- qualità forniture/prestazioni pregresse;
- risposta urgenze/emergenze;
- gestione dei rischi ambientali;
- rispetto delle norme di salute e sicurezza;
- rispetto degli standard sociali minimi.

E' compito di IDRAGEST accertarsi che vengano definiti i criteri per monitorare:

- la qualità del prodotto/servizio (es. rapporto qualità/prezzo, capacità di risposta a richieste urgenti e rispetto tempi di consegna/erogazione, ecc.);

- l'impatto sull'ambiente (es. verifica corretta gestione rifiuti, di eventuali sostanze pericolose e trasporto di materiali effettuato nel rispetto della normativa vigente, ecc.);
- i rischi per la salute e sicurezza (es. disponibilità di schede di sicurezza aggiornate per i prodotti e di libretti uso e manutenzione per le attrezzature; formazione del personale per l'utilizzo corretto di tutta l'attrezzatura aziendale; corretta applicazione di tutte le disposizioni relative alla sicurezza in cantiere inerenti il POS e l'utilizzo DPI; e, per i subappaltatori, rispetto e mantenimento dei requisiti tecnico – professionali per l'esecuzione dei lavori).

È fatto divieto avviare o proseguire rapporti, diretti o indiretti, con soggetti di cui sia anche solamente sospettata l'appartenenza o la contiguità ad ambienti malavitosi o che, comunque, siano sospettati di agevolare in qualsiasi forma, anche occasionalmente, la criminalità organizzata.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC	Responsabile Tecnico
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RFAM	Responsabile Facility Management
RPROG	Responsabile Progettazione
RGAD	Responsabile Gestione Archivi e Documenti
REC	Responsabile Esterno Contabilità

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di IDRAGEST S.r.l.;

- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l.

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

Il presente protocollo, le disposizioni del Codice Etico e del Modello, dovranno essere osservati da tutte le Funzioni Aziendali che si occupano del processo di scelta e gestione dei partner commerciali, sia essi fornitori di prodotti - come attrezzature elettroniche, prodotti di cancelleria, *software*, *etc.* -, sia essi fornitori di servizi – come società e/o professionisti che svolgono attività di consulenza, studi di commercialisti/avvocati, *etc.* –, nonché a tutti coloro che, a diverso titolo, sono coinvolti nella gestione di omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni.

Il processo di acquisto è gestito dal RCOM/APVG e dal PRES, a seconda della tipologia di fornitura.

5 PRINCIPI GENERALI DI COMPORTAMENTO E DESCRIZIONE DEL PROCESSO

In ordine alla scelta dei *partner* commerciale, il processo di selezione verrà eseguito dal RCOM/APVG e PRES, i quali dovranno assicurare, ognuno per le parti di rispettiva competenza, l'esecuzione dei seguenti controlli:

- Garantire, per importi superiori ad euro 5.000,00, che la selezione del fornitore sia sempre effettuata sulla base della valutazione del miglior rapporto tra qualità e convenienza del servizio / prodotto offerto / *business*, prediligendo i fornitori inseriti nell'elenco *"Elenco dei Fornitori Qualificati"* (fornitori con i quali esiste un rapporto di lunga data – ovvero, di almeno due anni – e che hanno assicurato la conformità dei loro prodotti);
- nell'ipotesi in cui il prodotto/servizio richiesto non sia reperibile presso i fornitori, il RCOM/APVG che, in relazione alla propria area di riferimento, debba selezionare un fornitore – anche ai fini dell'inserimento nel sopra citato "*elenco"* – deve sottoporre la scelta al PRES che siglerà il preventivo, solo per importi superiori ad euro 5.000,00;
- nei contratti che prevedono la gestione in *outsourcing* di attività aziendali presso la sede della società, il fornitore dovrà garantire che, in caso di impiego di personale proveniente da paesi terzi, questo dovrà essere in possesso di regolare permesso di soggiorno.

I contratti con i partner commerciali dovranno essere sottoscritti dal PRES, il quale dovrà previamente, verificare l'espressa previsione al rispetto delle leggi e dei i regolamenti in materia, nonché del rispetto a quanto previsto dal D.lgs. 231/2001.

Mentre, i processi di gestione degli omaggi e delle spese di rappresentanza hanno ad oggetto i beni destinati ad essere offerti, in qualità di cortesia commerciale, a soggetti terzi, quali, ad esempio, clienti, fornitori, Enti della Pubblica Amministrazione, istituzioni pubbliche o altre organizzazioni.
Si considerano atti di cortesia commerciale e/o istituzionale di modico valore gli omaggi provenienti o destinati al medesimo soggetto/ente, che non superino, in un anno solare, il valore di 150 euro.

I PROCESSI DI GESTIONE DELLE SPESE PER BENEFICENZE E PER SPONSORIZZAZIONI SI ARTICOLANO NELLE SEGUENTI FASI:

- ricezione della richiesta, inviata dagli Enti, di elargizioni e di beneficenze o sponsorizzazioni per progetti, iniziative, manifestazioni;
- individuazione di società/organizzazioni cui destinare le elargizioni;
- effettuazione delle attività di due diligence di IDRAGEST;
- esame/valutazione dell'iniziativa/progetto proposto;
- autorizzazione alla spesa e, qualora previsto, stipula dell'accordo/ contratto;
- erogazione delle elargizioni da parte di IDRAGEST.

Le spese per omaggi sono consentite purché di modico valore e, comunque, tali da non compromettere l'integrità e la reputazione di una delle parti e da non influenzare l'autonomia di giudizio del beneficiario, le Funzioni Aziendali, a qualsiasi titolo coinvolte nella gestione di omaggi, delle spese di rappresentanza, delle beneficenze e delle sponsorizzazioni sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna, nonché le eventuali previsioni del Codice Etico e del Codice Disciplinare di IDRAGEST, nonché dalle disposizioni in materia di anticorruzione.

IN PARTICOLARE:

- IDRAGEST può effettuare erogazioni sotto forma di beneficenze o sponsorizzazioni per sostenere iniziative di enti regolarmente costituiti ai sensi di legge e che non contrastino con i principi etici della Società e nel caso di beneficenze, tali enti non devono avere finalità di lucro;
- eventuali iniziative la cui classificazione rientri nei casi previsti per le "sponsorizzazioni" non possono essere oggetto contemporaneo di erogazione per beneficenza;
- le erogazioni devono essere riconosciute esclusivamente su un conto corrente intestato all'ente beneficiario; non è consentito effettuare pagamenti in contanti, in un Paese diverso da quello dell'ente beneficiario o a un soggetto diverso dallo stesso.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

• effettuare erogazioni, per iniziative di beneficenza o di sponsorizzazione, a favore di enti coinvolti vicende giudiziarie note, pratiche non rispettose dei diritti umani, o contrarie alle norme in tema di vivisezione e di tutela dell'ambiente. Non possono essere destinatari di erogazioni partiti e movimenti politici e le loro articolazioni organizzative, organizzazioni sindacali e di patronato, club (ad esempio Lions, Rotary, ecc.), associazioni e gruppi ricreativi, scuole private, parificate e/o legalmente riconosciute, salvo specifiche iniziative connotate da particolare rilievo sociale, culturale o scientifico che devono essere approvate dal PRES;

• effettuare elargizioni/omaggi a favore di enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persone ad essa collegate contravvenendo a quanto previsto nel presente protocollo;

• promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura a esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero altre organizzazioni con la finalità di promuovere o favorire interessi di IDRAGEST, anche a seguito di illecite pressioni. Il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla al proprio Responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta al PRES per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;

• promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparte o in relazione con IDRAGEST, al fine di favorire indebitamente gli interessi della Società;

• dare in omaggio beni per i quali non sia stata accertata la legittima provenienza ed il rispetto delle disposizioni che tutelano le opere dell'ingegno, i marchi e i diritti di proprietà industriale in genere, nonché le indicazioni geografiche e le denominazioni di origine protette.

Le Funzioni Aziendali interessate sono tenute a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

5.2 PRINCIPI DI CONTROLLO

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

• LIVELLI AUTORIZZATIVI DEFINITI:

o per quanto attiene ai beni destinati ad omaggi ed alle spese di rappresentanza, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe e/o apposite autorizzazioni in essere, che stabiliscano le facoltà di autonomia gestionale per natura di spesa e impegno.

o gli omaggi o le altre utilità di valore superiore a 150 euro possono essere ammissibili in via eccezionale, in considerazione del profilo del donante o del beneficiario, e comunque nei limiti della ragionevolezza, previa autorizzazione scritta del PRES.

• ATTIVITÀ DI CONTROLLO:

O IN PARTICOLARE È PREVISTA:

- l'analisi e la verifica del tipo di organizzazione e della finalità per la quale è costituita;
- la verifica ed approvazione di tutte le erogazioni da parte del PRES;
- la verifica che le erogazioni complessive siano stabilite annualmente e trovino capienza in apposito budget deliberato dagli Organi competenti;

o per le sponsorizzazioni è necessaria una puntuale verifica del corretto adempimento della controprestazione acquisendo idonea documentazione comprovante l'avvenuta esecuzione della stessa.

o disporre che venga regolarmente tenuto in evidenza l'elenco dei beneficiari, l'importo delle erogazioni ovvero gli omaggi distribuiti nonché le relative date/occasioni di elargizioni e tale elenco verrà condiviso nell'apposita piattaforma digitale all'uopo preposta come TEAMS (o simili).

• TRACCIABILITÀ DEL PROCESSO SIA A LIVELLO DI SISTEMA INFORMATIVO SIA IN TERMINI DOCUMENTALI:

o tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni anche attraverso la redazione di una reportistica sulle erogazioni effettuate e/o sui contratti stipulati;

o al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, le Funzioni Aziendali interessate sono responsabili dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione degli omaggi, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni e, pertanto, dovranno provvedere a caricare tutta la documentazione nell'apposita piattaforma digitale all'uopo preposta come TEAMS (o simili).

6 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutti i *Destinatari* coinvolti nella selezione e gestione dei fornitori di beni, servizi e incarichi professionali informano tempestivamente l'Organismo di Vigilanza di;

- ✓ situazioni anomale e/o poste in essere in deroga alla presente procedura;
- ✓ comportamenti posti in essere in violazione a quanto previsto nel Modello e nel Codice Etico.

Nell'ipotesi in cui si dubiti della moralità dei *partner* commerciali, la funzione aziendale che ha chiesto la fornitura/consulenza dovrà informare tempestivamente l'Organismo di Vigilanza, nonché comunicare l'eventuale insorgenza di criticità nei rapporti con il *partner*.

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, tenendo a disposizione dell'Organismo di Vigilanza – in un archivio ordinato – tutta la documentazione all'uopo necessaria.

Si precisa che, deve, essere annualmente trasmesso all'Organismo di Vigilanza l'elenco degli omaggi erogati a soggetti appartenenti alla Pubblica Amministrazione e/o a soggetti privati.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse ai Processi Sensibili al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute; infatti, è obbligo per chiunque segnalare, tempestivamente, all'OdV anomalie e/o violazione della presente procedura, del Modello e del Codice Etico relativi ai processi di gestione riguardanti le scelte dei partner commerciali, nonché quelli riguardanti l'elargizione degli omaggi, delle spese di rappresentanza, delle beneficenze e delle sponsorizzazioni.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

La violazione della presente procedura e dei suoi obblighi di comunicazione, integra una violazione del presente Modello di Organizzazione Gestione e Controllo e, pertanto, costituisce un illecito disciplinare passibile di sanzione ai sensi della legge vigente in materia, dello stesso Modello 231, nonché del contratto collettivo nazionale di lavoro applicato.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 1.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI E FUNZIONE DEL MODELLO 3

2 ACRONIMI AZIENDALI 5

3 RIFERIMENTI NORMATIVI 5

4 CAMPO DI APPLICAZIONE E RESPONSABILE DEL MODELLO 6

5 AREA SENSIBILE CONCERNENTE I REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO 7

5.1 OMICIDIO COLPOSO (ART. 589 C.P.) - LESIONI PERSONALI COLPOSE GRAVI O GRAVISSIME (ART. 590 COMMA 3 C.P.) 7

6 GESTIONE DEI RISCHI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO 9

7. SALUTE E SICUREZZA SUI LUOGHI DI LAVORO – GESTIONE EMERGENZA COVID 19**Errore. Il segnalibro non è definito.**

8 RISPETTO DEGLI STANDARD TECNICO STRUTTURALI DI LEGGE 13

9 L'ACQUISTO, UTILIZZO E MANUTENZIONE DELLE ATTREZZATURE 14

10 GESTIONE EMERGENZE E PRIMO SOCCORSO 15

11 COMUNICAZIONE E RAPPORTO CON L'ESTERNO 17

12 CONSULTAZIONE E PARTECIPAZIONE 17

13 ATTIVITÀ DI INFORMAZIONE E FORMAZIONE DEI LAVORATORI 17

14 LO STANZIAMENTO DI FONDI PER LA GESTIONE DEL SSL 19

15 RIESAME E VERIFICA ATTUAZIONE ED EFFICACIA DEL MODELLO 19

16 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO 20

1 OBIETTIVI E FUNZIONE DEL MODELLO

Il presente protocollo, uniformemente e ad integrazione del sistema di sicurezza sul lavoro adottato da IDRAGEST S.r.l., individua una serie di procedure, in conformità all'art. 30 D.lgs 81/2008 come modificato dalla Legge 11 marzo 2026, n. 34 e decreto del 13 febbraio 2014 emanato dal Ministero del Lavoro e Politiche Sociali, atte a verificare e controllare la corretta applicazione degli adempimenti previsti dalla vigente legislazione nazionale in materia di tutela della salute e della sicurezza negli ambienti di lavoro.

Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Modello e nel Codice Etico di IDRAGEST.

Il presente protocollo ha lo scopo di fornire all'OdV e alle Funzioni Aziendali che con lo stesso cooperano, gli strumenti per esercitare le attività di controllo, monitoraggio e verifica previste in materia di tutela della salute e della sicurezza negli ambienti di lavoro.

Pertanto, le Funzioni Aziendali che, per ragione del proprio incarico o della propria Funzione, siano coinvolti nella gestione del processo in oggetto devono:

- operare nel rispetto delle leggi e della normativa vigente in materia di salute e sicurezza sul lavoro, nei limiti dei poteri assegnati;
- attenersi alle regole di condotta conformemente a quanto prescritto dal presente documento, dal Modello e dal Codice Etico, al fine di prevenire ed impedire il verificarsi dei reati e degli illeciti amministrativi commessi per la violazione delle norme antinfortunistiche e sulla tutela della salute e della sicurezza negli ambienti di lavoro;
- comunicare, tempestivamente ed in via formale ai soggetti operanti nel Servizio di Protezione e Prevenzione, eventuali situazioni di potenziale rischio/pericolo (ad esempio "quasi infortuni") ed infortuni (indipendentemente dalla loro gravità);
- garantire la completa tracciabilità dell'*iter* decisionale, autorizzativo e delle attività di controllo svolte.

In particolare, il Datore di Lavoro, i delegati *ex* art. 16 D. Lgs. 81/2008 (ove presenti) nonché tutti i soggetti aventi compiti e responsabilità nella gestione degli adempimenti previsti delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, quali, a titolo esemplificativo, Responsabile del Servizio di Prevenzione e Protezione (RSPP), Preposti, Medico Competente - così

come individuati dalla Società coerentemente alle previsioni della vigente legislazione (cfr. Organigramma sulla sicurezza di IDRAGEST) - devono garantire, ognuno nell'ambito di propria competenza:

- l'applicazione degli obiettivi per la sicurezza e la salute dei lavoratori, l'identificazione continua dei rischi nonché la predisposizione delle misure di prevenzione e protezione conseguenti;
- il rispetto degli *standard* tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici, anche attraverso un processo continuo di aggiornamento sullo stato dell'arte degli *standard* e la manutenzione ordinaria e straordinaria degli impianti, delle attrezzature di lavoro e, in generale, delle strutture aziendali;
- un adeguato livello di informazione/formazione dei lavoratori, così come definiti dal D.lgs. 81/2008 ss.mm.ii., sulla gestione delle attività in materia di sicurezza e salute della Società e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla Società. In particolare, ciascun lavoratore dovrà ricevere formazione sufficiente ed adeguata con particolare riferimento al proprio posto di lavoro ed alle proprie mansioni. Tale formazione deve essere erogata nel rispetto del nuovo Accordo Stato-Regioni del 17 aprile 2025 [59], che aggiorna i contenuti, le metodologie e la durata dei corsi per datori di lavoro, dirigenti, preposti e lavoratori. La suddetta formazione deve essere fatta in occasione dell'assunzione, del trasferimento o cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro o di nuove tecnologie, di nuove sostanze e preparati pericolosi;
- la definizione e l'aggiornamento (in base ai cambiamenti nella struttura organizzativa ed operativa dalla Società nonché l'evolversi del panorama normativo) di procedure specifiche per la prevenzione di infortuni e malattie, in cui siano, tra l'altro, disciplinate le modalità di gestione degli incidenti e delle emergenze;
- l'idoneità delle risorse umane – in termini di numero e qualifiche professionali, formazione – e materiali, necessarie al raggiungimento degli obiettivi prefissati dalla Società per la sicurezza e la salute dei lavoratori.

I lavoratori devono comunicare tempestivamente, alle funzioni individuate e con le modalità definite nelle procedure operative, situazioni di pericolo, quasi infortuni, infortuni (indipendentemente dalla loro gravità) e violazioni alle regole di comportamento e alle procedure operative.

È FATTO ESPLICITO DIVIETO DI:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 septies del D.lgs. 231/2001);
- porre in essere o dare causa a violazioni dei principi di comportamento, dei protocolli e delle procedure aziendali;
- fruire di servizi in "appalto" con consulenti, *partner* ed in generale fornitori, in assenza dei requisiti di idoneità tecnico-professionale.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione (di seguito anche DL)
DL	Datore di Lavoro
PRES	Presidente CDA
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC	Responsabile Tecnico
MC	Medico Competente
RAM	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RFAM	Responsabile Facility Management
RPROG	Responsabile Progettazione
RATTR	Responsabile Attrezzature
RLS	Rappresentante Lavoratori per la Sicurezza

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Codice Etico di IDRAGEST S.r.l.;
- Decreto Legislativo 8 giugno 2001, n. 231 e s.s.mm.ii.;

- Decreto Legislativo 9 aprile 2008, n. 81 (Testo Unico in materia di salute e sicurezza sul lavoro), come modificato dalla Legge 11 marzo 2026, n. 34, con particolare riferimento agli artt. 17, 26, 28, 30, 37, 66, 121 e Titolo IV;
- Regio Decreto 16 marzo 1942, n. 262 (Codice Civile), con specifico riferimento all'art. 2086 (Assetti organizzativi adeguati) e all'art. 2087 (Tutela delle condizioni di lavoro);
- Accordo Stato-Regioni del 17 aprile 2025 (ai sensi dell'art. 37, comma 2, D.Lgs. 81/2008), in materia di formazione dei datori di lavoro, dirigenti, preposti e lavoratori in materia di salute e sicurezza [59];
- Decreto Legislativo 10 marzo 2023, n. 24 (Decreto Whistleblowing);
- Norma tecnica UNI EN ISO 45001:2023+A1:2024 (Sistema di Gestione della Salute e Sicurezza sul Lavoro) [60];
- Direttiva 2012/18/UE (Seveso III) e D.Lgs. 105/2015, per quanto applicabile alle attività di campo su infrastrutture idriche e reti di fluidi.

4 CAMPO DI APPLICAZIONE E RESPONSABILE DEL MODELLO

Il presente protocollo si applica a tutte le Funzioni Aziendali che operano per IDRAGEST, a tutti coloro che, esterni alla Società, intrattengano rapporti contrattuali con la stessa, nonché a tutti i terzi che accedono, a qualsiasi titolo, nei luoghi di lavoro in cui la Società svolge la propria attività.
Il presente protocollo si applica, in particolare, alle seguenti tipologie di attività svolte da IDRAGEST che presentano specifici profili di rischio:

1. attività di rilievo topografico su reti idriche e fognarie con accesso a camerette, pozzetti, cunicoli e spazi confinati (artt. 66 e 121 D.Lgs. 81/2008);
2. attività di campo in prossimità del traffico stradale (segnaletica, recinzione cantieri, DPI specifici);
3. attività in cantieri temporanei e mobili (Titolo IV D.Lgs. 81/2008);
4. attività in outsourcing presso clienti, con conseguente operatività in ambienti non direttamente controllati da IDRAGEST.

La gestione degli adempimenti in materia di salute e sicurezza sui luoghi di lavoro e dei relativi obblighi coinvolge ciascuno dei destinatari, ognuno nell'ambito delle proprie competenze ed attribuzioni, così come previsto all'interno del DVR e sulla base dell'Organigramma sicurezza; le corrispondenti funzioni individuate in IDRAGEST S.r.l. sono le seguenti:

1. Datore di Lavoro;

2. Responsabile del Servizio di Prevenzione e Protezione;
3. Medico Competente;
4. Rappresentante Lavoratori per la Sicurezza;
5. Preposti;
6. Lavoratori;
7. Addetti al servizio antincendio ed al servizio di primo soccorso.

I responsabili del sistema sicurezza sopra indicati devono essere valutati in base alle competenze, al titolo di studio e alle precedenti esperienze lavorative. Le verifiche devono essere effettuate attraverso l'acquisizione dei *curricula*.

5 AREA SENSIBILE CONCERNENTE I REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO

L'art. 25 septies del Decreto prevede tra gli illeciti presupposto della responsabilità degli Enti i delitti di omicidio colposo e di lesioni colpose gravi o gravissime, se commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Il Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro, (D. Lgs. 9 aprile 2008 n. 81) che ha profondamente riordinato le molteplici fonti normative previgenti in materia, ha previsto all'art. 30 le caratteristiche che deve presentare il Modello di organizzazione, gestione e controllo al fine della prevenzione dei reati in esame.

Finalità delle citate disposizioni è quella di fornire più efficaci mezzi di prevenzione e repressione in relazione alla recrudescenza del fenomeno degli incidenti sul lavoro ed alla esigenza di tutela dell'integrità psicofisica dei lavoratori e della sicurezza degli ambienti lavorativi.

5.1 OMICIDIO COLPOSO (ART. 589 C.P.) - LESIONI PERSONALI COLPOSE GRAVI O GRAVISSIME (ART. 590 COMMA 3 C.P.)

Le condotte punite dalle due fattispecie consistono nel cagionare per colpa, rispettivamente, la morte oppure una lesione dalla quale deriva una malattia, nel corpo o nella mente, grave o gravissima.

Per lesioni gravi si intendono quelle che causano una malattia che metta in pericolo la vita o provochi una incapacità di attendere alle ordinarie occupazioni per un periodo superiore ai quaranta giorni, oppure in un indebolimento permanente di un senso o di un organo; per lesioni gravissime si intendono la malattia probabilmente insanabile, la perdita di un senso, di un arto, di un organo o della

capacità di procreare, la difficoltà permanente nella favella, la deformazione o lo sfregio permanente del viso.

Ai sensi del predetto art. 25 septies del Decreto, entrambe le condotte devono essere caratterizzate dalla violazione delle norme dettate ai fini della prevenzione degli infortuni sul lavoro e sulla tutela dell'igiene e della salute sul lavoro.

La giurisprudenza più recente (Cass. Sez. L, N. 11918 del 6 maggio 2025) ha confermato che, in caso di compresenza organizzata di più lavoratori appartenenti ad imprese diverse, devono essere previsti obblighi di cooperazione, coordinamento e informazione in ordine alle misure da adottare per la sicurezza, l'igiene e la salute di tutti i lavoratori interessati, in attuazione dell'art. 26 D.Lgs. 81/2008. Ciò è di particolare rilievo per IDRAGEST che opera frequentemente in outsourcing presso i clienti o in coordinamento con imprese terze.

Vengono a tal proposito in considerazione molteplici disposizioni, ora in gran parte confluite nel Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro a seguito dell'abrogazione da parte del medesimo Testo Unico di varie leggi speciali previgenti, tra le quali, fondamentalmente: il D.P.R. 27.4.1955 n. 547 in tema di prevenzione degli infortuni; il D.P.R. 19.3.1956 n. 303 che disciplinava l'igiene del lavoro; il D. Lgs. 19.9.1994 n. 626 che conteneva norme generali sulla tutela della salute e della sicurezza dei lavoratori; il D. Lgs. 14.8.1996 n. 494 in tema di sicurezza dei cantieri.

A completamento del corpo normativo delineato dalle specifiche misure di prevenzione prescritte dalle leggi in materia si colloca la più generale previsione di cui all'art. 2087 del codice civile, in forza della quale il datore di lavoro deve adottare le misure che secondo la particolarità del lavoro, l'esperienza e la tecnica sono necessarie per tutelare l'integrità fisica e morale dei lavoratori.

In conformità con la giurisprudenza di merito (Tribunale di Castrovillari, Sentenza n. 1330 del 20 luglio 2025), il datore di lavoro è tenuto ad effettuare la valutazione dei rischi tenendo conto anche dei fattori di rischio interni ed esterni, e la relativa documentazione deve rispettare rigorosamente i requisiti di forma e contenuto prescritti dagli artt. 17 e 28 del D.Lgs. 81/2008. Laddove si contesti la responsabilità del datore di lavoro, l'onere della prova del nesso causale tra condotta omissiva ed evento dannoso è a carico del danneggiato; tuttavia, la Società è tenuta a garantire la completezza e l'aggiornamento della documentazione probatoria a propria discolpa.

Va infine tenuto presente che la giurisprudenza ritiene che i reati in questione siano imputabili al datore di lavoro anche qualora la persona offesa non sia un lavoratore, ma un estraneo, purché la sua presenza sul luogo di lavoro al momento dell'infortunio non abbia caratteri di anormalità ed eccezionalità.

6 GESTIONE DEI RISCHI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO

La gestione dei rischi in materia di salute e sicurezza sul lavoro riguarda qualunque tipologia di attività finalizzata a sviluppare ed assicurare un sistema di prevenzione e protezione dei rischi esistenti sul luogo di lavoro, in ottemperanza a quanto previsto dal D. Lgs. 81/2008 (di seguito Testo Unico).

Si rammenta anzitutto che, ai sensi del Testo Unico compete al Datore di lavoro la responsabilità per la definizione della politica aziendale riguardante la salute e la sicurezza dei lavoratori sul luogo di lavoro e compete al Committente e/o ai suoi delegati la responsabilità e la gestione dei cantieri temporanei o mobili disciplinati dal Titolo IV del Testo Unico nonché compete ad entrambi, per gli ambiti di rispettiva pertinenza, il rispetto degli obblighi relativi all'affidamento di contratti d'appalto, d'opera o di somministrazione previsti dall'art. 26 del medesimo Testo Unico.

In ottemperanza a quanto disposto dalla predetta normativa, IDRAGEST adotta e tiene aggiornato il "Documento di Valutazione dei Rischi" (DVR), che rappresenta l'evidenza documentale di un processo permanente di prevenzione dei rischi per la salute e la sicurezza dei lavoratori.

Il DVR è un documento elaborato dal Datore di Lavoro, in collaborazione con il Responsabile del Servizio di Prevenzione e Protezione e con il Medico Competente nei casi in cui sia obbligatoria la sorveglianza sanitaria, previa consultazione del Rappresentante dei Lavoratori per la Sicurezza.

"DOCUMENTO DI VALUTAZIONE DEI RISCHI" CONTIENE:

• la valutazione dei rischi per la sicurezza e la salute durante l'attività lavorativa;

• l'individuazione delle misure di prevenzione e protezione poste a tutela dei lavoratori ed il programma delle misure ritenute opportune per garantire il miglioramento nel tempo del livello di sicurezza;

• l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;

• l'indicazione del nominativo del Responsabile del Servizio di Prevenzione e Protezione, dei Rappresentanti dei Lavoratori per la Sicurezza e dei Medici Competenti che hanno partecipato alla valutazione del rischio;

• l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento;

• l'individuazione delle misure di prevenzione, di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione dei rischi connessi all'esercizio dell'attività lavorativa esercitata. Sul punto, il RSPP e i Preposti compilano scheda di consegna/gestione dei dispositivi di protezione individuali, necessari per la lavorazione e ne verificano il loro stato d'uso nonché l'eventuale scadenza;

Tale Documento è redatto in conformità alla normativa nazionale ed alle linee guida nazionali ed Europee (ISPESL, INAIL, UNI-EN-ISO, Agenzia Europea per la Salute e Sicurezza). In particolare, sono recepite le "Linee Guida per un Sistema di Gestione della Salute e Sicurezza sul Lavoro (SGSL)" UNI - INAIL del settembre 2001. A tal fine il Documento di Valutazione dei Rischi individua, all'interno dell'organizzazione aziendale, le responsabilità, le procedure, i processi e le risorse per la realizzazione della propria politica di prevenzione nel rispetto delle norme di salute e sicurezza vigenti. Nel medesimo Documento vengono descritte le modalità con le quali l'organizzazione risponde ai requisiti delle predette Linee Guida e sono esplicitati i processi operativi ed i documenti societari atti a garantire l'adempimento di quanto previsto dall'art. 30 - Modelli di organizzazione e di gestione - del Testo Unico.

Ancora, il DVR di IDRAGEST, **in relazione all'attività di campo** ha lo scopo preciso di definire le modalità operative adottate dalla Società per valutare e gestire i rischi per la salute e la sicurezza degli addetti ai lavori al fine di eliminare o ridurre i danni correlati alle attività di rilevo e/o misurazione portata/pressione delle reti idriche eseguito da personale specializzato impegnato nelle attività di campo.

La valutazione dei rischi consiste in un esame sistematico di tutti gli aspetti dell'attività lavorativa, volto a stabilire cosa può provocare lesioni o danni, se è possibile eliminare i pericoli e, nel caso in cui ciò non sia possibile, quali misure di prevenzione o di protezione sono o devono essere messe in atto per controllare i rischi.

L'adozione e l'applicazione di procedure operative di sicurezza aiutano a mitigare gli eventuali rischi residui in tutte quelle attività di lavoro per le quali, pur attuando tutte le disposizioni di sicurezza previste dalla normativa, restano in atto dei rischi direttamente correlati al tipo di attrezzatura utilizzata, all'ambiente di lavoro, ai prodotti impiegati e alle interferenze.

La politica aziendale in tema di salute e sicurezza sul lavoro deve essere diffusa, compresa, applicata ed aggiornata a tutti i livelli organizzativi, a tal fine vengono predisposti piani formativi adeguati e rispondenti alla normativa in materia, che tengano in considerazione il ruolo aziendale ricoperto, l'esposizione a specifici rischi e l'assegnazione di particolari incarichi per la gestione delle situazioni di

emergenza. Le linee d'azione generali di IDRAGEST devono essere orientate a un costante miglioramento della qualità della sicurezza e devono contribuire allo sviluppo effettivo di un "sistema di prevenzione e protezione". Tutte le Funzioni Aziendali devono osservare le disposizioni in materia di salute, di sicurezza e di igiene del lavoro e tenerne conto in occasione di qualsivoglia modifica degli assetti esistenti, compresi ristrutturazioni/allestimenti di siti operativi.

La valutazione dei rischi è aggiornata, utilizzando le informazioni ottenute dall'attività di monitoraggio e, comunque, ogni volta che intervengono cambiamenti significativi del processo produttivo o di organizzazione del lavoro, cambiamenti legislativi, evoluzione della tecnica o a seguito di eventi, quali emergenze, infortuni.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte di IDRAGEST, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

DESCRIZIONE DEL PROCESSO

Il processo di gestione dei rischi in materia di salute e sicurezza sul lavoro prevede le seguenti fasi:

• identificazione dei pericoli e loro classificazione (pericoli per la sicurezza e pericoli per la salute dei lavoratori);

• valutazione dei rischi;

• individuazione e predisposizione delle misure di prevenzione e di protezione;

• definizione di un piano di intervento con l'identificazione delle strutture aziendali competenti all'attuazione di detti interventi;

• realizzazione degli interventi pianificati nell'ambito di un programma;

• verifica dell'attuazione e controllo sull'efficacia delle misure adottate.

La valutazione dei rischi esamina in maniera sistematica tutti gli aspetti dei luoghi di lavoro, per definire le possibili od eventuali cause di lesioni o danni.

LA VALUTAZIONE DEI RISCHI

La valutazione dei rischi è uno strumento finalizzato alla programmazione delle misure di protezione e prevenzione, quindi, alla più generale organizzazione della prevenzione aziendale volta a salvaguardare la salute e la sicurezza dei lavoratori.

Il D. Lgs. 9 Aprile 2008, n. 81 e s.m.i. ribadisce l'obbligo della valutazione di tutti i rischi per la sicurezza e la salute dei lavoratori, con la conseguente elaborazione del documento previsto dall'art. 28.

La valutazione riguarderà anche la scelta delle attrezzature di lavoro e delle sostanze e dei preparati chimici impiegati, la sistemazione dei luoghi di lavoro, i rischi dei gruppi di lavoro esposti a rischi particolari (stress lavoro-correlato, lavoratrici in stato di gravidanza, minori, ect.), nonché quelli connessi alle differenze di genere, di età, di provenienza.

Ai sensi dell'art. 28, infatti, il documento redatto a conclusione della valutazione deve avere data certa e contenere:

a) Una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;

b) l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati, a seguito della valutazione di cui all'articolo 17, comma 1, lettera a);

c) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;

d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;

e) l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio;

f) l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Il documento sarà utilizzato come guida da tutti i soggetti facenti parte del sistema organizzativo della sicurezza, al fine di applicare tutte le misure da adottare in relazione ai rischi presenti.

Tutti saranno soggetti alla piena osservanza e applicazione delle misure di sicurezza riportate nel presente documento.

Le misure, i DPI e le cautele di sicurezza sono:

o TASSATIVAMENTE OBBLIGATORIE;

o DA IMPIEGARE CORRETTAMENTE E CONTINUAMENTE;

o DA OSSERVARE PERSONALMENTE.

CERTIFICAZIONI DI SISTEMA ISO

IDRAGEST ha adottato, altresì, strumenti professionali che comprovano la conformità dei propri sistemi di gestione dei processi aziendali a standard dettati da norme tecniche e, precisamente si è munita di:

1) UNA CERTIFICAZIONE ISO 45001:2023 RELATIVA AL "SISTEMA DI GESTIONE DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO" che assicura la conformità della Società agli standard internazionali sui requisiti del sistema di gestione della salute e sicurezza sul lavoro per migliorare la sicurezza e preservare la salute dei lavoratori e del personale esterno e che a seguito della Legge 11 marzo 2026, n. 34, costituisce base di presunzione di conformità ai requisiti dell'art. 30 D.Lgs. 81/2008 per le parti corrispondenti [

2) UNA CERTIFICAZIONE ISO 9001:2015 RELATIVA AL "SISTEMA DI GESTIONE PER LA QUALITÀ" che assicura la conformità della Società agli standard internazionali sui requisiti minimi da rispettare per consentire ad ogni organizzazione aziendale di garantire un ottimo livello di qualità dei prodotti e dei servizi erogati;

3) UNA CERTIFICAZIONE ISO 14001:2015 RELATIVA AL "SISTEMA DI GESTIONE AMBIENTALE" che assicura la conformità della Società agli standard internazionali sui requisiti necessari per fornire una struttura gestionale per l'integrazione delle pratiche di gestione ambientale, perseguendo la protezione dell'ambiente, la prevenzione dell'inquinamento, nonché la riduzione del consumo di energia e risorse;

4) UNA CERTIFICAZIONE ISO 39001:2016 RELATIVA AL "SISTEMA DI GESTIONE PER LA SICUREZZA STRADALE" che assicura la conformità della Società agli standard internazionali sui requisiti necessari per garantire la riduzione del rischio di incidenti gravi in relazione al traffico stradale. Infatti, un sistema di gestione di sicurezza stradale è uno strumento che consente all'organizzazione aziendale che lo ha implementato, la corretta gestione ed il monitoraggio costante di tutte le attività ed i processi ad essa correlati;

5) UNA CERTIFICAZIONE SA 8000:2014 come modello gestionale che si propone di valorizzare e tutelare tutto il personale ricadente nella sfera di controllo e di influenza delle Organizzazioni che lo adottano che vogliono distinguersi per il loro impegno nello sviluppo sostenibile e in particolare per le tematiche sociali

7 RISPETTO DEGLI STANDARD TECNICO STRUTTURALI DI LEGGE

Il RSPP, su indicazione del DL, con la collaborazione del MC, per quanto di sua competenza, e con il coinvolgimento preventivo del RLS, è tenuto a compilare e aggiornare un elenco di tutte le norme di salute e sicurezza applicabili all'azienda in cui riportare il campo di applicazione, la Funzione Aziendale

interessata, il responsabile dell'aggiornamento della normativa e della sua diffusione alle funzioni interessate.

8 L'ACQUISTO, UTILIZZO E MANUTENZIONE DELLE ATTREZZATURE

Tutte le attrezzature di IDRAGEST S.r.l. sono corredate da opportuna documentazione di legge attestante la conformità a tutte le norme di sicurezza e alle norme di riferimento. Su tutte le attrezzature di proprietà viene pianificata una manutenzione ordinaria e straordinaria verificabile da relativi certificati.

Con la cadenza prevista nei libretti d'uso e manutenzione delle apparecchiature e degli impianti il RATTR, anche avvalendosi di personale esperto e qualificato, dovrà effettuare verifiche di adeguatezza, integrità e regolarità degli stessi, in maniera documentale, facendole vistare dal RSPP, e sottoponendole all'approvazione del PRES.

Il RATTER si assicurerà, inoltre, che le attrezzature di lavoro:

- siano oggetto di idonea manutenzione al fine di garantire la permanenza dei requisiti di sicurezza
- siano corredate, ove necessario, da apposite istruzioni d'uso e libretto di manutenzione.

Anche i dispositivi personali di protezione devono essere tenuti in buono stato e sottoposti alla necessaria manutenzione.

A seguito di tali manutenzioni, ogni qualvolta siano effettuate, dovrà essere compilata una scheda con indicazione dell'intervento effettuato, delle parti eventualmente sostituite, la data dell'intervento, la firma del manutentore e la data del successivo intervento.

Il RAM/APVG, annualmente, deve monitorare le spese relative alla "gestione delle manutenzioni", assicurandosi che esse siano in linea con quelli sostenuti negli esercizi precedenti; a tal fine, deve vistare e conservare la documentazione (es. bilanci analitici).Gli appaltatori per poter operare all'interno o in collaborazione con la Società devono dare evidenza del rispetto e adempienza di tutte le norme vigenti applicabili, nonché dei parametri definiti dalla Società all'interno delle proprie procedure.

Il Datore di Lavoro, attraverso la propria struttura organizzativa, secondo quanto previsto dall'art. 26 del D. Lgs 81/2008, qualora siano presenti interferenze, promuove la cooperazione ed il coordinamento di cui ai punti precedenti, elaborando un Documento Unico di Valutazione dei Rischi per le Interferenze, nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo le interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera,

già in fase di procedura di affidamento. Il documento può essere, eventualmente, aggiornato all'atto della consegna delle aree.

È, peraltro, obbligatorio attivare le procedure di cui al TITOLO IV del D. Lgs. 81/2008 nel caso si tratti di cantieri temporanei e mobili.

Durante l'effettuazione dei lavori, il DL o un suo incaricato direttamente o tramite il soggetto identificato per il controllo, deve verificare che gli appaltatori operino ed agiscano in maniera compatibile e congruente con le indicazioni di SSL stabilite in sede di contratto, con la Politica dell'azienda, e con il DUVRI.

Viene regolamentata, anche attraverso *check list* compilative, la dotazione dei mezzi di trasporto al momento della partenza per i cantieri di competenza, del *travel kit* di primo soccorso, dei DPI, dell'attrezzatura per la recinzione dei cantieri e dei dispositivi in dotazione per contattare il Servizio Sanitario Nazionale in caso di infortunio, il tutto in misura adeguata al numero di lavoratori assegnati al cantiere.

Nei contratti di somministrazione (art. 1559 c.c.), di appalto (art. 1655 c.c.) e di subappalto (art. 1656 c.c.), devono essere specificamente indicati i costi relativi alla sicurezza del lavoro con particolare riferimento a quelli propri connessi allo specifico appalto. A tali dati possono accedere tutte le figure coinvolte con le modalità previste dal D. Lgs 81/2008, su richiesta, nonché il RSPP.

8.1 GESTIONE DELLE ATTREZZATURE SPECIFICHE PER LE ATTIVITÀ DI CAMPO

In aggiunta a quanto previsto nella sezione 9, per le attività di rilievo su reti idriche e fognarie, il RATTR, in accordo con il RSPP, deve assicurare che le dotazioni specifiche (es. rilevatori di gas multigas, dispositivi di ancoraggio, sistemi di recupero, indumenti ad alta visibilità) siano sempre in numero adeguato, calibrate, certificate, manutenute ed assegnate nominativamente ai lavoratori, con apposita scheda di consegna e verifica periodica dello stato d'uso.

9 GESTIONE EMERGENZE E PRIMO SOCCORSO

Il DL o un suo incaricato pianifica la gestione delle emergenze come segue:

1. designa i lavoratori, previa consultazione del RSPP e del RLS, incaricati dell'attuazione delle misure di prevenzione e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza. Gli addetti,

prima di essere adibiti a tali mansioni, devono essere formati ed addestrati come previsto dalla legge. Gli addetti alle emergenze e al primo soccorso devono essere disponibili all'occorrenza; la pronta disponibilità è intesa come presenza fisica, sempre assicurata, all'interno degli ambienti di lavoro. Pertanto, nella loro individuazione, è necessario tenere conto: della dislocazione dei lavoratori in più sedi aziendali, dei turni e della presenza di disabili. L'elenco degli addetti antincendio/primo soccorso viene reso noto a tutti i lavoratori e messo loro a disposizione, ad esempio, tramite apposita lista affissa in bacheca;

2. definisce le necessarie misure organizzative e gestionali, da attuare in caso di emergenza, affinché tutto il personale non impegnato nella gestione dell'emergenza possa mettersi al sicuro individuando le vie di esodo, i punti di raccolta, le raccomandazioni rispetto agli atteggiamenti da tenere durante l'evacuazione e redige il Piano di emergenza;
3. organizza le modalità di comunicazione con i servizi pubblici competenti in materia di primo soccorso, salvataggio, lotta antincendio e gestione delle emergenze;
4. stabilisce le modalità di diramazione dell'allarme (es.: sonoro, vocale, luminoso, *etc.*);
5. informa i lavoratori circa le misure predisposte e i comportamenti da adottare;
6. garantisce la presenza di planimetrie chiare, con l'indicazione delle vie di fuga e dei presidi antincendio;
7. organizza esercitazioni con cadenza annuale (similarmente a quanto previsto nel DVR), simulando le emergenze possibili, identificate e riportate, ove presente, nel piano di emergenza. Le esercitazioni sono necessarie al fine di verificare la consapevolezza dei lavoratori e degli addetti alle emergenze relativamente a: vie di fuga; porte resistenti al fuoco, ove esistenti, ubicazione dei dispositivi di allarme e delle attrezzature di spegnimento; collocazione della cassetta di primo soccorso, posizione dei luoghi di raccolta *etc.* L'esito delle prove di emergenza deve essere oggetto di attenta valutazione dell'adeguatezza delle misure di gestione delle emergenze programmate e può dare luogo a miglioramenti delle stesse.

Per la gestione delle emergenze si rinvia a quanto previsto dal sistema di gestione della sicurezza sul lavoro.

Il Datore di Lavoro, in collaborazione con il Medico Competente, organizza il servizio di primo soccorso.

10 COMUNICAZIONE E RAPPORTO CON L'ESTERNO

Il RSPP gestisce le comunicazioni interne ed esterne relativamente alle tematiche di Salute e Sicurezza, coinvolgendo, se opportuno, i lavoratori dell'azienda, come previsto dalla legislazione vigente e dai contratti collettivi di lavoro, raccogliendo osservazioni, commenti e proposte dai lavoratori e dagli altri soggetti interessati (enti locali, cittadini, dipendenti diretti e indiretti, clienti e fornitori, *etc.*).

11 CONSULTAZIONE E PARTECIPAZIONE

L'efficace attuazione del Modello presuppone la piena responsabilizzazione di tutti i soggetti presenti nel luogo di lavoro. L'Azienda promuove, quindi, la piena adesione al Modello di tutti i lavoratori, nonché la cooperazione in materia di salute e sicurezza negli ambienti di lavoro. L'Azienda assicura il tempo necessario per lo svolgimento del proprio incarico (contratti collettivi di lavoro) e la massima collaborazione. I lavoratori devono essere consultati, in particolare. per quanto previsto dalla legislazione vigente (un momento specifico di consultazione è la riunione *ex* art 35 del D.lgs. 81/2008).

12 ATTIVITÀ DI INFORMAZIONE E FORMAZIONE DEI LAVORATORI

Il DL ha la responsabilità di fornire i mezzi e le risorse adeguate allo svolgimento delle attività di addestramento, formazione ed informazione, incluse le competenze esterne o interne necessarie per la loro esecuzione; a questi spetta il compito di approvare il "Programma di formazione, informazione ed addestramento" proposto dal RSPP in collaborazione col RLS ed il Medico Competente; detto programma deve essere aggiornato in occasione della revisione ed eventuale rielaborazione della valutazione dei rischi, nel caso di modifiche legislative, di nuove assunzioni, di cambiamenti nelle mansioni, nei cambiamenti di attività o processi (nuove macchine, attrezzature, impianti, nuove modalità operative, etc.), dell'evoluzione tecnica.

Il RSPP ha il dovere di compilare il registro personale della formazione/informazione/addestramento per ciascun lavoratore e per i neo assunti e ha la responsabilità di conservare, nell'archivio delle registrazioni, la documentazione comprovante la formazione, l'informazione e l'addestramento effettuato (verbali di addestramento, copie di attestati di partecipazione, diplomi, etc.), i risultati relativi alla verifica delle qualifiche e all'efficacia delle azioni formative eseguite.

Al termine degli interventi formativi, deve essere verificato il grado di apprendimento secondo le modalità previste dall'Accordo Stato Regioni in materia di Formazione alla salute e sicurezza nei luoghi di lavoro, sia per i corsi organizzati dal DL stesso che per quelli erogati presso soggetti esterni.

Nell'ambito del programma di formazione è obbligatorio, inoltre, formare i lavoratori sugli aspetti principali del MOG e su ruoli, compiti e responsabilità di ciascuna figura in esso coinvolta.

Si precisa che la gestione dell'informazione dei lavoratori verrà implementata nell'organizzazione aziendale con l'ausilio di uno strumento didattico, ovvero di un un opuscolo informativo includente gli argomenti del D.Lgs 81/08, redatto dal RSPP in modo da risultare facilmente comprensibile e soprattutto specifico per l'attività svolta dall'azienda.

IDRAGEST assicura, altresì, ai propri dipendenti un'informazione ed una formazione adeguata in ragione del tipo di attività resa. Infatti, è prevista una formazione specifica che, tuttavia, non è sostitutiva della formazione obbligatoria spettante, comunque, a tutti i lavoratori e realizzata ai sensi dell'articolo 37 del d.lgs. n. 81/2008. Tale formazione deve, pertanto, considerarsi integrativa della formazione prevista dall'accordo Stato-Regioni di cui all'articolo 37, comma 2, del d.lgs. n. 81/2008.

I CORSI AGGIUNTIVI SONO DIRETTI A:

- lavoratori adibiti all'installazione ed alla rimozione della segnaletica di cantieri stradali in presenza di traffico o comunque addetti ad attività in presenza di traffico;
- preposti alle attività di cui all'articolo 1 del presente decreto;
- lavoratori addetti che svolgono attività lavorativa negli ambienti sospetti di inquinamento (artt. 66 e 121 del D. Lgs 81/2008) o spazi confinati (allegato IV – punto 3 del D. Lgs 81/2008). In particolare, i lavoratori devono essere in possesso di adeguata esperienza professionale, formazione, addestramento nonché specifica idoneità sanitaria.

OBBLIGHI DEI LAVORATORI

I lavoratori si sottopongono al programma di formazione e addestramento organizzato dal datore di lavoro. I lavoratori utilizzano i DPI e DPC messi a loro disposizione conformemente all'informazione e alla formazione ricevute e all'addestramento eventualmente organizzato, inoltre hanno cura dei DPI messi a loro disposizione e non vi apportano modifiche di propria iniziativa (art. 78 comma 3 D. Lgs. 81/08).

Al termine dell'utilizzo i lavoratori seguono le procedure aziendali in materia di riconsegna dei DPI e segnalano immediatamente al datore di lavoro o al dirigente o al preposto qualsiasi difetto o inconveniente da essi rilevato nei DPI messi a loro disposizione (art. 78, comma 4 e 5, D. Lgs. 81/08)

14 LO STANZIAMENTO DI FONDI PER LA GESTIONE DEL SSL

L'Organo amministrativo, in occasione dell'assemblea annuale di approvazione del bilancio, deve sottoporre all'assemblea dei soci lo stanziamento di adeguati fondi da destinare, nell'anno, in favore della Sicurezza e della Salute dei Lavoratori.

E' compito dell'Organismo di Vigilanza verificare l'effettiva approvazione del predetto stanziamento.

15 RIESAME E VERIFICA ATTUAZIONE ED EFFICACIA DEL MODELLO

Il DL deve riesaminare, annualmente, in relazione agli adempimenti relativi alla sicurezza sul lavoro, e con l'ausilio di consulenti all'uopo preposti, il Modello Organizzativo Gestionale per verificare che:

- sia attuato con efficacia;
- sia idoneo per il mantenimento ed il miglioramentodelle misure adottate;
- garantisca il raggiungimento degli obiettivi di SSL;
- permetta di esprimere una valutazione sulle prestazioni complessive;
- consenta di programmare le attività per il miglioramento continuo.

IN PARTICOLARE, IL DL DOVRÀ VERIFICARE:

- ✓ i risultati del monitoraggio interno, con riferimento al grado di raggiungimento degli obiettivi;
- ✓ gli esiti delle azioni intraprese nel precedente riesame e la loro efficacia;
- ✓ i dati sugli infortuni e malattie professionali;
- ✓ le analisi delle cause di eventuali infortuni, incidenti e situazioni di emergenza;
- ✓ le relazioni del Medico Competente, se nominato;
- ✓ i cambiamenti, interni ed esterni, rilevanti per l'impresa (nuove lavorazioni, personale, contratti, nuove leggi, novità in relazione al progresso scientifico e tecnologico, *etc.*) e l'emergere di eventuali nuovi rischi;
- ✓ rapporti sulle prove di emergenza;
- ✓ risultati delle azioni correttive e preventive intraprese sul modello;
- ✓ risultati della consultazione e del coinvolgimento;
- ✓ dati sulla formazione e addestramento effettuati;
- ✓ report o segnalazioni da parte dell'OdV;
- ✓ eventuali sanzioni applicate.

Qualora il DL lo ritenga opportuno può far coincidere il Riesame con la riunione periodica, ove prevista, *ex* art. 35 del D.lgs, 81/2008 e ss.mm.ii. In questo caso, le Figure Aziendali interessate ed i temi trattati devono rispettare anche quanto previsto dalla legislazione.

16 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Le Funzioni Aziendali responsabili dell'individuazione, dell'attuazione e del controllo sulle misure relative alla sicurezza, all'igiene e alla salute nei luoghi di lavoro sono tenuti a comunicare, tempestivamente e direttamente, all'Organismo di Vigilanza (OdV) qualsiasi condotta posta in essere in difformità al Modello, alla presente procedura ed al Codice Etico, indicando le ragioni delle difformità e precisando il processo autorizzativo seguito.

IL DATORE DI LAVORO, O SOGGETTO DEBITAMENTE AUTORIZZATO, INFORMA TEMPESTIVAMENTE L'ODV CIRCA:

- quasi infortuni e tutti gli infortuni che si verificano;
- eventuali azioni e/o interventi e/o provvedimenti dell'Autorità Giudiziaria nonché della Polizia Giudiziaria (compresa la ASL con funzione di Polizia Giudiziaria), o di altra Autorità competente, in caso di verifica circa il rispetto della normativa vigente in materia di sicurezza sui luoghi di lavoro;
- i *report* rilasciati dagli organismi di certificazione in sede di *audit*, e delle eventuali non conformità riscontrate.

In particolare, il Datore di Lavoro – coadiuvato dal Responsabile del Servizio di Prevenzione e Protezione – almeno annualmente provvede a informare/inviare l'OdV:

- in merito agli esiti delle verifiche sulla corretta attuazione della normativa vigente, informando lo stesso, costantemente, relativamente allo stato dei suggerimenti avanzati in sede di attività ispettiva;
- in merito alle statistiche relative agli incidenti verificatisi sul luogo di lavoro, specificandone la causa, l'avvenuto riconoscimento di infortuni e la relativa gravità;
- in merito all'andamento della sorveglianza sanitaria ed ai relativi esiti (relazione sanitaria annuale del medico competente e denunce di malattie professionali);
- in merito ad ogni variazione che richieda, o che abbia richiesto, l'aggiornamento della valutazione dei rischi;
- in merito agli acquisti/investimenti in situazioni di emergenza ed *extra-budget*;

- il verbale della riunione periodica (art. 35 D.lgs. 81/2008);
- il piano della formazione;
- lo stato di avanzamento rispetto al programma di miglioramento in materia di salute e sicurezza sul luogo di lavoro;
- eventuali provvedimenti disciplinari adottati nei confronti dei destinatari della presente procedura, per violazioni riguardanti la salute e sicurezza nei luoghi di lavoro.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari;

• proporre un eventuale aggiornamento del Modello o delle procedure previste per la sua attuazione, previa condivisione con il Datore di Lavoro.

Le Funzioni Aziendali devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio ordinato – tutta la documentazione all'uopo necessaria.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing", adottata ai sensi del D.Lgs. 24/2023 per dare attuazione a quanto previsto dall'art. 6, comma 2-bis, del D.Lgs. 231/2001, garantendo la riservatezza del segnalante e la protezione da qualsiasi ritorsione.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 09.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 03	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

Sommario 2

1 OBIETTIVI E LA FUNZIONE DEL MODELLO 3

2 ACRONIMI AZIENDALI 3

3 RIFERIMENTI NORMATIVI 4

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA 4

5 PRINCIPI GENERALI DI COMPORTAMENTO 4

5.1 Utilizzo di Sistemi di Intelligenza Artificiale (IA) e Contrasto al Web Scraping Abusivo 11

5. 2 PRESIDI E PROCEDURE PER L'USO DELL'INTELLIGENZA ARTIFICIALE 11

5.3 Mitigazione del Rischio di Allucinazione e Validazione dei Risultati (AI Quality Assurance) 12

5. 4. Alfabetizzazione e Formazione Obbligatoria (AI Literacy) 13

6 Il sistema dei controlli e i presidi a mitigazione dei rischi reato 13

7 Legge sulla protezione del diritto d'autore - Accordi tra SIAE, altri organismi di gestione collettiva ed entità di gestione indipendenti (Art. 181-bis L. 633/1941 introdotto e modificato da Legge n.166 del 14 novembre 2024) 14

8 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 15

1 OBIETTIVI E LA FUNZIONE DEL MODELLO

Il presente protocollo definisce i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento adottati da IDRAGEST S.r.l. nell'ambito del processo di gestione ed utilizzo di opere dell'ingegno per le attività a rischio connesse alle fattispecie di reato previste dall'art. 25 novies *"Reati in materia di violazione del diritto di autore"*, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione, nonché tracciabilità delle attività.

Inoltre, al fine di contrastare ancor più severamente la pirateria delle opere dell'ingegno e i gravi danni economici arrecati agli autori e all'industria connessa, la presente procedura rimanda ai reati contemplati dalla legge sul diritto d'autore (L. 633/1941).

Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Codice Etico di IDRAGEST.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RSGQ	Responsabile Sistema di Gestione Qualità
RAM	Responsabile Amministrazione - Risorse Umane
RTEC	Responsabile Tecnico
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RFAM	Responsabile Facility Management
RPROG	Responsabile Progettazione
RSCM	Responsabile singola commessa
RATTR	Responsabile Attrezzature e Mezzi
PROG	Programmatori

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE IN VIGORE.

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di IDRAGEST S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l.;
- Decreto-Legge 16 settembre 2024, n. 131, convertito con modificazioni dalla Legge 14 novembre 2024, n. 166;
- Legge 23 settembre 2025, n. 132 ("Disposizioni e deleghe al Governo in materia di intelligenza artificiale");
- Delibera ANAC n. 148 del 1° aprile 2026 (Aggiornamento Bando tipo n. 1-2023 in materia di IA);
- Decreto Ministeriale n. 180 del 17 dicembre 2025 (Linee guida per l'implementazione dell'IA nel mondo del lavoro).

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutti i *Destinatari* coinvolti nelle attività di gestione ed utilizzo di opere dell'ingegno all'interno della Società.

In particolare, la presente procedura si applica a tutto il personale dipendente, ai collaboratori esterni, ai consulenti, ai tecnici di cantiere e ai programmatori di IDRAGEST S.r.l. coinvolti nelle attività di:

1. Rilievo topografico, catastale e restituzione cartografica su Sistemi Informativi Territoriali (SIT);
2. Sviluppo e integrazione di software personalizzato e basi di dati;
3. Progettazione di opere civili e idrauliche (fognature, acquedotti);
4. Redazione di specifiche tecniche e supporto alla valutazione di offerte di fornitori terzi.

Il principale responsabile dell'attuazione e del costante aggiornamento della presente procedura è il PRES.

5 PRINCIPI GENERALI DI COMPORTAMENTO

Le Funzioni Aziendali che, per ragione del proprio incarico o della propria funzione, sono coinvolte nella gestione ed utilizzo di opere dell'ingegno e dei sistemi informatici aziendali devono rispettare le norme in materia di proprietà intellettuale ed impiegare i beni aziendali per adottare condotte che non violino la tutela dei diritti d'autore.

Inoltre, è fatto divieto di utilizzare o installare programmi diversi da quelli autorizzati.

La presente procedura è strettamente correlata con la PMOG 08 "Gestione ed utilizzo delle risorse informatiche" e con la PMOG 03 "Gestione operazioni di tesoreria".

I DESTINATARI DEVONO ATTENERSI, OGNUNO PER LE PARTI DI COMPETENZA, AI SEGUENTI DIVIETI:

- è vietato violare le condizioni di licenza di un software;
- è vietato acquistare software "pirati" per l'azienda;
- è vietato utilizzare banche dati senza la relativa autorizzazione;
- è vietato distribuire ed installare dispositivi di decodificazione per l'accesso a un servizio criptato, senza pagamento del canone;
- è vietato l'impiego per finalità aziendali di beni tutelati da diritti acquisiti in elusione dei relativi obblighi o, comunque, con modalità difformi da quelle previste dal titolare;
- è vietata la condivisione o lo scambio di file in violazione della normativa del diritto d'autore e, comunque, al di fuori degli ordinari e leciti circuiti commerciali dei beni oggetto di proprietà intellettuale (File sharing);
- è vietata l'immissione o condivisione, senza averne diritto, di contenuti protetti da diritti d'autore in un sistema di reti telematiche (upload/download);
- è vietato l'utilizzo di apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere reati riguardanti gli strumenti di pagamento diversi dai contanti o sono specificamente adattati al medesimo scopo;
- è vietato l'utilizzo e l'installazione abusiva di apparecchiature ed altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche, nonché le condotte atte a danneggiare o interrompere un sistema informatico o telematico.

IDRAGEST, assicura il puntuale rispetto delle norme in materia di proprietà intellettuale e della tutela dei diritti d'autore.

Legge n. 166 del 14 novembre 2024 E LEGGE N.132 DEL 23 SETTEMBRE 2025 "DISPOSIZIONI E DELEGHE AL GOVERNO IN MATERIA DI INTELLIGENZA ARTIFICIALE"

Il 15 novembre 2024 è entrata in vigore la Legge 166/2024, che ha convertito con modificazioni il Decreto Legge 131/2024 del 16 settembre 2024. Questo intervento normativo, pubblicato nella Gazzetta Ufficiale n. 267 del 14 novembre 2024, introduce importanti cambiamenti in materia di diritto d'autore e nella disciplina sanzionatoria prevista dal Decreto Legislativo 231/2001.

La Legge 166/2024 è stata emanata per adeguare l'ordinamento italiano agli obblighi derivanti dall'Unione Europea, in particolare per rispondere a una procedura di infrazione avviata contro l'Italia. L'obiettivo è garantire una maggiore conformità alle direttive europee in tema di gestione collettiva del diritto d'autore e di concorrenza nel settore.

1) ATTIVITÀ DI INTERMEDIAZIONE NEL DIRITTO D'AUTORE:

L'esclusiva della Società Italiana degli Autori ed Editori (SIAE) è stata superata.

Ora, anche altri organismi di gestione collettiva e entità di gestione indipendenti possono svolgere attività di intermediazione nel settore del diritto d'autore.

2) ESTENSIONE DELLE SANZIONI PENALI:

Gli articoli 171-bis, 171-ter e 171-septies della Legge 633/1941 puniscono non solo la contraffazione dei contrassegni SIAE, ma anche quella relativa ai contrassegni rilasciati da altri organismi di gestione collettiva o da entità di gestione indipendenti.

Peraltro, la legge n. 187 del 9 dicembre 2024 ha semplificato le procedure per l'ingresso di lavoratori dall'estero, introducendo tra l'altro una gestione telematica delle domande di nulla osta, con la possibilità di apporre firma digitale ai permessi. Nella gestione dei flussi il decreto, e ora la legge di conversione, rafforza le tutele per le vittime di caporalato, tratta e sfruttamento lavorativo.

La legge 132/2025, in particolare, rinvia all'art. 3, par. 1, n. 1, AI Act, che definisce un "sistema di i.a." come «*un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali*».

La legge 132/2025 ha introdotto la disposizione di cui all'art. 612 quater c.p.c. "*Illecita diffusione di contenuti generati o manipolati artificialmente* ", che punisce con la reclusione da uno a cinque anni «*chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità*». *Il delitto è punibile a querela della persona offesa, salvo che il fatto sia connesso con un altro delitto per il quale si deve procedere d'ufficio oppure sia «commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate*».

In materia di diritto d'autore, la legge 132/2025 introduce poi una nuova fattispecie all'art. 171, c. 1, lett. a-ter, l. 22 aprile 1941, n. 633, che punisce chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma, «*riproduce o estrae testo o dati da opere o altri materiali disponibili in rete o in banche di dati in violazione degli articoli 70-ter e 70-quater, anche attraverso sistemi di intelligenza artificiale*». Tale fattispecie di reato si va ad

aggiungere alle fattispecie già previste dall'art. 171 l. 633/1941 in materia di violazione del diritto d'autore; come queste ultime, la nuova fattispecie è punita con la pena della multa da 51 a 2.065 euro, e si applica salvo quanto previsto dagli artt. 171-bis e 171-ter (che puniscono, rispettivamente, la duplicazione di "programmi per elaboratore" e la diffusione abusiva, per uso non personale, di opere letterarie. Invero, la nuova figura di reato mira a contrastare il fenomeno del c.d. data scraping, ovverosia di quella pratica di estrazione massiva, indiscriminata e non autorizzata di contenuti pubblicati online, finalizzata ad addestrare i modelli di i.a.

IDRAGEST assicura, altresì, l'utilizzo e l'installazione di programmi autorizzati.

Invero, le suddette condotte vengono poste in essere, al fine di prevenire i reati previsti dal D.Lgs. 231/2001 all'art. 25-novies e, precisamente:

• DIVULGAZIONE TRAMITE RETI TELEMATICHE DI UN'OPERA DELL'INGEGNO PROTETTA (ART. 171 COMMA 1 LETT. A-BIS E COMMA 3. LEGGE 633/1941 MODIFICATO DALLA L. N.166 DEL 14 NOVEMBRE 2024).

In relazione alla fattispecie delittuosa di cui all'art. 171 della Legge sul Diritto d'Autore, il Decreto 231 ha preso in considerazione esclusivamente due fattispecie, ovvero:

- la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa;
- la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

Se, dunque, nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete, nella seconda ipotesi il bene giuridico protetto non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

• MESSA A DISPOSIZIONE DEL PUBBLICO DI UN'OPERA DELL'INGEGNO PROTETTA O DI PARTE DI ESSA ART. 171, L. 633/1941 COMMA 1 LETTERA A) BIS

"*Salvo quanto disposto dall´art. 171-bis e dall´articolo 171-ter è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:*

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un´opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nello Stato esemplari prodotti all´estero contrariamente alla legge italiana;

a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un´opera dell´ingegno protetta, o parte di essa;

b) rappresenta, esegue o recita in pubblico o diffonde, con o senza variazioni od aggiunte, un´opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell´opera cinematografica, l´esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;

c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di riprodurre o di rappresentare;

e) (soppresso)"

• RIPRODUZIONE, TRASFERIMENTO SU ALTRO SUPPORTO DEL CONTENUTO DI UNA BANCA DATI (ART. 171-BIS L. 633/1941 COMMA 2, MODIFICATO DALLA LEGGE N. 166/2024)

Chiunque, al fine di trarne profitto, su supporti non contrassegnati ai sensi della L. n.166/2024 riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

La norma mira a sanzionare penalmente fatti offensivi del diritto d'autore. Il reato è integrato da varie condotte alternative: duplicazione di programmi per elaboratore, importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale, concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; ovvero riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione in pubblico del contenuto di una banca dati in violazione delle disposizioni, estrazione, reimpiego della banca dati, distribuzione, vendita o concessione in locazione della banca dati.

Con particolare riferimento al processo di liberalizzazione del settore della gestione collettiva dei diritti d'autore, all'apertura del mercato anche alle entità di gestione indipendenti e all'integrazione delle disposizioni inerenti alla gestione di alcune facoltà esclusive, attraverso la L. n.166 del 14 novembre 2024, si è avuto l'ampliamento dei soggetti ammessi all'esercizio dell'attività di intermediazione, eliminando l'obbligo di applicazione del contrassegno SIAE, che può comunque essere apposto su richiesta degli interessati, estendendo l'ambito oggettivo di applicazione dei reati relativi alla tutela dei diritti d'autore in modo da ricomprendervi anche i contrassegni apposti da organismi di gestione collettiva o dalle entità di gestione indipendenti.

- **LEGGE SULLA PROTEZIONE DEL DIRITTO D'AUTORE - ABUSIVA DUPLICAZIONE CONTENUTA IN SUPPORTI NON CONTRASSEGNATI AI SENSI DELLA L. N.166/2024- (ART. 171-BIS L. 633/1941 COMMA 1 – MODIFICATO DA L. N.166 DEL 14 NOVEMBRE 2024)**

Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati ai sensi della L. n.166/2024 è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

- **LEGGE SULLA PROTEZIONE DEL DIRITTO D'AUTORE - ABUSIVA DUPLICAZIONE DI OPERE DELL'INGEGNO DESTINATE AL CIRCUITO TELEVISIVO, CINEMATOGRAFICO, ETC. (ART. 171-TER L. 633/1941 MODIFICATO DA LEGGE N.93 DEL 14 LUGLIO 2023 E DA L. N.166 DEL 14 NOVEMBRE 2024)**

È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento

La Legge n.93 del 14 luglio 2023 ha inserito il comma h-bis nel contrasto alla diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica.
h-bis) abusivamente, anche con le modalità indicate al comma 1 dell'articolo 85-bis del testo unico delle leggi di pubblica sicurezza, di cui al regio decreto 18 giugno 1931, n. 773, esegue la fissazione su supporto digitale, audio, video o audiovideo, in tutto o in parte, di un'opera cinematografica, audiovisiva o editoriale ovvero effettua la riproduzione, l'esecuzione o la comunicazione al pubblico della fissazione abusivamente eseguita.

- **LEGGE SULLA PROTEZIONE DEL DIRITTO D'AUTORE - MANCATA COMUNICAZIONE DEI DATI DI IDENTIFICAZIONE DEI SUPPORTI AI SENSI DELLA L. N.166/2024 (ART. 171-SEPTIES L. 633/1941 – MODIFICATO DA L. N.166/2024)**

La pena di cui all'articolo 171-ter, comma 1, si applica, salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

- **FRAUDOLENTA PRODUZIONE, VENDITA O IMPORTAZIONE DI APPARATI DI DECODIFICA (ART. 171-OCTIES L. 633/1941)**

"*Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.*

La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità."

- **LEGGE SULLA PROTEZIONE DEL DIRITTO D'AUTORE (ART. 174-TER L. 633/1941 MODIFICATO DA LEGGE N.93 DEL 14 LUGLIO 2023)**

La nuova legge 93/2023 ha ad oggetto "*Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica*". La legge mira a contrastare più incisivamente gli abusi e le violazioni del diritto d'autore online, revisionando e integrando le disposizioni già vigenti.

In particolare, la citata legge ha disposto l'aumento della "*sanzione amministrativa sino a 5000 euro in caso di recidiva o di fatto grave nella diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica come indicato al comma 2 sotto riportato.*

2. In caso di recidiva o di fatto grave per la quantità delle violazioni o delle copie acquistate o noleggiate o per la quantità di opere o materiali protetti resi potenzialmente accessibili in maniera abusiva attraverso gli strumenti di cui al comma 1, la sanzione amministrativa è aumentata sino ad euro 5.000,00 ed il fatto è punito con la confisca degli strumenti e del materiale, con la pubblicazione del provvedimento su due o più giornali quotidiani a diffusione nazionale o su uno o più periodici specializzati nel settore dello spettacolo e, se si tratta di attività imprenditoriale, con la revoca della concessione o dell'autorizzazione di diffusione radiotelevisiva o dell'autorizzazione per l'esercizio dell'attività produttiva o commerciale".

5.1 Utilizzo di Sistemi di Intelligenza Artificiale (IA) e Contrasto al Web Scraping Abusivo

In applicazione della Legge n. 132/2025 e a tutela della proprietà intellettuale online:

Divieto di Web Scraping non autorizzato (Art. 171, c. 1, lett. a-ter L.d.A.): È vietato riprodurre o estrarre testi, dati, immagini o cartografie da opere o materiali disponibili in rete o in banche di dati, anche attraverso sistemi di intelligenza artificiale, in violazione degli articoli 70-ter e 70-quater della legge sul diritto d'autore (c.d. data mining o web scraping abusivo per l'addestramento di modelli o la creazione di dataset aziendali). Qualsiasi attività di estrazione dati deve essere preceduta dalla verifica delle condizioni d'uso dei siti web d'origine e del rispetto del diritto di opt-out esercitato dai titolari dei diritti.

Divieto di utilizzo di contenuti generati o alterati con IA (Art. 612-quater c.p.): È vietato produrre, cedere o diffondere, senza il consenso dell'interessato, immagini, video o voci falsificati o alterati tramite IA (c.d. deepfake) idonei a indurre in inganno sulla loro genuinità e tali da cagionare un danno ingiusto.

Divieto di immissione di dati riservati (Information Risk): È vietato inserire informazioni riservate dell'azienda, specifiche tecniche protette da segreto industriale, dati sensibili relativi alla consistenza delle reti dei fluidi dei clienti o dati personali nei sistemi di IA generativa esterni privi di adeguate garanzie contrattuali di riservatezza e protezione dei dati.

5. 2 PRESIDI E PROCEDURE PER L'USO DELL'INTELLIGENZA ARTIFICIALE

Dichiarazioni in Materia di IA nei Contratti e Appalti Pubblici (Delibera ANAC n. 148/2026)

Qualora IDRAGEST partecipi a procedure di affidamento di contratti pubblici per servizi di ingegneria, progettazione, rilievi topografici o sviluppo software, il Responsabile Commerciale (RCOM/APVG) e il Responsabile della Singola Commessa (RSCM) devono garantire che nella predisposizione dell'offerta tecnica e nell'espletamento delle prestazioni siano rese le dichiarazioni conformi allo schema ANAC.
In particolare:

1. **IN SEDE DI PRESENTAZIONE DELL'OFFERTA LA SOCIETÀ DOVRÀ DICHIARARE:**

"*IDRAGEST S.r.l. DICHIARA che nella predisposizione dell'offerta:*

- non si è avvalso di sistemi di intelligenza artificiale;

o, in alternativa

- si è avvalso di sistemi di intelligenza artificiale per lo svolgimento di attività meramente strumentali e di supporto nella redazione dell'offerta tecnica, nel rispetto del Regolamento UE 2024/1689, della legge n. 132 del 2025 e della vigente normativa sul trattamento e protezione dei dati (Regolamento UE 2016/679, D.Lgs. 196/2003)."

2. IN CASO DI AGGIUDICAZIONE DELLA COMMESSA, IDRAGEST SI IMPEGNA A:

"*avvalersi di sistemi di intelligenza artificiale al fine esclusivo di supportare ed efficientare il servizio, assicurando comunque la prevalenza del lavoro intellettuale, il controllo e la verifica dei risultati ottenuti (c.d. validazione umana) e garantendo che l'uso di tali sistemi avverrà nel rispetto del Regolamento UE 2024/1689, della legge n. 132 del 2025 e della vigente normativa sul trattamento e protezione dei dati."*

5.3 Mitigazione del Rischio di Allucinazione e Validazione dei Risultati (AI Quality Assurance)

Nello sviluppo di software personalizzato, nella modellazione di bilanci idrici e nella gestione delle perdite di rete tramite algoritmi predittivi, si applicano i seguenti standard organizzativi (ispirati alle migliori pratiche di trasparenza AGCM):

- Rapporto di Conformità e Validazione Tecnica: Ogni output generato da sistemi di IA (codice sorgente generato da assistenti di codifica, calcoli di bilanci idrici automatizzati, elaborazioni di dati topografici) deve essere sottoposto a un controllo sistematico e a una verifica critica (peer review) da parte del Responsabile di Progettazione (RPROG) o dei Programmatori (PROG) prima della sua integrazione nei sistemi finali destinati al cliente.

- Prevenzione dei Bias e del Plagio: Gli strumenti di IA impiegati devono essere monitorati per prevenire violazioni involontarie di copyright (es. copia di porzioni di codice open source protette da licenze restrittive tipo GPL senza attribuzione) o errori sistematici ("allucinazioni").

5. 4. Alfabetizzazione e Formazione Obbligatoria (AI Literacy)

In attuazione dell'art. 4 dell'AI Act, del D.M. 180/2025 del Ministero del Lavoro e della Legge 132/2025, IDRAGEST organizza annualmente corsi di formazione obbligatori per il proprio personale (ingegneri, programmatori, tecnici e amministrativi) sui rischi operativi, etici e legali connessi all'uso dell'Intelligenza Artificiale, con particolare attenzione alla protezione dei dati e alla tutela del diritto d'autore.

6 IL SISTEMA DEI CONTROLLI E I PRESIDI A MITIGAZIONE DEI RISCHI REATO

Per ognuna delle attività sensibili identificate sono stati individuati i sistemi dei controlli e i presidi in essere a mitigazione dei rischi reato in riferimento ai reati di delitti in materia di violazione del diritto di autore,

IN PARTICOLARE:

- Adozione di regole comportamentali all'interno del Codice Etico che prevedono il divieto a tutte le funzioni aziendali, nell'ambito delle proprie attività lavorative e/o mediante utilizzo delle risorse di IDRAGEST di porre in essere comportamenti di qualsivoglia natura atti a ledere diritti di proprietà intellettuale altrui, assicurando il rispetto delle leggi e delle disposizioni regolamentari nazionali, comunitarie e internazionali poste a tutela della proprietà industriale, della proprietà intellettuale e del diritto d'autore;
- disporre una regola comportamentale che impone ai dipendenti di curare diligentemente gli adempimenti di carattere amministrativo connessi all'utilizzo di opere protette dal diritto d'autore (software, banche dati, ecc.) nell'ambito dell'utilizzo di applicazioni software di terzi;
- **PER QUANTO ATTIENE ALL'USO DELLE DOTAZIONI INFORMATICHE È RICHIESTO AI DIPENDENTI DI NON:**

✓ I software e le banche dati installati sui sistemi informativi dell'azienda siano sempre muniti di valida licenza di utilizzo

✓ La rete informatica aziendale ed i dati presenti nella stessa siano preservati da accessi ed utilizzi impropri

✓ utilizzare in azienda apparecchiature informatiche private, connettendole in qualsiasi modo alla rete informatica aziendale;

✓ installare sui computer o sui dispositivi aziendali assegnati programmi (software) provenienti dall'esterno ovvero dispositivi di memorizzazione, comunicazione o altro (masterizzatori, modem, chiavi USB);

✓ duplicare CD e DVD od ogni altro supporto multimediale atto a contenere dati di qualsiasi natura protetti dalla normativa a tutela del diritto d'autore.

- IDRAGEST garantisce che i software di terzi utilizzati per lo svolgimento delle attività aziendali, siano opportunamente identificati e che il pagamento delle licenze ai rispettivi fornitori, sia oggetto di un controllo periodico.

A TAL FINE È RICHIESTO A TUTTI I DESTINATARI DI:

- Utilizzare esclusivamente i software, le applicazioni, i files e le apparecchiature informatiche fornite dall'azienda e farlo esclusivamente per finalità strettamente attinenti allo svolgimento delle proprie mansioni
- Osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici ed ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'azienda
- Rispettare le policy interne in merito ai dispositivi antintrusione e antivirus
- Custodire le password di accesso alla rete aziendale ed alle diverse applicazioni e le chiavi personali secondo criteri idonei a impedirne una facile individuazione ed un uso improprio
- Non prestare o permettere a terzi l'uso delle apparecchiature informatiche aziendali o dell'archivio informatico della stessa, senza la preventiva autorizzazione del Responsabile della Sicurezza dei Sistemi Informativi
- Astenersi dall'effettuare copie non specificamente autorizzate dal Responsabile della Sicurezza dei Sistemi Informativi di dati e di software di proprietà dell'azienda
- Evitare di trasferire all'esterno dell'azienda e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà interna, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni
- Qualora per la connessione alla rete internet si utilizzino collegamenti wireless, proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni all'azienda, possano illecitamente collegarsi alla rete internet tramite i router della stessa e compiere illeciti ascrivibili ai dipendenti
- Utilizzare opere dell'ingegno senza l'autorizzazione del soggetto che legittimamente ne detiene i diritti, ovvero senza aver stipulato un valido contratto di licenza

7 LEGGE SULLA PROTEZIONE DEL DIRITTO D'AUTORE - ACCORDI TRA SIAE, ALTRI ORGANISMI DI GESTIONE COLLETTIVA ED ENTITÀ DI GESTIONE INDIPENDENTI (ART. 181-BIS L. 633/1941 INTRODOTTO E MODIFICATO DA LEGGE N.166 DEL 14 NOVEMBRE 2024)

Il legislatore con la Legge n.166/2024 ha sancito che la Società italiana degli autori ed editori (SIAE), gli altri organismi di gestione collettiva o le entità di gestione indipendenti, su richiesta degli interessati, possono apporre un contrassegno su ogni supporto contenente programmi per elaboratore o multimediali nonché su ogni supporto contenente suoni, voci o immagini in movimento, destinati ad essere posti comunque in commercio o ceduti in uso a qualunque titolo a fine di lucro.

Con il comma 2 il legislatore dispone che il contrassegno è apposto sui supporti di cui al comma 1 ai soli fini della tutela dei diritti relativi alle opere dell'ingegno, previa attestazione da parte del richiedente dell'assolvimento degli obblighi derivanti dalla normativa sul diritto d'autore e sui diritti connessi.

Al comma 3 è sancito che il contrassegno, secondo modalità e nelle ipotesi previste nel regolamento di cui al comma 4, che tiene conto di apposite convenzioni stipulate tra la SIAE, gli altri organismi di gestione collettiva o le entità di gestione indipendenti e le categorie interessate, può non essere apposto sui supporti contenenti programmi per elaboratore disciplinati dal decreto legislativo 29 dicembre 1992, n. 518, utilizzati esclusivamente mediante elaboratore elettronico, sempre che tali programmi non contengano suoni, voci o sequenze di immagini in movimento tali da costituire opere fonografiche, cinematografiche o audiovisive intere, non realizzate espressamente per il programma per elaboratore.
Inoltre, viene stabilito che il contrassegno deve avere, comunque, caratteristiche tali da non poter essere trasferito su altro supporto contenendo elementi tali da permettere l'identificazione del titolo dell'opera per la quale è stato richiesto, del nome dell'autore, del produttore o del titolare del diritto d'autore. Deve contenere altresì l'indicazione di un numero progressivo per ogni singola opera riprodotta o registrata nonché della sua destinazione alla vendita, al noleggio e a qualsiasi altra forma di distribuzione.
Per quanto attiene l'apposizione materiale del contrassegno, la stessa può essere affidata anche in parte al richiedente o ad un terzo da questi delegato, i quali assumono le conseguenti responsabilità in termini di legge. I medesimi soggetti informano almeno trimestralmente la SIAE, gli altri organismi di gestione collettiva e le entità di gestione indipendenti circa l'attività svolta e lo stadio di utilizzo del materiale consegnato.
La SIAE, gli altri organismi di gestione collettiva o le entità di gestione indipendenti e il richiedente possono concordare che l'apposizione del contrassegno sia sostituita da attestazione temporanea resa ai sensi del comma 2, corredata dalla presa d'atto della SIAE, degli altri organismi di gestione collettiva o delle entità di gestione indipendenti.

Infine, al comma 8 il legislatore statuisce che, agli effetti dell'applicazione della legge penale, il contrassegno è considerato come un segno distintivo di opera dell'ingegno.

8 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutte le Funzioni Aziendali coinvolte nelle attività di gestione ed utilizzo delle opere di ingegno sono tenuti a comunicare tempestivamente all'Organismo di Vigilanza:

- qualsiasi violazione ai principi di comportamento adottati;
- qualsiasi situazione non conforme alla normativa;

- qualsiasi violazione del Modello e del Codice Etico, indicando le ragioni delle difformità e rilevando il processo autorizzativo seguito.

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio ordinato – tutta la documentazione all'uopo necessaria.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse alla presente procedura, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo, nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI 2

2 ACRONIMI AZIENDALI 2

3 INDICAZIONI COMPORTAMENTALI 4

4 ABBREVIAZIONI ..... **Errore. Il segnalibro non è definito.**

3 RIFERIMENTI NORMATIVI 3

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA 3

5 L'UTILIZZO DI RISORSE FINANZIARIE LEGATO AGLI INVESTIMENTI E/O ACQUISTO DI BENI E SERVIZI FINANZIATI DALLA P.A. 6

6 AREA SENSIBILE E REATI PRESUPPOSTI 7

6 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO 9

1 OBIETTIVI

La presente procedura definisce le operazioni che ciascuna Funzione Aziendale deve porre in essere nelle attività inerenti la richiesta di autorizzazioni, finanziamenti, licenze o altri provvedimenti amministrativi o l'esecuzione di adempimenti verso la Pubblica Amministrazione, finalizzate allo svolgimento dell'attività caratteristica della Società, nel rispetto della normativa vigente e dei principi di trasparenza, oggettività e veridicità delle informazioni

IN PARTICOLARE:

- sono previste procedure per la gestione delle richieste di autorizzazioni, finanziamenti, licenze o altri provvedimenti amministrativi o l'esecuzione di adempimenti verso la Pubblica Amministrazione;
- si prevede che i poteri autorizzativi e/o negoziali esercitati dai soggetti nei confronti della Pubblica Amministrazione devono essere individuati in base allo specifico ruolo attribuito a ciascuna Funzione dall'organigramma aziendale, ovvero dalla Funzione Aziendale all'uopo preposta attraverso apposita delega intera e/o autorizzazione;
- è prevista una segregazione di funzioni tra chi predispone la documentazione necessaria per la richiesta di un'autorizzazione/licenza, chi la controlla e chi sottoscrive la richiesta;
- è necessario assicurare che le attività siano svolte in modo da garantire la veridicità, la completezza, la congruità e la tempestività nella predisposizione dei dati e delle informazioni a supporto dell'istanza di autorizzazione o forniti in esecuzione degli adempimenti prevedendo specifici controlli in contraddittorio;
- è prevista la tracciabilità del processo sia a livello di sistema informatico sia in termini documentali e la conservazione della documentazione prodotta da parte della Funzione Aziendale all'uopo preposta;
- è previsto il monitoraggio periodico volto a verificare il persistere delle condizioni in base alle quali è stata ottenuta l'autorizzazione e la tempestiva comunicazione alla Pubblica Amministrazione di eventuali modifiche/aggiornamenti;
- è prevista la verifica attraverso appositi scadenzari delle autorizzazioni/licenze ottenute al fine di richiedere il rinnovo delle stesse nel rispetto dei termini di legge.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA

RSGQ	Responsabile Sistema di Gestione Qualità
RAM	Responsabile Amministrazione - Risorse Umane
RTEC	Responsabile Tecnico
RCOM/APVG	Responsabile Commerciale – Approvvigionamento
RFAM	Responsabile Facility Management
RPROG	Responsabile Progettazione
RSCM	Responsabile singola commessa
RATTR	Responsabile Attrezzature e Mezzi
PROG	Programmatori
RGAD	Responsabile Gestione Archivi e Documenti

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di IDRAGEST S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l..
- Codice penale, con richiamo ai reati rilevanti nei rapporti con la P.A.: artt. 318, 319, 319-bis, 319-quater, 321, 322, 322-bis, 346-bis, 640, 640-bis c.p.
- D.lgs. 36/2023 per i rapporti con stazioni appaltanti/enti concedenti e per il rischio di false dichiarazioni, cause di esclusione e illecito professionale;
- L. 190/2012, limitatamente alla centralità dei procedimenti di autorizzazione/concessione, scelta del contraente ed erogazioni pubbliche come aree tipiche di rischio corruttivo;
- D.lgs. 24/2023 sulla disciplina whistleblowing, da coordinare con il MOG 231 e con il sistema disciplinare.

4 CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutte le Funzioni Aziendali che, direttamente o indirettamente, intervengono nella:

1. richiesta, gestione, rinnovo, modifica o rendicontazione di finanziamenti pubblici, contributi, sovvenzioni, agevolazioni, licenze, permessi, autorizzazioni, concessioni, nulla osta e atti equipollenti;
2. predisposizione e trasmissione di dichiarazioni, attestazioni, istanze, relazioni tecniche, elaborati progettuali, documentazione amministrativa e contabile destinata alla Pubblica Amministrazione;
3. gestione di adempimenti richiesti da amministrazioni, enti pubblici, autorità di vigilanza o organismi di controllo;
4. esecuzione di attività svolte dalla Società nell'interesse proprio o, ove compatibile con il Modello 231, nell'interesse dei clienti, quando l'attività implichi interlocuzioni documentali o procedimentali con soggetti pubblici.

Tenuto conto del core business di IDRAGEST S.r.l. descritto nella procedura, la presente disciplina si applica anche alle attività tecniche, progettuali, topografiche, informatiche e ingegneristiche che comportino richieste, comunicazioni o adempimenti verso la Pubblica Amministrazione.

Il responsabile della procedura è l'Organo Amministrativo, che assicura l'adozione, l'aggiornamento, il controllo sull'attuazione e la coerenza della procedura con il Modello 231 e con il sistema delle deleghe interne.

5. INDICAZIONI COMPORTAMENTALI

Tutte le Funzioni Aziendali coinvolte, a qualsiasi titolo, nella predisposizione, sottoscrizione, invio, gestione, monitoraggio o rendicontazione di pratiche verso la Pubblica Amministrazione devono:

1. garantire la veridicità, completezza, correttezza, congruità e aggiornamento delle dichiarazioni, attestazioni, comunicazioni e della documentazione trasmessa alla Pubblica Amministrazione;
2. assicurare che ogni dato, informazione o allegato inviato anche mediante strumenti informatici o telematici sia riconducibile con certezza al soggetto che lo ha formato, verificato e autorizzato;
3. destinare eventuali somme ricevute a titolo di contributo, sovvenzione o finanziamento esclusivamente alle finalità per le quali sono state erogate;

4. predisporre e conservare idonea documentazione di supporto alla spesa, al pagamento e alla rendicontazione;
5. garantire la piena tracciabilità dell'intero iter documentale e decisionale;
6. segnalare tempestivamente all'Organo Amministrativo e all'Organismo di Vigilanza ogni anomalia, richiesta indebita, pressione, tentativo di condizionamento o irregolarità riscontrata.

È fatto divieto ai Destinatari di:

1. offrire, promettere, dare o autorizzare, direttamente o indirettamente, denaro o altra utilità a pubblici ufficiali o incaricati di pubblico servizio per l'esercizio delle loro funzioni o dei loro poteri, ovvero per influenzarne indebitamente l'operato;
2. porre in essere condotte che possano integrare istigazione alla corruzione, anche nel caso in cui la promessa o offerta non sia accettata;
3. attestare falsamente al pubblico ufficiale, in un atto pubblico, fatti destinati a provare la verità;
4. presentare documentazione mendace, incompleta o fuorviante, ovvero omettere circostanze rilevanti ai fini del procedimento amministrativo;
5. avvalersi di soggetti che, sfruttando o vantando relazioni con pubblici ufficiali o incaricati di pubblico servizio, richiedano o ricevano utilità quale prezzo di una mediazione illecita; resta fermo il divieto di ricorrere a intermediazioni illecite nei rapporti con la Pubblica Amministrazione, in coerenza con l'attuale disciplina dell'art. 346-bis c.p. come modificata nel 2024 e scrutinata dalla Corte costituzionale;
6. offrire omaggi, utilità, trattamenti di favore o regalie non consentiti dalle regole interne e comunque idonei a compromettere l'imparzialità del funzionario pubblico;
7. sollecitare o ottenere informazioni riservate fuori dai casi consentiti dalla legge;
8. conferire incarichi o consulenze in presenza di conflitti di interesse, anche potenziali, non previamente dichiarati e gestiti;
9. occultare fatti veri o esporre fatti non corrispondenti al vero nelle comunicazioni, segnalazioni o risposte indirizzate alla Pubblica Amministrazione.

Nella predisposizione delle comunicazioni, segnalazioni e risposte verso la Pubblica Amministrazione è obbligatorio adottare i principi di completezza, integrità, oggettività, verificabilità e trasparenza.

5 L'UTILIZZO DI RISORSE FINANZIARIE LEGATO AGLI INVESTIMENTI E/O ACQUISTO DI BENI E SERVIZI FINANZIATI DALLA P.A.

Per l'utilizzo di risorse finanziarie collegate agli investimenti e/o all'acquisto di beni e servizi finanziati dalla P.A., è necessario rispettare, i criteri qui di seguito indicati:

1. l'esborso deve essere autorizzato dal PRES, con apposizione di una precisa causale e deve essere registrato in conformità ai principi di correttezza professionale e contabile;
2. il pagamento deve essere effettuato esclusivamente sul conto corrente indicato nel contratto;
3. il pagamento deve corrispondere a quanto indicato nel contratto;
4. vige il divieto di eseguire pagamenti su conti cifrati e/o pagamenti in favore di un soggetto diverso dalla controparte contrattuale;
5. il pagamento non può essere effettuato in un Paese terzo rispetto a quello delle parti contraenti o di esecuzione del contratto;
6. il pagamento effettuato su conti correnti di banche appartenenti od operanti in Paesi elencati tra i c.d. "paradisi fiscali", o in favore di società "*off shore*", deve essere eseguito nel rispetto di leggi vigenti in materia;
7. garantire la tracciabilità del pagamento, ovvero stampare e/o archiviare digitalmente la contabile del bonifico eseguito;
8. la documentazione relativa ai pagamenti deve essere inserita nel fascicolo di riferimento;
9. le relative registrazioni contabili – o le schede contabili che dovranno essere richieste al professionista incaricato della tenuta della contabilità se esterna alla Società - devono essere controllate, a campione, dal PRES ed essere conformi alla tipologia di acquisto;

In ultimo, occorre osservare come l'art. 6-ter della Legge 137/2023 ha introdotto all'interno dell'art. 25-octies.1, concernente i delitti in materia di strumenti di pagamento diversi dai contanti, la fattispecie di trasferimento fraudolento di valori (art. 512-bis c.p.), in relazione al quale è prevista per gli Enti la sanzione pecuniaria da 250 a 600 quote; alle citate sanzioni si aggiungono le sanzioni interdittive di cui ex art. 9, co. 2 del D.Lgs. n. 231/2001.

Pertanto, la suddetta Legge 137/2023 ha inserito tra i reati-presupposto il delitto di trasferimento fraudolento di valori di cui all'art. 512-bis c.p..

Dunque, il delitto di "Trasferimento fraudolento di valori" si aggiunge all'indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.); alla detenzione e diffusione di dispositivi diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.) e alla frode informatica (art. 640-ter c.p.) aggravata dal trasferimento di denaro.

Nei casi di condanna per i delitti menzionati si applicano all'ente le sanzioni interdittive dell'interdizione dall'esercizio dell'attività; della sospensione o della revoca delle autorizzazioni, licenze o concessioni; del divieto di contrattare con la pubblica amministrazione, dell'esclusione da agevolazioni, finanziamenti, contributi o sussidi; del divieto di pubblicizzare beni o servizi (art. 9 comma 2, d.lg. n. 231/2001).

6 AREA SENSIBILE E REATI PRESUPPOSTI

La presente procedura presidia un'area sensibile del Modello 231 connessa ai rapporti tra la Società e la Pubblica Amministrazione, con particolare riguardo alla gestione di richieste di finanziamenti, autorizzazioni, permessi, licenze e altri provvedimenti amministrativi.

Le condotte da prevenire comprendono, in particolare:

A) CORRUZIONE PER L'ESERCIZIO DELLA FUNZIONE – ART. 318 C.P.

"*Il pubblico ufficiale, che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità, o ne accetta la promessa, è punito con la reclusione da tre a otto anni*".

Il reato si configura allorquando un Pubblico Ufficiale o un Incaricato di Pubblico Servizio riceva per sé o per altri, denaro o altra utilità o ne accetta la promessa, per l'esercizio delle sue funzioni o dei suoi poteri.

Ai fini della ricorrenza di tale reato è necessario che la promessa di denaro o di altra utilità siano accettate dal pubblico ufficiale, poiché, in caso contrario, deve ritenersi integrata la diversa fattispecie di istigazione alla corruzione, prevista dall'art. 322 c.p.

A titolo di esempio il reato potrebbe configurarsi laddove un pubblico ufficiale e un referente della società, anche consulente si accordino in modo che a fronte di un pagamento in denaro, il pubblico ufficiale adotti un provvedimento del suo ufficio (es. rilascio di una licenza nei termini) nei confronti della Società.

La procedura mira a prevenire qualunque promessa, offerta o utilità indebita destinata a pubblici ufficiali o incaricati di pubblico servizio.

B) CORRUZIONE DEL PRIVATO NEI CONFRONTI DEL PUBBLICO AGENTE – ART. 321 C.P.

"*Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'articolo 319-ter, e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi da o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilita'*."

La procedura vieta dunque non solo la ricezione, ma anche la dazione o promessa di utilità da parte di esponenti della Società.

C) ISTIGAZIONE ALLA CORRUZIONE – ART. 322 C.P.

La fattispecie rileva anche quando la promessa o dazione non sia accettata; la fonte disponibile conferma, inoltre, la rilevanza della sollecitazione proveniente dal pubblico agente per finalità corruttive.

D) FALSITÀ IDEOLOGICA COMMESSA DAL PRIVATO IN ATTO PUBBLICO – ART. 483 C.P.

"*Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni.*

A titolo esemplificativo tale fattispecie potrebbe trovare applicazione nel caso in cui un dipendente della Società, dichiari, per via telematica, che la Società ha adempiuto a determinati obblighi di legge al fine di ottenere una licenza/autorizzazione. La fattispecie è particolarmente rilevante con riguardo a istanze, dichiarazioni, autocertificazioni, relazioni tecniche e documentazione inviata anche per via telematica alla Pubblica Amministrazione.

E) TRAFFICO DI INFLUENZE ILLECITE – ART. 346-BIS C.P.

La procedura presidia altresì il rischio di ricorso a soggetti che si propongano quali mediatori indebiti verso pubblici ufficiali. La disciplina dell'art. 346-bis c.p. è stata modificata nel 2024; la Corte costituzionale ha chiarito il quadro evolutivo della fattispecie e la distinzione tra forme legittime e illegittime di intermediazione.

F) TRUFFA AI DANNI DELLO STATO O DI ALTRO ENTE PUBBLICO ART. 640 COMM1 C.P.

"Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. (…) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo

immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità [649];2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5".

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato, oppure ad altro Ente Pubblico.

A mero titolo di esempio, il reato potrebbe realizzarsi qualora allo scopo di ottenere una licenza od una autorizzazione amministrativa, vengano indotti in errore i pubblici ufficiali incaricati mediante facendo apparire agli stessi una falsa rappresentazione della realtà, ottenendo così indebitamente il provvedimento.

Con l'ultima modifica apportata dalla Legge n.90 del 28 Giugno 2024 è stato introdotto il comma 2-ter) con cui si è estesa la punibilità anche quando il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal secondo comma, a eccezione di quella di cui al numero 2-ter).

Pertanto, è espressamente vietato nella predisposizione di documenti o dati per la partecipazione a procedure di gara fornire alla Pubblica Amministrazione informazioni non veritiere, anche attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione.

La procedura resta finalizzata a impedire condotte ingannevoli, artifici, raggiri, false rappresentazioni della realtà o omissioni rilevanti idonee a indurre in errore la Pubblica Amministrazione ai fini del rilascio di provvedimenti o dell'attribuzione di utilità.

7 COMUNICAZIONI ALL'ORGANISMO DI VIGILANZA E POTERI DI CONTROLLO

Tutti le Funzioni Aziendali coinvolte nelle attività oggetto della presente procedura informano tempestivamente l'Organismo di Vigilanza di:

- ✓ situazioni anomale e/o in contrasto con quanto disposto nel Modello;
- ✓ di qualsivoglia comportamento non conforme alle disposizioni previste dal Codice Etico.

In particolare, deve essere comunicato, da parte dell'Organo Amministrativo all'Organismo di Vigilanza l'elenco riassuntivo relativo ai finanziamenti pubblici richiesti, con cadenza semestrale.

I Destinatari devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo predisposto su apposita piattaforma informatica - tutta la documentazione necessaria.

I Destinatari devono, altresì, garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto nell'apposita piattaforma di condivisione - tutta la documentazione necessaria.

Tutta la documentazione relativa alla tenuta della contabilità, alla predisposizione del bilancio e della documentazione connessa, è archiviata a cura del RAM/RRU, o della funzione eventualmente incaricata dal PRES, ed è tenuta a disposizione dell'OdV.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di corporate governance per la prevenzione dei reati di false comunicazioni sociali;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

8 CLAUSOLA FINALE SANZIONATORIA

La violazione della presente procedura, dei relativi obblighi di comportamento, controllo, tracciabilità e comunicazione, costituisce violazione del Modello di Organizzazione, Gestione e Controllo adottato dalla Società e integra illecito disciplinare, con applicazione delle misure previste dalla normativa vigente, dal Modello 231 e dal contratto collettivo applicato.

Resta fermo che, nei casi previsti dal D.lgs. 231/2001, la Società può essere esposta anche alle sanzioni interdittive di cui all'art. 9, comma 2, incluso il divieto di contrattare con la Pubblica Amministrazione e l'esclusione da agevolazioni, finanziamenti, contributi o sussidi.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE

PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO 4

2 ACRONIMI AZIENDALI 9

3 RIFERIMENTI NORMATIVI 9

4 CAMPO DI APPLICAZIONE RESPONSABILE DELLA PROCEDURA 10

5 PRINCIPI GENERALI DI COMPORTAMENTO 10

5.1 OBBLIGHI GENERALI DI CONDOTTA.....11

5.2 GESTIONE DELLE AUTORIZZAZIONI AMBIENTALI 12

5.3 SELEZIONE E QUALIFICA DEI FORNITORI AMBIENTALI.....13

5.4 TRACCIABILITÀ DEI RIFIUTI E SISTEMI DIGITALI.....13

6. L. 147/2025 reati ambientali e responsabilità amministrativa degli enti 15

7 PRESIDI DI CONTROLLO E IMPEGNI PER LA SALVAGUARDIA AMBIENTALE 16

7.1 ASSEGNAZIONE DI RESPONSABILITÀ GESTIONALI.....16

7.2 RICERCA TECNOLOGICA E MIGLIORAMENTO CONTINUO 17

7.3 SISTEMA DI GESTIONE AMBIENTALE (ISO 14001:2015).....17

7.4 MONITORAGGIO DELLE PERFORMANCE AMBIENTALI.....18

7.5 COINVOLGIMENTO DI DIPENDENTI E FORNITORI 19

8 Legge n. 137/2023 – LA TUTELA PENALE DELL'AMBIENTE 19

9 Decreto Legge n.116 dell'8 agosto 2025 convertito in legge n. 147 del 3 ottobre 2025 20

9.1 Abbandono di rifiuti non pericolosi in casi particolari (Art. 255-bis D. Lgs. n. 152/2006 (Introdotto da Decreto Legge n. 116 dell'8 agosto 2025 e convertito da Legge n.147 del 3 ottobre 2025) 21

9.2 Abbandono di rifiuti pericolosi (Art. 255-ter D. Lgs. n. 152/2006 (Introdotto da Decreto Legge n. 116 dell'8 agosto 2025 e convertito da Legge n.147 del 3 ottobre 2025) 22

9.3 Attività di gestione di rifiuti non autorizzata (Art.256 D. Lgs. n. 152/2006 modificato da D.Lgs.n.46/2014, da Decreto Legge n. 116 dell'8 agosto 2025 e modificato da Legge n. 147 del 3 ottobre 2025) 22

9.4 Combustione illecita di rifiuti (Art. 256-bis D. Lgs. n. 152/2006 (Introdotto e modificato da Decreto Legge n. 116 dell'8 agosto 2025 e convertito da Legge n.147 del 3 ottobre 2025) 24

9.5 Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (Art. 258 D. Lgs. n. 152/2006 modificato da Art.4 del D.Lgs.n.116 del 3 settembre 2020, da Decreto Legge n. 116 dell'8 agosto 2025 e da Legge n.147 del 3 ottobre 2025) 25

9.6 Spedizione illegale di rifiuti (Art. 259 D. Lgs. n. 152/2006 modificati rubrica e testo da Decreto Legge n. 116 dell'8 agosto 2025 e convertito con Legge n. 147 del 3 ottobre 2025) 29

9.7 Aggravante dell'attività di impresa (Art. 259-bis D. Lgs. n. 152/2006 introdotto da Decreto Legge n. 116 dell'8 agosto 2025 e convertito dalla Legge n.147 del 3 ottobre 2025) 29

9.8 Delitti colposi in materia di rifiuti (Art. 259-ter D. Lgs. n. 152/2006 introdotto da Decreto Legge n. 116 dell'8 agosto 2025 e convertito dalla Legge n.147 del 3 ottobre 2025) 30

10 CERTIFICAZIONE ISO 14001:2015 30

11 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO 30

1 OBIETTIVI E FUNZIONI DEL MODELLO

Con il D. Lgs. 7 luglio 2011 n. 121, entrato in vigore il 16 agosto 2011, sono stati introdotti nel novero dei reati presupposto della responsabilità dell'Ente ex D.Lgs. 231/01 i reati c.d. "ambientali".

Si tratta dei reati in violazione degli artt. 727-bis e 733-bis c.p., alcuni dei reati di cui al D.Lgs. 152/06 (Testo Unico Ambientale), nonché alcuni reati di cui alle leggi 150/92, 549/97 e D.Lgs. 202/07.

Successivamente, con la Legge 22 maggio 2015 n. 68, il novero dei reati è stato integrato con le fattispecie di cui agli artt. 452-bis, 452-quater, 452-quinquies, 452-sexies e 452-octies c.p. (c.d. "ecoreati").

Infine, il D. Lgs 1° marzo 2018, n. 21, ha abrogato l'art. 260 del D. Lgs. 156/06 introducendo l'art. 452-quaterdecies c.p.

IN PARTICOLARE, L'ART. ART. 25-UNDECIES, D.LGS. 231/01, DISCIPLINA I SEGUENTI REATI:

- inquinamento ambientale (art. 452-bis c.p.);
- disastro ambientale (art. 452-quater c.p.);
- delitti colposi contro l'ambiente (art. 452-quinquies c.p.);
- traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.);
- circostanze aggravanti (art. 452-octies c.p.);
- uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.);
- distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.);
- scarichi di acque reflue industriali senza autorizzazione (art. 137, commi 2, 3 e 5, d. lgs. n.152/2006);
- scarichi nel sottosuolo e nelle acque sotterranee (art. 137, comma 11, d. lgs. n. 152/2006);
- traffico illecito di rifiuti (d. lgs n.152/2006, art. 259);
- scarichi nelle acque del mare di sostanze o materiali vietati da parte di navi o aero-mobili (art. 137, comma 13, D.lgs. 152/06);
- attività di gestione di rifiuti non autorizzata (art. 256, commi 1, 3, 5, 6, primo periodo, D.lgs. 152/06);
- bonifica dei siti (art. 257, commi 1 e 2, D.Lgs. 152/06);
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, comma 4, secondo periodo, D.Lgs. 152/06);
- traffico illecito di rifiuti (art. 259, comma 1, D.Lgs. 152/06);
- attività organizzate per il traffico illecito di rifiuti (art. 260, commi 1 e 2, D.Lgs. 152/06);

− sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis, commi 6 e 7, secondo e terzo periodo, D.Lgs. 152/06);
− sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis, comma 8, D.Lgs. 152/06);
− superamento dei valori limite di emissione e dei valori limite di qualità dell'aria (art. 279, comma 5, D.Lgs. 152/06);
− commercio internazionale di specie animali e vegetali in via di estinzione (art. 1, commi 1 e 2, Legge 150/1992);
− commercio internazionale di specie animali e vegetali in via di estinzione (art. 2, commi 1 e 2, Legge 150/1992);
− commercio internazionale di specie animali e vegetali in via di estinzione (art. 3-bis, comma 1, Legge 150/1992);
− commercio internazionale di specie animali e vegetali in via di estinzione (art. 6, comma 4, Legge 150/1992);
− cessazione e riduzione dell'impiego delle sostanze lesive dell'ozono (art. 3, comma 6, Legge 549/1993);
− inquinamento doloso (art. 8, commi 1 e 2, D.Lgs. 202/2007);
− inquinamento colposo (art. 9, commi 1 e 2, D.Lgs. 202/2007).

Pertanto, sono state analizzate, le fattispecie di illeciti presupposto per le quali si applica il Decreto e con riferimento a ciascuna categoria dei medesimi sono state identificate in IDRAGEST le aree aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati.

Per ciascuna di tali aree si sono quindi individuate le singole attività sensibili e qualificati i principi di controllo e di comportamento cui devono attenersi tutti coloro che vi operano.

Dunque, in considerazione dell'analisi dei rischi effettuata, IDRAGEST adotta tutte le misure necessarie a prevenire i reati di cui D.Lgs. 231/2001 all'art. 25-undecies, ed in particolare:

• **SANZIONI PENALI IN MATERIA DI SCARICHI DI ACQUE REFLUE (ART. 137 D.LGS. 152/2006)**

Tale ipotesi di reato si configura nel caso in cui lo svolgimento delle attività aziendali comporti lo scarico di acque reflue aziendali contenenti sostanze pericolose in concentrazioni difformi dalle prescrizioni legislative o le attività stesse siano condotte in difformità rispetto alle previsioni autorizzative.

• **REATI IN MATERIA DI GESTIONE NON AUTORIZZATA DI RIFIUTI (ART. 256 D.LGS. 152/2006)**

Tale ipotesi di reato si configura nel caso in cui sia svolta l'attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti – sia pericolosi che non pericolosi – in mancanza

della prescritta autorizzazione; sia effettuato illegittimamente il deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi; sia realizzata o gestita una discarica non autorizzata, anche eventualmente destinata ai rifiuti pericolosi; siano svolte attività non consentite di miscelazione di rifiuti.

• VIOLAZIONE DEGLI OBBLIGHI DI COMUNICAZIONE, DI TENUTA DEI REGISTRI OBBLIGATORI E DEI FORMULARI (ART. 258 D.LGS. 152/2006)

Tale ipotesi di reato punisce chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico- fisiche dei rifiuti, nonché chi fa uso di un certificato falso durante il trasporto.

• TRAFFICO E ABBANDONO DI MATERIALE AD ALTA RADIOATTIVITÀ (ART. 452-SEXIES C.P. INTRODOTTO DA L. N 68 DEL 22 MAGGIO 2015 E MODIFICATO DA DECRETO LEGGE N.116 DELL'8 AGOSTO 2025 E CONVERTITO DA LEGGE N.147 DEL 3 OTTOBRE 2025)

Questo reato introdotto dall'articolo 1, comma 1 della legge n.68 del 22 maggio 2015 si verifica quando chiunque abusivamente cede, acquista, riceve, trasporta, importa, esporta, procura ad altri, detiene, trasferisce, abbandona o si disfa illegittimamente di materiale ad alta radioattività .

Il reato è punito con la reclusione da due a sei anni e con la multa da 10.000 a euro 50.000. Con il DL n. 116 dell'8 agosto 2025, confermato dalla Legge n.147 del 3 ottobre 2025, la pena è aumentata fino alla metà se dal fatto deriva il pericolo di compromissione o deterioramento del suolo, delle acque, dell'aria, di un ecosistema, dell'agricoltura, della flora e della fauna oppure il fatto è commesso in siti contaminati o potenzialmente contaminati o comunque sulle strade di accesso ai predetti siti e relative pertinenze

• IMPEDIMENTO DEL CONTROLLO (ART. 452-SEPTIES C.P. INTRODOTTO DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E CONVERTITO DA LEGGE N.147 DEL 3 OTTOBRE 2025)

Il reato contemplato dall'Art. 452- septies si verifica quando si nega l'accesso, predisponendo ostacoli o mutando artificiosamente lo stato dei luoghi, per impedire, intralciare o eludere l'attività di vigilanza e controllo ambientali e di sicurezza e igiene del lavoro, compromettendo così gli esiti del controllo. Il DL n. 116 dell'8 agosto 2025, confermato dalla Legge n.147/2025 ha previsto per la violazione dell'articolo 452-septies la sanzione pecuniaria fino a duecentocinquanta quote e la reclusione da sei mesi a tre anni.

• OMESSA BONIFICA (ART. 452-TERDECIES C.P. INTRODOTTO DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E CONVERTITO DA LEGGE N.147 DEL 3 OTTOBRE 2025)

Il reato introdotto dal Decreto Legge n. 116 e confermato poi dalla Legge 147/2025, si verifica quando, obbligati per legge, per ordine del giudice ovvero di un'autorità pubblica, non si provvede alla bonifica, al ripristino o al recupero dello stato dei luoghi

Tale reato viene punito con la pena della reclusione da uno a quattro anni e con la multa da euro 20.000 a euro 80.000

• ATTIVITÀ ORGANIZZATE PER IL TRAFFICO ILLECITO DI RIFIUTI (ART. 452-QUATERDECIES C.P. MODIFICATO DALLA LEGGE 147/2025)

La norma prevede una specifica aggravante di pena per i reati di associazione a delinquere aventi lo scopo di commettere taluno dei delitti ambientali previsti dal codice penale. Se si tratta di reato di "Associazione mafiosa", costituisce aggravante il fatto stesso dell'acquisizione della gestione o del controllo di attività economiche, di concessioni, autorizzazioni, appalti o di servizi pubblici in materia ambientale.

Tale ipotesi di reato punisce, quindi, chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa o comunque gestisce abusivamente ingenti quantitativi di rifiuti.

Il reato si realizza quando, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, si cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti

La pena della reclusione prevista per tale reato è da uno a sei anni che salgono da tre a otto anni se trattasi di rifiuti radioattivi.

L'art. 452 quaterdecies c.p. dispone testualmente che "*Chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti è punito con la reclusione da uno a sei anni Se si tratta di rifiuti ad alta radioattività si applica la pena della reclusione da tre a otto anni.*

Le pene previste dai commi che precedono sono aumentate fino alla metà, quando:

a) dal fatto deriva pericolo per la vita o per la incolumità delle persone ovvero pericolo di compromissione o deterioramento:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna

b) il fatto è commesso in siti contaminati o potenzialmente contaminati ai sensi dell'articolo 240 o comunque sulle strade di accesso ai predetti siti e relative pertinenze.

Alla condanna conseguono le pene accessorie di cui agli articoli 28, 30, 32-bis e 32-ter, con la limitazione di cui all'articolo 33.

Il giudice, con la sentenza di condanna o con quella emessa ai sensi dell'articolo 444 del codice di procedura penale, ordina il ripristino dello stato dell'ambiente e può subordinare la concessione della sospensione condizionale della pena all'eliminazione del danno o del pericolo per l'ambiente.

È sempre ordinata la confisca delle cose che servirono a commettere il reato o che costituiscono il prodotto o il profitto del reato, salvo che appartengano a persone estranee al reato.

Quando essa non sia possibile, il giudice individua beni di valore equivalente di cui il condannato abbia anche indirettamente o per interposta persona la disponibilità e ne ordina la confisca".

•FALSITÀ NELLA TRACCIABILITÀ DEI RIFIUTI MEDIANTE IL SISTRI (ART. 260 BIS, COMMA 6 – COMMA 7, 2° E 3° PERIODO - COMMA 8, C. A.)85

Al sistema informatico di controllo della tracciabilità dei rifiuti, denominato SISTRI, partecipano obbligatoriamente o su base volontaria, secondo i criteri di cui all'art. 188 ter C.A., i produttori di rifiuti e gli altri soggetti che intervengono nella loro gestione (commercianti, intermediari, consorzi di recupero o riciclaggio, soggetti che compiono operazioni di recupero o di smaltimento, trasportatori). In tale contesto sono puniti i delitti consistenti nel fornire false indicazioni sulla natura e sulle caratteristiche di rifiuti al fine della predisposizione di un certificato di analisi dei rifiuti da inserire in SISTRI, nell'inserire nel sistema un certificato falso o nell'utilizzare tale certificato per il trasporto dei rifiuti.

È altresì punito il trasportatore che accompagna il trasporto con una copia cartacea fraudolentemente alterata della scheda SISTRI compilata per la movimentazione dei rifiuti.

NELLO SPECIFICO, LA PRESENTE PROCEDURA HA LO SCOPO DI:

a) indicare le procedure che i collaboratori di IDRAGEST sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, e ai responsabili delle funzioni aziendali che cooperano con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

All'uopo, IDRAGEST ha previsto un sistema di deleghe per la compilazione del Formulario di Identificazione dei Rifiuti (FIR), ovvero il documento che deve accompagnare il rifiuto durante le fasi di trasporto al fine di garantirne la tracciabilità, poiché il ritiro da parte della Ditta incaricata, assicurando una puntuale formazione in ordine alle "Modalità di compilazione del modello di cui all'art.5 del D.M. n.59 del 2023" riguardante le "Istruzioni per la compilazione del formulario di identificazione del rifiuto

(FIR)" emesso dal Ministero dell'Ambiente e della Sicurezza energetica che ha pubblicato il Decreto Direttoriale n.251/2023 con il quale ha definito le modalità operative previste per il registro cronologico di carico e scarico rifiuti e il formulario di identificazione del rifiuto (FIR) come previsto dall'art. 21 del Decreto RENTRI.

La presente Parte Speciale presidia i rischi ambientali connessi alle attività effettivamente svolte dalla Società, con particolare riguardo a sopralluoghi tecnici, rilievi di campo, utilizzo di strumentazione, gestione di rifiuti tecnici, rapporti con fornitori autorizzati, eventuali scarichi o reflui di sede e gestione di anomalie riscontrate presso infrastrutture del cliente. Il presidio considera le fattispecie di reato ambientale rilevanti ai sensi dell'art. 25-undecies del D.Lgs. 231/2001, incluse le ipotesi di inquinamento ambientale, disastro ambientale, delitti colposi contro l'ambiente, traffico e abbandono di materiale ad alta radioattività, impedimento del controllo, omessa bonifica e attività organizzate per il traffico illecito di rifiuti, nonché le fattispecie richiamate dal D.Lgs. 152/2006.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC	Responsabile Tecnico
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RFAM	Responsabile Facility Management
RPROG	Responsabile Progettazione
RATTR	Responsabile Attrezzature e Mezzi

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);

- Codice Etico di IDRAGEST S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l.

4 CAMPO DI APPLICAZIONE RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutti coloro i quali agiscono in nome e per conto della Società e la cui attività possa comportare la commissione dei reati di cui all'art. 25-undecies.

Orbene, dall'analisi della mappatura dei rischi, è emerso come i principali processi sensibili ritenuti più specificatamente a rischio, in ambito IDRAGEST, sono i seguenti:

- Gestione e caratterizzazione dei rifiuti
- Gestione delle acque reflue.

Le disposizioni della presente Parte Speciale hanno per Destinatari tutti i soggetti coinvolti nei processi sopra identificati, affinché gli stessi adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi dei delitti ivi considerati.

NELLO SPECIFICO LA PRESENTE PARTE SPECIALE HA LO SCOPO DI:

a) indicare i principi che i destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, ed ai Responsabili delle funzioni aziendali che con lo stesso cooperano, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

Il principale responsabile della presente procedura è l'Organo Amministrativo.

5 PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di carattere generale si applicano agli organi sociali, ai dirigenti ed a tutti i dipendenti di IDRAGEST, inclusi i soggetti assunti con contratti di somministrazione per l'espletamento di specifiche commesse, nonché ai collaboratori esterni, ai consulenti e a tutti i terzi che agiscano in nome o per conto della Società nell'ambito delle attività disciplinate dalla presente Procedura.

Ai suddetti soggetti è fatto divieto di porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale — con particolare riferimento ai reati ambientali di cui all'art. 25-undecies D.Lgs. 231/2001, ai reati di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare di cui all'art. 25-duodecies D.Lgs. 231/2001 e al reato di intermediazione illecita e sfruttamento del lavoro di cui all'art. 603-bis c.p. — nonché le violazioni ai

principi comportamentali e ai divieti previsti nella presente Parte Speciale e nel Codice Etico di IDRAGEST.

5.1 OBBLIGHI GENERALI DI CONDOTTA

Conformemente a quanto previsto nel Codice Etico, nelle procedure e nelle norme aziendali applicabili, i soggetti sopra individuati devono:

a) Tenere un comportamento corretto, trasparente e diligente, nel rispetto delle norme di legge, dei limiti e delle prescrizioni contenute nelle autorizzazioni ambientali ricevute, nonché delle procedure aziendali interne, in tutte le attività finalizzate a:

alla gestione degli scarichi di acque reflue industriali e civili;

alla gestione, manutenzione e sanitizzazione degli ambienti di lavoro di proprietà o in uso a IDRAGEST;

alla raccolta, al deposito temporaneo e al conferimento dei rifiuti prodotti nell'ambito delle attività aziendali e delle commesse gestite.

b) Nella selezione dei fornitori cui è demandata la raccolta, il trasporto e lo smaltimento dei rifiuti, porre particolare attenzione alla verifica dell'affidabilità tecnico-professionale degli stessi, accertandosi del possesso dei requisiti di legge richiesti (iscrizione all'Albo Nazionale Gestori Ambientali, autorizzazioni all'esercizio, regolarità contributiva e fiscale).

c) Rispettare la regolamentazione e gli obblighi legislativi vigenti in materia di tracciabilità dei rifiuti, inclusi i nuovi obblighi derivanti dall'adesione e dall'operatività del Registro Elettronico Nazionale per la Tracciabilità dei Rifiuti (RENTRI), di cui al D.Lgs. 3 settembre 2020, n. 116 e relativo decreto attuativo.

d) Segnalare tempestivamente al proprio responsabile gerarchico e, ove necessario, all'Organismo di Vigilanza (OdV), qualsiasi situazione anomala, rischio potenziale o evento contaminante riscontrato nell'esercizio delle proprie attività.

e) Garantire la massima cooperazione in sede di ispezioni, audit e verifiche da parte delle Autorità competenti e degli Organismi di controllo, fornendo informazioni veritiere, complete e documentate.

Divieti Generali

AI SOGGETTI SOPRA INDIVIDUATI È VIETATO, A MERO TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO:

f) Porre in essere o dare causa a violazioni dei protocolli specifici di comportamento e di controllo contenuti nella presente Parte Speciale, nonché della regolamentazione aziendale in materia di gestione ambientale;

g) In sede di realizzazione di prescrizioni imposte dalla legge o da Enti pubblici in materia ambientale, perseguire l'obiettivo di risparmio sui costi o sui tempi a scapito della tutela dell'ambiente e della salute pubblica;

h) Presentare, predisporre o utilizzare, anche in concorso con terzi, certificati falsi di analisi dei rifiuti ovvero documentazione tecnica non veritiera relativa alla caratterizzazione, classificazione o smaltimento dei rifiuti stessi;

i) Superare i limiti consentiti, in termini di tempo e di quantità, per il deposito temporaneo di rifiuti, ivi inclusi i rifiuti sanitari, i rifiuti pericolosi e i rifiuti speciali;

j) In sede di ispezioni e verifiche da parte delle Autorità competenti, adottare comportamenti finalizzati a influenzare indebitamente, nell'interesse della Società o di terzi, il giudizio o il parere degli Organismi di controllo;

k) Ricorrere, anche indirettamente tramite la catena dei subappalti e della filiera dei servizi, all'impiego di lavoratori privi di regolare titolo di soggiorno o di soggetti vittime di intermediazione illecita e sfruttamento lavorativo.

5.2 GESTIONE DELLE AUTORIZZAZIONI AMBIENTALI

Le Funzioni Aziendali competenti, a qualsiasi titolo coinvolte nella gestione dei processi ambientali, sono tenute ad assicurare che IDRAGEST operi in conformità ai titoli autorizzativi vigenti, garantendo il tempestivo aggiornamento degli stessi al mutare delle condizioni operative o normative.

IN PARTICOLARE, LE FUNZIONI AZIENDALI INTERESSATE DEVONO:

1. Monitorare le scadenze di tutti i titoli autorizzativi ambientali in essere (Autorizzazione Unica Ambientale, autorizzazioni allo scarico, provvedimenti di AIA o VIA ove applicabili), avviando le procedure di rinnovo con congruo anticipo rispetto alla data di scadenza;
2. Conservare in apposito archivio informatico tutti i titoli autorizzativi, i relativi allegati tecnici, le prescrizioni operative e la corrispondenza con gli enti competenti;
3. Verificare che le prescrizioni contenute nei provvedimenti autorizzativi siano recepite nei processi operativi e comunicate al personale coinvolto;

Trasmettere all'OdV copia dei nuovi provvedimenti autorizzativi ricevuti o delle comunicazioni di avvio di procedimenti di rinnovo, modifica o revoca, nei termini e con le modalità definiti nella Sezione 11 della presente Procedura.

Vige il divieto per tutte le Funzioni Aziendali di avviare o continuare attività produttive e di gestione ambientale in assenza dei prescritti titoli autorizzativi ovvero in violazione delle prescrizioni ivi contenute.

5.3 SELEZIONE E QUALIFICA DEI FORNITORI AMBIENTALI

La selezione dei soggetti terzi cui sono affidate attività di raccolta, trasporto, recupero e smaltimento dei rifiuti, nonché di bonifica e messa in sicurezza dei siti, costituisce un'attività sensibile ad alto rischio ai fini del D.Lgs. 231/2001 e deve essere svolta con criteri di trasparenza, oggettività e tracciabilità.

LE FUNZIONI AZIENDALI COMPETENTI DEVONO, PRIMA DELL'AVVIO DI QUALSIASI RAPPORTO CONTRATTUALE CON UN FORNITORE AMBIENTALE:

1. Acquisire e verificare la documentazione attestante l'iscrizione all'Albo Nazionale Gestori Ambientali nelle categorie pertinenti all'attività da svolgere, ai sensi del D.Lgs. 3 aprile 2006, n. 152 (Codice dell'Ambiente) e successive modificazioni;
2. Verificare la validità e l'adeguatezza delle autorizzazioni all'esercizio degli impianti di destinazione dei rifiuti (recupero, smaltimento, trattamento);
3. Acquisire il DURC (Documento Unico di Regolarità Contributiva) e verificarne la regolarità;
4. Effettuare una valutazione del profilo reputazionale e di conformità normativa del fornitore, inclusa la verifica di eventuali precedenti penali o amministrativi rilevanti;
5. Inserire in tutti i contratti stipulati con fornitori ambientali specifiche clausole di compliance 231 che prevedano l'obbligo di rispetto del Modello e del Codice Etico di IDRAGEST, nonché la facoltà di risoluzione del contratto in caso di violazioni;
6. Archiviare tutta la documentazione raccolta in apposita cartella informatica dedicata al fornitore, aggiornandola ad ogni rinnovo contrattuale o modifica delle condizioni.

Vige il divieto di affidare attività di gestione dei rifiuti o di bonifica a soggetti privi delle necessarie abilitazioni e autorizzazioni, ovvero a soggetti rispetto ai quali emergano elementi di non conformità normativa o reputazionale.

5.4 TRACCIABILITÀ DEI RIFIUTI E SISTEMI DIGITALI

La corretta tenuta dei documenti e dei registri di tracciabilità dei rifiuti rappresenta un presidio fondamentale per la prevenzione dei reati ambientali e per la tutela dell'integrità aziendale.

LE FUNZIONI AZIENDALI INTERESSATE SONO TENUTE A GARANTIRE:

1. La corretta e tempestiva compilazione del Registro di carico e scarico dei rifiuti e dei Formulari di Identificazione dei Rifiuti (FIR) per ogni movimento di rifiuto in uscita, nel rispetto delle disposizioni del D.Lgs. 152/2006 e del D.Lgs. 116/2020;
2. L'accreditamento e l'operatività sul portale RENTRI (Registro Elettronico Nazionale per la Tracciabilità dei Rifiuti), provvedendo alla trasmissione dei dati nei tempi e con le modalità stabiliti dalla normativa vigente;
3. La conservazione di tutta la documentazione di tracciabilità (registri, formulari, certificati di analisi, schede di caratterizzazione) per il periodo minimo previsto dalla legge, in formato sia cartaceo che informatico;
4. La riconciliazione periodica tra i dati di carico/scarico registrati e la documentazione di trasporto e smaltimento ricevuta dai fornitori (quarta copia FIR o equivalente digitale);
5. La segnalazione immediata all'OdV di qualsiasi anomalia, discrepanza o irregolarità riscontrata nella documentazione di tracciabilità.

Vige il divieto di alterare, omettere o antidatare qualsiasi documento di tracciabilità dei rifiuti, nonché di utilizzare formulari o registri non conformi ai modelli ufficiali previsti dalla normativa vigente.

REGOLE SPECIFICHE DI CONDOTTA

Ad integrazione dei principi comportamentali e dei divieti sopra elencati, oltre che alle previsioni del Codice Etico, si ricorda che sono state formalizzate specifiche procedure interne e norme aziendali volte a disciplinare le attività operative ed i controlli in essere nell'ambito dei principali processi aziendali.

Nello svolgimento delle attività sensibili e/o strumentali, tutti i Destinatari del Modello, ed in particolare i soggetti aziendali coinvolti nelle aree a rischio, sono tenuti a tenere un comportamento corretto e trasparente, in conformità a quanto disposto dalle previsioni di legge esistenti in materia, dal Codice Etico adottato dalla Società e dalle procedure e norme aziendali sopra richiamate.

In particolare i Destinatari della presente procedura dovranno porre in essere:

1. Attività di identificazione, caratterizzazione e classificazione dei rifiuti

2. Attività di raccolta e deposito temporaneo dei rifiuti

3. Selezione e gestione dei fornitori per l'attività di trasporto e smaltimento dei rifiuti

4. Comunicazione di eventi che siano potenzialmente in grado di contaminare il suolo, il sottosuolo, le acque superficiali e/o le acque sotterranee

5. Attività di bonifica di suolo, sottosuolo, acque superficiali e/o acque sotterranee

6. L. 147/2025 REATI AMBIENTALI E RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI

L'art. 6 del DL 116/2025 amplia in modo diretto la responsabilità amministrativa egli enti in relazione ai reati ambientali modificando l'art. 25-undecies del D.lgs. 231/2001.
Le modifiche mirano a introdurre nuovi reati con riferimento a:

- Art. 452-quaterdecies c.p., omessa bonifica;
- Art. 452-septies c.p., impedimento di controllo;
- Art. 259-ter D. lgs 152/2006, delitti colposi in materia dei rifiuti;
- Art. 259-bis D. Lgs 152/2006, aggravante dell'attività di imprese;
- Art. 256- bis D. lgs 152/2006, combustione illecita di rifiuti;
- Art. 256- ter D. lgs 152/2006, abbandono di rifiuti pericolosi;
- Art. 255- bis D. lgs 152/2006, abbandono di rifiuti non pericolosi in casi particolari;

Inoltre, le modifiche mirano a rafforzare il sistema sanzionatorio a carico degli enti per i reati ambientali, ampliando le condotte punibili, innalzando le sanzioni e prevedendo misure interdittive più severe e articolate:

1. l'aumento delle sanzioni pecuniarie: sono stati innalzati gli importi minimi e massimi delle sanzioni per numerose fattispecie di reati ambientali, come ad esempio per i reati di cui agli artt. 452-bis, 452-quater, 452-sexies, 452-terdecies e 452-quaterdecies c.p., nonché per le violazioni degli artt. 255-bis, 255-ter, 256 e 256-bis del D.lgs. n. 152/2006.
2. l'ampliamento delle ipotesi sanzionatorie: sono state inserite nuove lettere (e-bis, e-ter, e-quater, a-bis, a-ter, b-bis) che prevedono ulteriori fattispecie sanzionate, tra cui nuovi reati ambientali come la violazione degli artt. 452-septies, 452-terdecies e 452-quaterdecies c.p. e di diverse disposizioni del D.lgs. n. 152/2006.
3. la riformulazione e abrogazione di alcune disposizioni: alcune lettere sono state riscritte (es. lettera e) o abrogate (es. lettera f).
4. il coordinamento normativo: modificato il comma 1-bis per includere nuove lettere e semplificare la formulazione, eliminando alcune limitazioni temporali.

5. la riduzione delle sanzioni in casi particolari: introdotto il nuovo comma 2-bis che prevede una riduzione delle sanzioni da un terzo a due terzi in presenza delle condizioni di cui all'art. 259-ter del D.lgs. n. 152/2006.
6. l'innalzamento delle sanzioni interdittive. Sono state ridefinite le ipotesi e la durata delle sanzioni interdittive, specificando i casi in cui si applicano per sei mesi o fino a un anno, e prevedendo l'interdizione definitiva dall'attività per gli enti che facilitano sistematicamente determinati reati ambientali.

7 PRESIDI DI CONTROLLO E IMPEGNI PER LA SALVAGUARDIA AMBIENTALE

IDRAGEST è consapevole che l'impegno costante verso la compatibilità ambientale, al fine di prevenire — nel rispetto della legislazione vigente — l'inquinamento e garantire una gestione razionale delle risorse naturali, rappresenti un'opportunità di sviluppo per l'azienda, migliorandone l'immagine nel contesto sociale in cui opera e contribuendo alla soddisfazione dei clienti finali.

La Società persegue l'obiettivo di coniugare le esigenze operative con la salvaguardia dell'ambiente, in coerenza con la propria Politica Ambientale e con i principi del D.Lgs. 231/2001 e del D.Lgs. 152/2006 (Testo Unico Ambientale). A tal fine, la presente Sezione definisce i presidi di controllo e gli impegni programmatici che IDRAGEST adotta per garantire un piano strutturato di miglioramento continuo della gestione ambientale.

7.1 ASSEGNAZIONE DI RESPONSABILITÀ GESTIONALI

Al fine di garantire un'efficace gestione dei profili ambientali connessi alle attività aziendali, IDRAGEST definisce chiaramente i ruoli, i poteri e le responsabilità all'interno della propria struttura organizzativa, assicurando che ogni funzione coinvolta disponga delle competenze tecniche e delle deleghe formali necessarie.

LE FUNZIONI AZIENDALI COMPETENTI DEVONO:

1. Individuare formalmente i soggetti responsabili della gestione ambientale — tra cui, a titolo esemplificativo, il Responsabile Tecnico, il RSPP e i referenti di sito — definendone i poteri di spesa, di intervento e le modalità di coordinamento con le strutture operative;
2. Assicurare che i soggetti delegati possiedano le competenze tecniche e l'esperienza adeguate per l'adempimento degli obblighi normativi in materia ambientale;

3. Predisporre e conservare documentazione formale attestante l'attribuzione delle responsabilità ambientali (es. organigramma, lettere di nomina, deleghe di funzione);
4. Verificare periodicamente l'adeguatezza delle deleghe in essere, provvedendo al loro tempestivo aggiornamento in caso di mutamenti organizzativi, variazioni di sede o modifiche alle attività produttive.

Vige il divieto di operare in ambiti sensibili sotto il profilo ambientale in assenza di una chiara e formale attribuzione di responsabilità, ovvero di agire in carenza di poteri decisionali e di spesa coerenti con l'incarico affidato.

7.2 RICERCA TECNOLOGICA E MIGLIORAMENTO CONTINUO

IDRAGEST persegue la riduzione sistematica degli impatti ambientali attraverso l'adozione delle migliori tecnologie disponibili (BAT — Best Available Techniques) e l'ottimizzazione continua dei processi operativi, al fine di minimizzare il consumo di risorse naturali e prevenire eventi contaminanti.

LA SOCIETÀ E LE FUNZIONI INTERESSATE SONO TENUTE A:

1. Valutare periodicamente l'introduzione di soluzioni tecnologiche volte a ridurre le emissioni in atmosfera, ottimizzare il consumo di risorse idriche ed energetiche e minimizzare la produzione di rifiuti;
2. Definire e approvare formalmente un Piano di Miglioramento Ambientale su base annuale, recante obiettivi misurabili, indicatori di performance (KPI) e scadenze certe, garantendone il costante monitoraggio sullo stato di avanzamento;
3. Privilegiare, in sede di acquisto o sostituzione di macchinari, impianti e attrezzature, soluzioni a basso impatto ambientale, alta efficienza energetica e conformi alle prescrizioni autorizzative vigenti;
4. Documentare le valutazioni tecnico-ambientali effettuate a supporto delle scelte di investimento, al fine di garantirne la tracciabilità.

7.3 SISTEMA DI GESTIONE AMBIENTALE (ISO 14001:2015)

Il principale presidio di controllo per la prevenzione dei reati ambientali di cui al D.Lgs. 231/2001 è costituito dal Sistema di Gestione Ambientale (SGA), implementato in conformità allo standard internazionale ISO 14001:2015. Il SGA rappresenta lo strumento organizzativo attraverso il quale

IDRAGEST garantisce il controllo sistematico degli aspetti ambientali significativi e l'adempimento degli obblighi di conformità.

LE FUNZIONI COMPETENTI DEVONO:

1. Mantenere attiva la certificazione del SGA, assicurando il regolare svolgimento degli audit di sorveglianza e di rinnovo da parte dell'Ente certificatore accreditato;
2. Garantire che tutte le procedure operative ambientali siano costantemente aggiornate rispetto all'evoluzione normativa e tecnica, e portate a conoscenza del personale operativo mediante adeguati strumenti di comunicazione e formazione;
3. Pianificare ed eseguire audit interni periodici, con frequenza almeno annuale, per verificare la conformità dei processi aziendali ai requisiti dello standard ISO 14001:2015, alle prescrizioni autorizzative e alle disposizioni di legge;
4. Registrare formalmente le non conformità rilevate, definendo azioni correttive proporzionate e monitorandone la chiusura entro i termini previsti;
5. Conservare tutta la documentazione del SGA (procedure, registrazioni, rapporti di audit, piani d'azione) in modo ordinato e accessibile, garantendone la tracciabilità nel tempo.

7.4 MONITORAGGIO DELLE PERFORMANCE AMBIENTALI

La Società adotta un sistema strutturato di monitoraggio continuo per verificare l'efficacia dei presidi ambientali in essere, assicurare il rispetto dei limiti imposti dai titoli autorizzativi e rilevare tempestivamente eventuali scostamenti rispetto agli obiettivi definiti nel Piano di Miglioramento Ambientale.

LE STRUTTURE OPERATIVE SONO TENUTE A:

1. Eseguire campionamenti e analisi periodiche sulle matrici ambientali di pertinenza (es. scarichi idrici, emissioni in atmosfera, rifiuti prodotti), avvalendosi di laboratori accreditati secondo le normative vigenti e nel rispetto delle frequenze stabilite dalle autorizzazioni ambientali;
2. Registrare sistematicamente i dati relativi ai consumi di materie prime, di energia e di risorse idriche, nonché i volumi di rifiuti prodotti e avviati al recupero o allo smaltimento, secondo le modalità previste dalle procedure del SGA;
3. Analizzare periodicamente gli scostamenti tra i dati rilevati e i target prefissati, individuando le cause e avviando le conseguenti azioni correttive o preventive;

4. Conservare tutta la documentazione di monitoraggio e i relativi certificati analitici, rendendola disponibile in occasione di ispezioni da parte delle Autorità competenti (ARPA, NOE, ATS, ecc.);
5. Trasmettere all'Organismo di Vigilanza (OdV) un report semestrale sintetico sulle performance ambientali rilevate, sullo stato di avanzamento degli obiettivi del Piano di Miglioramento e sull'esito dei monitoraggi effettuati.

7.5 COINVOLGIMENTO DI DIPENDENTI E FORNITORI

La salvaguardia dell'ambiente richiede il coinvolgimento attivo e responsabile di tutti i soggetti che, a qualsiasi titolo, operano per conto di IDRAGEST o nelle proprie strutture, inclusi i fornitori e i subappaltatori che intervengono nel ciclo produttivo e operativo aziendale.

IDRAGEST SI IMPEGNA A:

1. Promuovere, con cadenza almeno annuale, iniziative di sensibilizzazione, formazione e addestramento specifico per il personale dipendente sulle corrette modalità di gestione dei rischi ambientali, con particolare riguardo alle attività aventi impatti significativi sull'ambiente;
2. Inserire nei processi di qualifica e selezione dei fornitori e subappaltatori specifici requisiti di compatibilità ambientale, richiedendo l'adesione ai medesimi standard di tutela adottati dalla Società e la dichiarazione di assenza di precedenti condanne per reati ambientali;
3. Prevedere nei contratti con i fornitori e subappaltatori apposite clausole ambientali, che contemplino il rispetto della normativa vigente, l'obbligo di comunicazione tempestiva di incidenti o anomalie e la facoltà di risoluzione del contratto in caso di gravi e reiterate violazioni;
4. Verificare l'operato dei fornitori e subappaltatori in fase di esecuzione contrattuale, anche mediante audit o sopralluoghi, e documentare le risultanze delle verifiche effettuate;
5. Incentivare la segnalazione di eventi sentinella ("near miss" ambientali) da parte di tutto il personale, garantendo l'anonimato e la protezione del segnalante, al fine di prevenire il verificarsi di eventi contaminanti reali.

8 LEGGE N. 137/2023 – LA TUTELA PENALE DELL'AMBIENTE

La Legge n. 137/2023 che ha convertito in legge, con modificazioni, il D.L. 10 agosto 2023 n. 105 (cd. Decreto Giustizia) ha previsto la trasformazione da illecito amministrativo a reato contravvenzionale della fattispecie di abbandono di rifiuti di cui all'art. 255 D.Lgs. n. 152/2006.

La norma punisce con l'ammenda da 1.000 a 10.000 euro – fatto salvo quanto disposto dall'art. 256, comma 2, in materia di responsabilità penale per abbandono di rifiuti dei responsabili di enti o imprese – chiunque abbandoni o depositi rifiuti ovvero li immetta nelle acque superficiali o sotterranee in violazione degli artt. 192, commi 1 e 2 (che vietano l'abbandono e il deposito incontrollati di rifiuti sul suolo e nel suolo e l'immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee), 226 comma 2 (che vieta l'immissione di imballaggi terziari nel normale circuito di raccolta dei rifiuti urbani), e 231, commi 1 e 2 (in materia di demolizione di veicoli fuori uso), del cd. Codice dell'Ambiente.

La pena è aumentata fino al doppio se l'abbandono riguarda rifiuti pericolosi.

Il legislatore è intervenuto, inoltre, sulle disposizioni in materia di confisca di cui all'art. 240-bis c.p., estendendo il catalogo dei reati per i quali è prevista, in caso di condanna o patteggiamento, la confisca del denaro o dei beni di cui il condannato abbia la disponibilità in valore sproporzionato rispetto al proprio reddito e di cui non possa giustificare la provenienza (cd. confisca allargata).

In particolare, viene estesa la confisca, già prevista per i delitti di disastro ambientale (art. 452-quater c.p.) e di associazione a delinquere finalizzata alla commissione di delitti contro l'ambiente (art. 452-octies, primo comma, c.p.), anche alle seguenti fattispecie:

- l'inquinamento ambientale (art. 452-bis c.p.);
- la morte o lesioni come conseguenza del delitto di inquinamento ambientale (art. 452-ter c.p.);
- il traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.);
- le attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.).

9 DECRETO LEGGE N.116 DELL'8 AGOSTO 2025 CONVERTITO IN LEGGE N. 147 DEL 3 OTTOBRE 2025

Con il Decreto Legge n.116 dell'8 agosto 2025 "*Disposizioni urgenti per il contrasto alle attività illecite in materia di rifiuti, per la bonifica dell'area denominata Terra dei fuochi, nonché in materia di assistenza alla popolazione colpita da eventi calamitosi*" il legislatore mira a contrastare i reati ambientali e a tutelare la salute pubblica e l'ambiente, prendendo spunto dalla realtà ambientale, particolarmente minacciata nelle provincie di Napoli e Caserta a seguito di sversamenti incontrollati di rifiuti e loro distruzione tramite incendi. Inoltre, il Decreto Legge n.116 dell'8 agosto 2025, confermato dalla Legge n.147 del 3 ottobre 2025, in merito alle operazioni sotto

copertura, già contemplate dai reati transnazionali, ha esteso l'Art.9 comma 1 lettera a) Legge n.146 del 16 marzo 2006 anche ai reati ambientali.

9.1 ABBANDONO DI RIFIUTI NON PERICOLOSI IN CASI PARTICOLARI (ART. 255-BIS D. LGS. N. 152/2006 (INTRODOTTO DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E CONVERTITO DA LEGGE N.147 DEL 3 OTTOBRE 2025)

Questo nuovo reato è stato introdotto dal DL n. 116 dell'8 agosto 2025 per punire chi abbandona o deposita rifiuti non pericolosi ovvero li immette nelle acque superficiali o sotterranee.

Si riporta il testo integrale dell'articolo in cui, come per l'Art.255 "Abbandono di rifiuti non pericolosi", vengono coinvolti i titolari di imprese e responsabili di enti ed è prevista la sanzione accessoria della sospensione della patente di guida da due a sei mesi quando l'abbandono o il deposito vengono effettuati mediante l'utilizzo di veicoli a motore.

[I]. Chiunque, in violazione delle disposizioni degli articoli 192, commi 1 e 2, 226, comma 2, e 231, commi 1 e 2, abbandona o deposita rifiuti non pericolosi ovvero li immette nelle acque superficiali o sotterranee è punito con la reclusione da sei mesi a cinque anni se:

a) dal fatto deriva pericolo per la vita o l'incolumità delle persone ovvero pericolo di compromissione o deterioramento:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna

b) il fatto è commesso in siti contaminati o potenzialmente contaminati ai sensi dell'articolo 240 o comunque sulle strade di accesso ai predetti siti e relative pertinenze

[II]. I titolari di imprese e i responsabili di enti che, ricorrendo taluno dei casi di cui al comma 1, abbandonano o depositano in modo incontrollato rifiuti non pericolosi ovvero li immettono nelle acque superficiali o sotterranee in violazione del divieto di cui all'articolo 192, commi 1 e 2, sono puniti con la reclusione da nove mesi a cinque anni e sei mesi

[III]. Quando l'abbandono o il deposito vengono effettuati mediante l'utilizzo di veicoli a motore, al conducente del veicolo si applica, altresì, la sanzione accessoria della sospensione della patente di guida da due a sei mesi. Si applicano le disposizioni di cui al Titolo VI, Capo II, Sezione II del decreto legislativo 30 aprile 1992, n. 285.

9.2 ABBANDONO DI RIFIUTI PERICOLOSI (ART. 255-TER D. LGS. N. 152/2006 (INTRODOTTO DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E CONVERTITO DA LEGGE N.147 DEL 3 OTTOBRE 2025)

Il reato delll'Art.255-ter, introdotto dal DL n. 116 dell'8 agosto 2025, a differenza di quelli previsti dai precedenti articoli 255 e 255-bis si riferisce all'abbandono o al deposito di rifiuti pericolosi o la loro immersione nelle acque superficiali o sotterranee

L'art. 255 ter D.LGS. N. 152/2006 dispone testualmente che "*Chiunque, in violazione delle disposizioni degli articoli 192, commi 1 e 2, 226, comma 2, e 231, commi 1 e 2, abbandona o deposita rifiuti pericolosi ovvero li immette nelle acque superficiali o sotterranee è punito con la reclusione da uno a cinque anni.*

La pena è della reclusione da un anno e sei mesi a sei anni quando:

a) dal fatto deriva pericolo per la vita o per la incolumità delle persone ovvero pericolo di compromissione o deterioramento:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna

b) il fatto è commesso in siti contaminati o potenzialmente contaminati ai sensi dell'articolo 240 o comunque sulle strade di accesso ai predetti siti e relative pertinenze.

I titolari di imprese e i responsabili di enti che abbandonano o depositano in modo incontrollato rifiuti pericolosi ovvero li immettono nelle acque superficiali o sotterranee in violazione del divieto di cui all'articolo 192, commi 1 e 2 sono puniti con la reclusione da un anno a cinque anni e sei mesi. Quando ricorre taluno dei casi di cui al comma 2, la pena è della reclusione da due anni a sei anni e sei mesi.".

9.3 ATTIVITÀ DI GESTIONE DI RIFIUTI NON AUTORIZZATA (ART.256 D. LGS. N. 152/2006 MODIFICATO DA D.LGS.N.46/2014, DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E MODIFICATO DA LEGGE N. 147 DEL 3 OTTOBRE 2025)

Il reato si realizza quando si effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione

L'art. 256 D.LGS. N. 152/2006, completamente modificato dalla Legge n.147 del 3 ottobre 2025, dispone che "*Fuori dai casi sanzionati ai sensi dell'articolo 29-quattuordecies, comma 1, chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216 è punito con la pena dell'arresto da tre mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro. Se i fatti riguardano rifiuti pericolosi, la pena è della reclusione da uno a cinque anni*

La pena per i fatti di cui al comma 1, primo periodo, è della reclusione da uno a cinque anni quando:

a) dal fatto deriva pericolo per la vita o per la incolumità delle persone ovvero pericolo di compromissione o deterioramento:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna

b) il fatto è commesso in siti contaminati o potenzialmente contaminati ai sensi dell'articolo 240 o comunque sulle strade di accesso ai predetti siti e relative pertinenze

Se, ricorrendo taluno dei casi di cui al periodo che precede, i fatti riguardano rifiuti pericolosi, la pena è della reclusione da due anni a sei anni e sei mesi

Nel caso in cui le violazioni di cui ai commi 1 e 1-bis siano commesse mediante l'utilizzo di veicoli a motore, al conducente del veicolo si applica, altresì, la sanzione accessoria della sospensione della patente di guida da tre a nove mesi, secondo le disposizioni di cui al Titolo VI, Capo II, Sezione II del decreto legislativo 30 aprile 1992, n. 285

Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale per taluno dei fatti di cui ai commi 1 e 1-bis, consegue la confisca

del mezzo utilizzato per la commissione del reato, salvo che appartenga a persona estranea al reato

Fuori da casi sanzionati ai sensi dell'articolo 29-quattuordecies, comma 1, chiunque realizza o gestisce una discarica non autorizzata è punito con la reclusione da uno a cinque anni. Si applica la reclusione da un anno e sei mesi a cinque anni e sei mesi se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi

La realizzazione o gestione di una discarica non autorizzata è punita con la reclusione da due a sei anni quando:

a) dal fatto deriva pericolo per la vita o per la incolumità delle persone ovvero pericolo di compromissione o deterioramento:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna

b) il fatto è commesso in siti contaminati o potenzialmente contaminati ai sensi dell'articolo 240 o comunque sulle strade di accesso ai predetti siti e relative pertinenze

Se, ricorrendo taluno dei casi di cui al periodo che precede, la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi, la pena è della reclusione da due anni e sei mesi a sette anni

Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale per taluno dei fatti di cui ai commi 3 e 3-bis, consegue la confisca dell'area sulla quale è realizzata la discarica abusiva, salvo che appartenga a persona estranea al reato, fatti comunque salvi gli obblighi di bonifica o di ripristino dello stato dei luoghi

Salvo che il fatto costituisca più grave reato, si applica la pena dell'ammenda da euro 6.000 a euro 52.000 o dell'arresto fino a tre anni nei confronti di colui che, pur essendo titolare di autorizzazioni, iscrizioni o comunicazioni di cui agli articoli

208, 209, 210, 211, 212, 214, 215 e 216, non osservi le prescrizioni contenute o richiamate nelle autorizzazioni o nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni, sempre che il fatto riguardi rifiuti non pericolosi e quando non ricorrono le condizioni di cui al comma 1-bis, lettera a), numeri 1) e 2), e lettera b).
Chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti, è punito con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro
Chiunque effettua il deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi, con violazione delle disposizioni di cui all'articolo 227, comma 1, lettera b), è punito con la pena dell'arresto da tre mesi ad un anno o con la pena dell'ammenda da duemilaseicento euro a ventiseimila euro. Si applica la sanzione amministrativa pecuniaria da duemilaseicento euro a quindicimila cinquecento euro per i quantitativi non superiori a duecento litri o quantità equivalenti
Chiunque viola gli obblighi di cui agli articoli 231, commi 7, 8 e 9, 233, commi 12 e 13, e 234, comma 14, è punito con la sanzione amministrativa pecuniaria da duecentosessanta euro a mille cinquecentocinquanta euro.
I soggetti di cui agli articoli 233, 235 e 236 che non adempiono agli obblighi di partecipazione ivi previsti sono puniti con una sanzione amministrativa pecuniaria da ottomila euro a quarantacinquemila euro, fatto comunque salvo l'obbligo di corrispondere i contributi pregressi. Ai soggetti di cui all'articolo 234 che non adempiono agli obblighi di partecipazione ivi previsti, si applica la sanzione amministrativa pecuniaria di euro 5.000, fatto comunque salvo l'obbligo di corrispondere i contributi pregressi.".

9.4 COMBUSTIONE ILLECITA DI RIFIUTI (ART. 256-BIS D. LGS. N. 152/2006 (INTRODOTTO E MODIFICATO DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E CONVERTITO DA LEGGE N.147 DEL 3 OTTOBRE 2025)

Questo nuovo reato introdotto dal Decreto Legge n. 116 dell'8 agosto 2025 e confermato dalla Legge n.147 del 3 ottobre 2025, vuole punire chi appicca il fuoco a rifiuti, sia pericolosi che non pericolosi, abbandonati ovvero depositati in maniera incontrollata Oltre alla pena della reclusione il responsabile del reato è tenuto al ripristino dello stato dei luoghi, al risarcimento del danno ambientale e al pagamento, anche in via di regresso, delle spese per la bonifica.
ART. 256-BIS D. LGS. N. 152/2006 dispone che "*Salvo che il fatto costituisca più grave reato, chiunque appicca il fuoco a rifiuti abbandonati ovvero depositati in maniera incontrollata è punito con la reclusione da due a cinque anni. Nel caso in cui sia appiccato il fuoco a rifiuti pericolosi, si applica la pena della reclusione da tre a sei anni. Il responsabile è tenuto al ripristino dello stato dei luoghi, al risarcimento del danno ambientale e al pagamento, anche in via di regresso, delle spese per la bonifica.*

Le stesse pene si applicano a colui che tiene le condotte di cui all'articolo 255, commi 1 e 1.1 in funzione della successiva combustione illecita di rifiuti. Se i fatti di cui agli articoli 255-bis, 255-ter, 256 e 259 sono commessi in funzione della successiva combustione illecita di rifiuti, le pene per i predetti reati non possono essere inferiori a quelle stabilite dal comma 1.

La combustione di rifiuti non pericolosi è punita con la reclusione da tre a sei anni, quando:

a) dal fatto deriva pericolo per la vita o per la incolumità delle persone ovvero pericolo di compromissione o deterioramento:

1) delle acque o dell'aria, o di porzioni estese o significative del suolo o del sottosuolo

2) di un ecosistema, della biodiversità, anche agraria, della flora o della fauna

b) il fatto è commesso in siti contaminati o potenzialmente contaminati ai sensi dell'articolo 240 o comunque sulle strade di accesso ai predetti siti e relative pertinenze.

La combustione di rifiuti pericolosi, quando ricorre taluno dei casi di cui al periodo che precede, è punita con la reclusione da tre anni e sei mesi a sette anni.

Se ai fatti di cui al comma 3-bis segue l'incendio, le pene ivi previste sono aumentate sino alla metà.

La pena è aumentata di un terzo se i fatti di cui ai commi 1 e 3-bis sono commessi in territori che, al momento della condotta e comunque nei cinque anni precedenti, siano o siano stati interessati da dichiarazioni di stato di emergenza nel settore dei rifiuti ai sensi della legge 24 febbraio 1992, n. 225.

I mezzi utilizzati per il trasporto di rifiuti oggetto del reato di cui al comma 1 del presente articolo, inceneriti in aree o in impianti non autorizzati, sono confiscati ai sensi dell'articolo 259, comma 2, salvo che il mezzo appartenga a persona estranea alle condotte di cui al citato comma 1 del presente articolo e che non si configuri concorso di persona nella commissione del reato. Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale consegue la confisca dell'area sulla quale è commesso il reato, se di proprietà dell'autore o del concorrente nel reato, fatti salvi gli obblighi di bonifica e ripristino dello stato dei luoghi.

Fermo restando quanto previsto dall'articolo 182, comma 6-bis, le disposizioni del presente articolo non si applicano all'abbruciamento di materiale agricolo o forestale naturale, anche derivato da verde pubblico o privato.

9.5 VIOLAZIONE DEGLI OBBLIGHI DI COMUNICAZIONE, DI TENUTA DEI REGISTRI OBBLIGATORI E DEI FORMULARI (ART. 258 D. LGS. N. 152/2006 MODIFICATO DA ART.4 DEL D.LGS.N.116 DEL 3 SETTEMBRE 2020, DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E DA LEGGE N.147 DEL 3 OTTOBRE 2025)

Con il Decreto Legge n. 116 dell'8 agosto 2025 confermato dalla Legge n. 147 del 3 ottobre 2025, oltre all'inasprimento delle pene pecuniarie, con l'aggiunta del comma 2-bis si è aggiunta la sanzione

amministrativa accessoria della sospensione della patente di guida da uno a quattro mesi se si tratta di rifiuti non pericolosi e da due a otto mesi se si tratta di rifiuti pericolosi a all'accertamento della violazione consegue altresì la sospensione dall'Albo nazionale dei gestori ambientali di cui all'articolo 212 per un periodo da due a sei mesi se il trasporto riguarda rifiuti non pericolosi e da quattro a dodici mesi se il trasporto riguarda rifiuti pericolosi.

Con l'aggiunta del comma «4-bis viene stabilita la confisca del mezzo utilizzato per la commissione del reato, salvo che appartenga a persona estranea al reato.

L'Art. 258 D. Lgs. n. 152/2006 dispone che "*I soggetti di cui all'articolo 189, comma 3, che non effettuano la comunicazione ivi prescritta ovvero la effettuano in modo incompleto o inesatto sono puniti con la sanzione amministrativa pecuniaria da duemila a diecimila euro; se la comunicazione è effettuata entro il sessantesimo giorno dalla scadenza del termine stabilito ai sensi della legge 25 gennaio 1994, n. 70, si applica la sanzione amministrativa pecuniaria da ventisei euro a centosessanta euro.*

Chiunque omette di tenere ovvero tiene in modo incompleto il registro di carico e scarico di cui all'articolo 190, comma 1, è punito con la sanzione amministrativa pecuniaria da quattromila a ventimila euro. Se il registro è relativo a rifiuti pericolosi si applica la sanzione amministrativa pecuniaria da diecimila euro a trentamila euro, nonché nei casi più gravi, la sanzione amministrativa accessoria facoltativa della sospensione da un mese a un anno dalla carica rivestita dal soggetto responsabile dell'infrazione e dalla carica di amministratore.

All'accertamento della violazione di cui al comma 2 consegue in ogni caso la sanzione amministrativa accessoria della sospensione della patente di guida da uno a quattro mesi se si tratta di rifiuti non pericolosi e da due a otto mesi se si tratta di rifiuti pericolosi. Si applicano le disposizioni di cui al Titolo VI, Capo I, Sezione II del decreto legislativo 30 aprile 1992, n. 285. All'accertamento della violazione consegue altresì la sospensione dall'Albo nazionale dei gestori ambientali di cui all'articolo 212 per un periodo da due a sei mesi se il trasporto riguarda rifiuti non pericolosi e da quattro a dodici mesi se il trasporto riguarda rifiuti pericolosi.

Nel caso di imprese che occupino un numero di unità lavorative inferiore a 15 dipendenti, le sanzioni sono quantificate nelle misure minime e massime da mille quaranta euro a seimila duecento euro per i rifiuti non pericolosi e da duemila settanta euro a dodicimila quattrocento.

euro per i rifiuti pericolosi. Il numero di unità lavorative è calcolato con riferimento al numero di dipendenti occupati mediamente a tempo pieno durante un anno, mentre i lavoratori a tempo parziale e quelli stagionali rappresentano frazioni di unità lavorative annue; ai predetti fini l'anno da prendere in considerazione è quello dell'ultimo esercizio contabile approvato, precedente il momento di accertamento dell'infrazione.

Salvo che il fatto costituisca reato, chiunque effettua il trasporto di rifiuti senza il formulario di cui all'articolo 193 o senza i documenti sostitutivi ivi previsti, ovvero riporta nel formulario stesso dati incompleti o inesatti è punito con la sanzione amministrativa pecuniaria da milleseicento euro a diecimila euro. Fatta salva l'applicazione del comma 5, chiunque effettua il trasporto di rifiuti pericolosi senza il formulario di cui all'articolo 193 o senza i documenti sostitutivi ivi previsti è punito con la pena della reclusione da uno a tre anni. Tale ultima pena si applica anche a chi nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto.

Alla sentenza di condanna o alla sentenza emessa ai sensi dell'articolo 444 del codice di procedura penale per taluno dei reati di cui al comma 4, secondo e terzo periodo, consegue la confisca del mezzo utilizzato per la commissione del reato, salvo che appartenga a persona estranea al reato.

Nei casi di cui ai commi 1,2 e 4, ove le informazioni, pur formalmente incomplete o inesatte, siano rinvenibili in forma corretta dai dati riportati nella comunicazione al catasto, nei registri cronologici di carico e scarico, nei formulari di identificazione dei rifiuti trasportati e nelle altre scritture contabili tenute per legge, si applica la sanzione amministrativa pecuniaria da duecentosessanta euro a mille cinquecentocinquanta euro. La stessa pena si applica nei casi di indicazioni formalmente incomplete o inesatte, ma contenenti gli elementi atti a ricostruire le informazioni richieste ai sensi di legge, nonché' nei casi di mancato invio alle autorità' competenti e di mancata conservazione dei registri di cui all'articolo 190, comma 1, o del formulario di cui all'articolo 193. La sanzione ridotta di cui alla presente disposizione si applica alla omessa o incompleta tenuta dei registri cronologici di carico e scarico da parte del produttore quando siano presenti i formulari di trasporto, a condizione che la data di produzione e presa in carico dei rifiuti possa essere dimostrata, o coincida con la data di scarico dei rifiuti stessi.

I soggetti di cui all'articolo 220, comma 2, che non effettuano la comunicazione ivi prescritta ovvero la effettuino in modo incompleto o inesatto sono puniti con la sanzione amministrativa pecuniaria da duemila euro a diecimila euro; nel caso in cui la comunicazione sia effettuata entro il sessantesimo giorno dalla scadenza del termine stabilito ai sensi della legge 25 gennaio 1994, n. 70, si applica la sanzione amministrativa pecuniaria da ventisei euro a centosessanta euro.

I soggetti responsabili del servizio di gestione integrata dei rifiuti urbani e assimilati che non effettuano la comunicazione di cui all'articolo 189, comma 3, ovvero la effettuano in modo incompleto o inesatto, sono puniti con la sanzione amministrativa pecuniaria da duemila euro a diecimila euro; nel caso in cui la comunicazione sia effettuata entro il sessantesimo giorno dalla scadenza del termine stabilito ai sensi della legge 25 gennaio 1994, n. 70, si applica la sanzione amministrativa pecuniaria da ventisei euro a centosessanta euro.

In caso di violazione di uno o più degli obblighi previsti dall'articolo 184, commi 5- bis.1 e 5-bis.2, e dall'articolo 241-bis, commi 4-bis, 4-ter e 4-quater, del presente decreto, il comandante del poligono militare delle Forze armate è punito con la sanzione amministrativa pecuniaria da tremila euro a diecimila euro. In caso di violazione reiterata degli stessi obblighi si applica la sanzione amministrativa pecuniaria da cinquemila euro a ventimila euro.

Chi con un'azione od omissione viola diverse disposizioni di cui al presente articolo, ovvero commette più violazioni della stessa disposizione, soggiace alla sanzione amministrativa prevista per la violazione più grave, aumentata sino al doppio. La stessa sanzione si applica a chi con più azioni od omissioni, esecutive di un medesimo disegno, commette anche in tempi diversi più violazioni della stessa o di diverse disposizioni di cui al presente articolo.

Le disposizioni di cui al comma 9 si applicano a tutte le violazioni commesse anteriormente alla data di entrata in vigore del decreto legislativo 3 settembre 2020, n. 116, per le quali non sia già intervenuta sentenza passata in giudicato.

Salvo che il fatto costituisca reato e fermo restando l'obbligo di corrispondere i contributi pregressi eventualmente non versati, la mancata o irregolare iscrizione al Registro di cui all'articolo 188-bis, nelle tempistiche e con le modalità' definite nel decreto di cui al comma 1 del medesimo articolo, comporta l'applicazione di una sanzione amministrativa pecuniaria da cinquecento euro a duemila euro, per i rifiuti non pericolosi, e da mille euro a tremila euro per i rifiuti pericolosi. La mancata o incompleta trasmissione dei dati informativi con le tempistiche e le modalità ivi definite comporta l'applicazione di una sanzione amministrativa pecuniaria da cinquecento euro a duemila euro per i rifiuti non pericolosi e da mille euro a tremila euro per i rifiuti pericolosi.

Le sanzioni di cui al comma 10 sono ridotte ad un terzo nel caso in cui si proceda all'iscrizione nel Registro entro 60 giorni dalla scadenza dei termini previsti dal decreto di cui al comma 1 dell'articolo 188-bis e dalle procedure operative. Non è soggetta alle sanzioni di cui al comma 11 la mera correzione di dati, comunicata con le modalità' previste dal decreto citato. Gli importi delle sanzioni di cui al comma 10 sono versati ad apposito capitolo dell'entrata del bilancio dello Stato per essere riassegnati, con decreto del Ministro dell'economia e delle finanze, ai pertinenti capitoli dello stato di previsione del Ministero dell'ambiente e della tutela del territorio e del mare, destinati agli interventi di bonifica dei siti di cui all'articolo 252, comma 5, ove ricorrano le condizioni di cui all'articolo 253, comma 5, secondo criteri e modalità di ripartizione fissati con decreto del Ministro dell'ambiente e della tutela del territorio e del mare.

Le sanzioni di cui al presente articolo, conseguenti alla trasmissione o all'annotazione di dati incompleti o inesatti sono applicate solo nell'ipotesi in cui i dati siano rilevanti ai fini della tracciabilità, con esclusione degli errori materiali e violazioni formali. In caso di dati incompleti o inesatti rilevanti ai fini della tracciabilità di tipo seriale, si applica una sola sanzione aumentata fino al triplo.

9.6 SPEDIZIONE ILLEGALE DI RIFIUTI (ART. 259 D. LGS. N. 152/2006 MODIFICATI RUBRICA E TESTO DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E CONVERTITO CON LEGGE N. 147 DEL 3 OTTOBRE 2025)

Il Decreto Legge n. 116 dell'8 agosto 2025, convertito dalla Legge n.147 del 3 ottobre 2025,5ha modificato la rubrica dell'Art.259 da "Traffico illecito di rifiuti" a "Spedizione illegale di rifiuti" ai sensi degli articoli 2, punto 35 del regolamento (CE) n. 1013/2006 del Parlamento europeo e del Consiglio, del 14 giugno 2006 e dell'articolo 3, punto 26 del regolamento (UE) n. 2024/1157 del Parlamento europeo e del Consiglio dell'11 aprile 2024

Si riporta il testo dell'articolo così modificato:

"*Chiunque effettua una spedizione di rifiuti costituente spedizione illegale ai sensi degli articoli 2, punto 35 del regolamento (CE) n. 1013/2006 del Parlamento europeo e del Consiglio, del 14 giugno 2006 e dell'articolo 3, punto 26 del regolamento (UE) n. 2024/1157 del Parlamento europeo e del Consiglio dell'11 aprile 2024, è punito con la reclusione da uno a cinque anni. La pena è aumentata in caso di spedizione di rifiuti pericolosi.*

Alla sentenza di condanna, o a quella emessa ai sensi dell'articolo 444 del codice di procedura penale, per i reati relativi al traffico illecito di cui al comma 1 o al trasporto illecito di cui agli articoli 25 e 258, comma 4, consegue obbligatoriamente la confisca del mezzo di trasporto.".

9.7 AGGRAVANTE DELL'ATTIVITÀ DI IMPRESA (ART. 259-BIS D. LGS. N. 152/2006 INTRODOTTO DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E CONVERTITO DALLA LEGGE N.147 DEL 3 OTTOBRE 2025)

Con l'Art.259-bis il legislatore ha inteso punire con l'aumento delle pene rispettivamente previste dagli articoli 256, 256-bis e 259 e con le sanzioni previste dall'articolo 9, comma 2, del decreto legislativo 8 giugno 2001, n. 231 il titolare dell'impresa o il responsabile di una attività anche per l'omessa vigilanza sull'operato degli autori materiali del delitto ambientale comunque riconducibili all'impresa o all'attività stessa.

Si riporta testualmente il testo dell'articolo:

"*Le pene rispettivamente previste dagli articoli 256, 256-bis e 259 sono aumentate di un terzo se i fatti sono commessi nell'ambito dell'attività di un'impresa o comunque di un'attività organizzata. Il titolare dell'impresa o il responsabile dell'attività comunque organizzata è responsabile anche sotto l'autonomo profilo dell'omessa vigilanza sull'operato degli autori.*

materiali del delitto comunque riconducibili all'impresa o all'attività stessa. Ai predetti titolari d'impresa o responsabili dell'attività si applicano altresì le sanzioni previste dall'articolo 9, comma 2, del decreto legislativo 8 giugno 2001, n. 231.".

9.8 DELITTI COLPOSI IN MATERIA DI RIFIUTI (ART. 259-TER D. LGS. N. 152/2006 INTRODOTTO DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E CONVERTITO DALLA LEGGE N.147 DEL 3 OTTOBRE 2025)

L'art. 259 ter del D.LGS. N. 152/2006 dispone testualmente che "*Se taluno dei fatti di cui agli articoli 255-bis, 255-ter, 256 e 259 è commesso per colpa, le pene previste dai medesimi articoli sono diminuite da un terzo a due terzi*".

7.9

10 CERTIFICAZIONE ISO 14001:2015

Come previsto nella PMOG10, IDRAGEST si è munita di una certificazione ISO 14001:2015 relativa al "Sistema di Gestione Ambientale", che assicura la conformità della Società agli standard internazionali sui requisiti necessari per fornire una struttura gestionale per l'integrazione delle pratiche di gestione ambientale, perseguendo la protezione dell'ambiente, la prevenzione dell'inquinamento, nonché la riduzione del consumo di energia e risorse.

Invero, in tal modo IDRAGEST dimostra di gestire le proprie attività nei confronti dell'ambiente ed il proprio impegno per:

A. limitare l'inquinamento.

B. soddisfare requisiti legali ed altri applicabili

C. migliorare in modo continuativo il proprio sistema di gestione ambientale in modo da migliorare;

in senso globale, la propria prestazione ambientale.

11 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto su apposita piattaforma informatica – tutta la documentazione necessaria.

Conclusa l'ispezione, il PRES, o il responsabile della Funzione aziendale interessata, all'uopo incaricata, dovrà inviare una relazione riepilogativa all'OdV.

In ogni caso, il Responsabile della procedura informa, tempestivamente, l'Organismo di Vigilanza sulle ispezioni della Pubblica Amministrazione e sugli adempimenti richiesti alla Società.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse ai Processi Sensibili, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

CIÒ POSTO, IL RESPONSABILE DELLA PROCEDURA INFORMA TEMPESTIVAMENTE L'ODV IN ORDINE A:

1. ispezioni e contestazioni ambientali;
2. eventi di sversamento o abbandono di rifiuti;
3. non conformità nel deposito temporaneo;
4. irregolarità della documentazione di trasporto o conferimento;
5. ostacoli ai controlli;
6. prescrizioni di bonifica o ripristino;
7. reclami ambientali provenienti da clienti o autorità.

L'OdV svolge verifiche periodiche sull'effettiva attuazione dei controlli.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI E FUNZIONI DEL MODELLO 3

2 ACRONIMI AZIENDALI 5

3 RIFERIMENTI NORMATIVI 6

4 CAMPO DI APPLICAZIONE RESPONSABILE DELLA PROCEDURA 6

5 I REATI DI CUI ALL'ART. 24-TER DEL DECRETO 6

5.1. - ASSOCIAZIONE PER DELINQUERE (ART. 416 C.P.) 7

5.2. – ASSOCIAZIONE DI TIPO MAFIOSO ANCHE STRANIERA (ART. 416-BIS C.P.) . 8

5.3. – SCAMBIO ELETTORALE POLITICO MAFIOSO (ART. 416-TER C.P.).....10

5.4. - SEQUESTRO DI PERSONA A SCOPO DI ESTORSIONE (ART. 630 C.P.).....11

5.5. - TRATTAMENTO SANZIONATORIO PER LE FATTISPECIE DI CUI ALL'ART. 24-TER DEL DECRETO 12

6. – ATTIVITA' SENSIBILI A RISCHIO REATO ED I PRESIDI DI CONTROLLO 12

7 PRINCIPI GENERALI DI COMPORTAMENTO E REGOLE DI CONDOTTA 22

8 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO 23

1 OBIETTIVI E FUNZIONI DEL MODELLO

L'art. 24-ter rubricato "*Delitti di criminalità organizzata*" è stato inserito nel novero dei reati presupposto della responsabilità amministrativa degli Enti dalla legge 15 luglio 2009, n. 94.

L'inserimento dei delitti contro la criminalità organizzata non rappresenta una novità assoluta, in quanto l'articolo 10 della legge n. 146/2006 ("Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001") aveva già previsto alcuni delitti associativi tra i reati presupposto della responsabilità amministrativa dell'Ente, seppur circoscrivendo la stessa responsabilità alle ipotesi in cui i reati rivestissero carattere transnazionale. Invero, con l'estensione di tali delitti anche all'ambito nazionale, il legislatore ha cercato di fornire una risposta all'esigenza di rafforzare la lotta contro i fenomeni di criminalità di impresa.

L'ART. 2, COMMA 29, DELLA SOPRA CITATA LEGGE N. 94/2009, INSERENDO L'ART. 24-TER HA AGGIUNTO, AL COMMA 1, UNA PRIMA SERIE DI REATI:

• associazione per delinquere finalizzata al compimento di specifiche ipotesi di reato (art. 416 comma 6 c.p.);

• associazione di stampo mafioso (art. 416-bis c.p.);

• scambio elettorale politico-mafioso (art. 416-ter c.p.);

• sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.);

• delitti commessi avvalendosi delle condizioni derivanti dalla presenza di un'associazione di tipo mafioso ovvero al fine di agevolarne l'attività;

• associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope (art. 74 D.P.R. n. 309/1990).

IL COMMA 2 DELL'ARTICOLO CITATO PREVEDE, INOLTRE, QUALI POTENZIALI FONTI DI RESPONSABILITÀ DELL'ENTE, I SEGUENTI DELITTI:

• associazione per delinquere (art. 416 c.p.);

• art. 407 comma 2 lett. a) n. 5 c.p.p. ("delitti di illegale fabbricazione, introduzione nello Stato, messa in cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra, di esplosivi e di armi clandestine").

Dunque, l'associazione per delinquere di cui all'art. 416 c.p. si configura: "*Quando tre o più persone si associano allo scopo di commettere più delitti*"; la condotta incriminata consiste sia nel "*promuovere, costituire od organizzare*"

l'associazione, sia nel "*partecipare*" all'associazione. Elemento fondamentale è la coscienza e volontà di far parte in maniera permanente di un sodalizio criminoso, ed anche l'"*intenzione di contribuire all'attuazione del generico programma criminoso",* tuttavia non è necessario che la volontà abbia quale oggetto immediato la realizzazione di delitti specificamente individuati.

Orbene, l'inserimento del delitto di associazione per delinquere nel catalogo 231 comporta che laddove un numero non inferiore a tre di soggetti operanti in seno alla società (subordinati o apicali) si associ allo scopo di commettere reati, potrebbe essere contestata la fattispecie di associazione per delinquere anche a carico dell'ente che sarebbe chiamato a rispondere patrimonialmente per tale evento.

Orbene, poiché la contestazione dell'art. 416 c.p. - in quanto disposizione "aperta", idonea a ricomprendere nei reati-presupposto qualsiasi reato - determina una violazione del principio di tassatività del sistema sanzionatorio del D.lgs.vo n. 231 del 2001, è necessario trasferire gli elementi costitutivi del delitto di associazione per delinquere sul piano aziendale, al fine di eseguire una concreta mappatura del rischio di tale fattispecie criminosa.

Infatti, con la presente procedura si vogliono definire le regole di condotta e le procedure concrete che tutti i Destinatari sono tenuti ad asservare, al fine preciso di individuare le attività a rischio-reato ai sensi dell'articolo 6, comma 2, lett. a) del D.lgs.vo 231/2001 e prevenire la commissione dei delitti di criminalità organizzata, tenendo presente che la stessa natura del reato impedisce l'individuazione di peculiari settori dell'attività aziendale in cui vi sia rischio di perpetrazione dello stesso.

Ancora, la necessità di implementare la presente procedura è data dalle novità introdotte dal Codice dei contratti pubblici D.Lgs. n. 36/2023 e dall'interazione dello stesso decreto con il D.Lgs. 231/2001.

Invero, tra le novità di maggior interesse per le imprese private apportate dal nuovo Codice degli appalti, vi è quella relativa alle causa di esclusione automatica di un operatore economico dalla procedura (art. 94), senza alcun margine valutativo per la stazione appaltante, relativa alla condanna (per l'ente, nel procedimento 231, o per un esponente aziendale, in sede penale) per una serie di reati, tra i quali: associazione per delinquere, associazione di stampo mafioso, associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope, contrabbando, traffico illecito di rifiuti, reati contro la pubblica amministrazione, turbata libertà degli incanti, frode nelle pubbliche forniture, false comunicazioni sociali, reati di terrorismo, reati di riciclaggio, sfruttamento del lavoro minorile, tratta di esseri umani e ogni altro reato da cui derivi la pena accessoria dell'incapacità di contrattare con la pubblica amministrazione.

Ancora, in ordine alle interazioni del nuovo Codice degli Appalti con il D.Lgs. n. 231/2001, le previsioni di cui sopra collegano espressamente l'esclusione degli operatori economici al sistema della responsabilità amministrativa degli enti ed in particolare:

• esclusione automatica nel caso di condanna dell'ente, ai sensi del D.Lgs. n. 231/2001, per uno dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti;

• esclusione automatica nel caso di condanna penale delle persone fisiche legate all'ente (art. 94, comma 3) per uno dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti;

• esclusione automatica degli enti già destinatari della sanzione interdittiva di cui all'art. 9, comma 2, lett. c), del D.Lgs. n. 231/2001 («*il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio*») o di altra sanzione che comporta il divieto di contrarre con la pubblica amministrazione (senza vincolo alcuno, in questo caso, all'elenco dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti);

• esclusione non automatica dell'ente di cui si accerti la commissione di un illecito professionale grave, desumibile – fra gli altri motivi – dalla commissione o dalla mera contestazione di un qualsiasi reato-presupposto di cui al D.Lgs. n. 231/2001.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RSPP	Responsabile del Servizio Prevenzione e Protezione
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC	Responsabile Tecnico
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale - Approvvigionamento
RFAM	Responsabile Facility Management
RPROG	Responsabile Progettazione
RATTR	Responsabile Attrezzature e Mezzi
GRPROG	Gruppo Progettisti
PROG	Programmatori
RSCM	Responsabile singola commessa

CDL Consulente del lavoro

REC Responsabile esterno contabilità

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

- Decreto Legislativo 231/2001 e s.s. mm.ii (di seguito anche D.Lgs 231/01);
- Codice Etico di IDRAGEST S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di IDRAGEST S.r.l.

4 CAMPO DI APPLICAZIONE RESPONSABILE DELLA PROCEDURA

La presente procedura si applica a tutti coloro i quali agiscono in nome e per conto della Società e la cui attività possa comportare la commissione dei reati di cui all'24-ter rubricato "*Delitti di criminalità organizzata*".

Le disposizioni della presente Parte Speciale hanno tutte le Funzioni Aziendali che agiscono in nome e per conto della Società affinché gli stessi adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi dei delitti ivi considerati.

NELLO SPECIFICO LA PRESENTE PARTE SPECIALE HA LO SCOPO DI:

a) indicare i principi che i destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, ed ai Responsabili delle funzioni aziendali che con lo stesso cooperano, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

Il principale responsabile della presente procedura è l'Organo Amministrativo.

5 I REATI DI CUI ALL'ART. 24-TER DEL DECRETO

L'art. 24 ter, d.lgs. 231/2001 prevede sanzioni pecuniarie ed interdittive per l'ente che si rende responsabile di uno degli illeciti dipendenti dai reati di criminalità organizzata.

Il reato di associazione per delinquere di cui all'art. 416 c.p. è un delitto di tipo associativo caratterizzato dalla concretizzazione di uno determinato e predefinito programma sociale criminale, caratterizzato dall'accordo tra più persone per formare una compagine stabile.

La fattispecie di cui all'art. 416 bis c.p. è invece un delitto contraddistinto dal controllo di settori di attività finanziarie ed economiche, di appalti e servizi pubblici, dal turbamento del libero esercizio del voto. È però possibile parlare di associazione di tipo mafioso, solo se l'attività criminale è caratterizzata dall'utilizzo della forza intimidatrice, mentre le vittime devono trovarsi in una condizione di assoggettamento e omertà nei confronti dell'organizzazione stessa in ragione dell'intimidazione da questa esercitata.

Ai fini dell'applicazione d.lgs. 231/2001, in ambito aziendale e societario, i reati presupposto in argomento vengono annoverati nell'ambito delle attività cd. sensibili ed astrattamente realizzabili, in via prioritaria, nell'ambito di attività di gestione e funzionamento del soggetto giuridico (sponsorizzazioni, gestione risorse umane, rapporti con i fornitori).

5.1. - ASSOCIAZIONE PER DELINQUERE (ART. 416 C.P.)

Ai sensi dell'art. 416 c.p. "*Quando tre o più persone si associano allo scopo di commettere più delitti, coloro che promuovono o costituiscono od organizzano l'associazione sono puniti, per ciò solo, con la reclusione da tre a sette anni. Per il solo fatto di partecipare all'associazione, la pena è della reclusione da uno a cinque anni.*

I capi soggiacciono alla stessa pena stabilita per i promotori. Se gli associati scorrono in armi le campagne o le pubbliche vie, si applica la reclusione da cinque a quindici anni. La pena è aumentata se il numero degli associati è di dieci o più.

Se l'associazione è diretta a commettere taluno dei delitti di cui agli articoli 600, 601, 601-bis e 602, nonché all'articolo 12, comma 3-bis, del testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero, di cui al decreto legislativo 25 luglio 1998, n. 286, nonché agli articoli 22, commi 3 e 4, e 22-bis, comma 1, della legge 1° aprile 1999, n. 91, si applica la reclusione da cinque a quindici anni nei casi previsti dal primo comma e da quattro a nove anni nei casi previsti dal secondo comma 2.

Se l'associazione è diretta a commettere taluno dei delitti previsti dagli articoli 600-bis, 600-ter, 600- quater, 600-quater.1, 600-quinquies, 609-bis, quando il fatto è commesso in danno di un minore di anni diciotto, 609-quater, 609-quinquies, 609-octies, quando il fatto è commesso in danno di un minore di anni diciotto, e 609-undecies, si applica la reclusione da quattro a otto anni nei casi previsti dal primo comma e la reclusione da due a sei anni nei casi previsti dal secondo comma".

Si tratta di una fattispecie che ha natura plurisoggettiva, essendo necessaria per la configurabilità del reato la partecipazione di almeno tre persone.

Elemento costitutivo dell'associazione è la formazione e permanenza di un vincolo associativo continuativo, al fine di commettere una serie indeterminata di delitti, con la predisposizione comune dei

mezzi occorrenti per la realizzazione del programma criminale e la permanente consapevolezza di ciascun consociato di far parte del sodalizio criminoso. Non è necessario che l'associazione costituisca un organismo formale e tragga origine da un regolare atto di costruzione, essendo indifferente la forma di organizzazione adottata.

Come si evince dal secondo comma, la sola partecipazione all'associazione, subordinata all'effettiva esistenza del vincolo associativo, integra il delitto in quanto elemento di per sé idoneo a mettere in pericolo, anche solo in maniera potenziale, l'ordine pubblico.

I consociati, pertanto, risponderanno sempre del delitto associativo in ragione della sola sussistenza del sodalizio a nulla rilevando la concreta commissione di altro reato di scopo, il quale potrà consistere in qualsiasi reato previsto nel codice penale.

Qualora dovesse essere realizzato taluno dei reati fine, ciascun correo risponderà anche di quest'ultimo in concorso formale con il delitto associativo, potendo altresì trovare applicazione l'istituto del reato continuato.

Il delitto, inoltre, si differenzia dal concorso eventuale di persone nel reato ai sensi dell'art. 110 c.p. in quanto si sostanzia in uno stabile apparato organizzativo, idoneo a essere nuovamente "utilizzato" anche in seguito all'eventuale commissione dei reati-scopo, mentre, nel caso del concorso di persone, il sodalizio criminoso ha natura occasionale ed è destinato a cessare una volta commessa la fattispecie concertata dai correi.

Non è esclusa, invece, la possibilità che si configuri il c.d. "concorso esterno" nel delitto associativo, il quale troverà applicazione ove l'agente, pur non partecipando all'associazione stessa, si limiti a fornire un contributo cosciente, volontario e riconducibile - sotto il profilo causale - a un apporto concreto volto a favorire le attività e gli scopi del sodalizio.

Il carattere stabile del vincolo associativo conferisce al reato in esame carattere permanente e si consuma nel luogo e nel momento di costituzione del vincolo associativo diretto allo scopo comune.

Il comma sesto rappresenta un'ipotesi associativa sorretta dal dolo specifico del fine di commettere uno o più delitti tra quelli elencati.

5.2. – ASSOCIAZIONE DI TIPO MAFIOSO ANCHE STRANIERA (ART. 416-BIS C.P.)

Ai sensi dell'art. 416-bis c.p. "*Chiunque fa parte di un'associazione di tipo mafioso formata da tre o più persone, è punito con la reclusione da dieci a quindici anni.*

Coloro che promuovono, dirigono o organizzano l'associazione sono puniti, per ciò solo, con la reclusione da dodici a diciotto anni.

L'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

Se l'associazione è armata si applica la pena della reclusione da dodici a venti anni nei casi previsti dal primo comma e da quindici a ventisei anni nei casi previsti dal secondo comma.

L'associazione si considera armata quando i partecipanti hanno la disponibilità, per il conseguimento della finalità dell'associazione, di armi o materie esplodenti, anche se occultate o tenute in luogo di deposito.

Se le attività economiche di cui gli associati intendono assumere o mantenere il controllo sono finanziate in tutto o in parte con il prezzo, il prodotto, o il profitto di delitti, le pene stabilite nei commi precedenti sono aumentate da un terzo alla metà.

Nei confronti del condannato è sempre obbligatoria la confisca delle cose che servirono o furono destinate a commettere il reato e delle cose che ne sono il prezzo, il prodotto, il profitto o che ne costituiscono l'impiego.

Le disposizioni del presente articolo si applicano anche alla camorra, alla 'ndrangheta e alle altre associazioni, comunque localmente denominate, anche straniere, che valendosi della forza intimidatrice del vincolo associativo perseguono scopi corrispondenti a quelli delle associazioni di tipo mafioso."

La norma in esame rappresenta una speciale ipotesi di delitto associativo introdotta al fine di contrastare con uno strumento *ad hoc* il fenomeno della criminalità di stampo mafioso, per la cui integrazione devono concorrere ulteriori e specifici requisiti.

Il delitto in esame si distingue dal precedente per l'eterogeneità degli scopi che l'associazione mira a realizzare e per il ricorso alla forza di intimidazione nel conseguimento dei fini propri dell'associazione stessa, pertanto, la tipicità della norma risiede nelle modalità attraverso cui l'associazione si manifesta concretamente.

I membri dell'associazione ex art. 416-bis c.p. si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva. Con riferimento alla forza di intimidazione è utile precisare che questa deriva non dal singolo affiliato, ma dall'associazione stessa quale timore che il sodalizio è in grado di incutere.

La condizione di assoggettamento e di omertà ha una funzione tipizzante rispetto alla forza di intimidazione, in particolare, il requisito dell'assoggettamento viene inteso come sottomissione, mentre quello di omertà come reticenza e rifiuto di collaborare con gli organi dello Stato per timore di rappresaglie da parte dell'associazione.

Occorre inoltre specificare che l'elemento del c.d. metodo mafioso, oltre a differenziare il reato in esame dal delitto generale di cui all'art. 416 c.p., qualifica le ulteriori forme di delinquenza organizzata che, pur non rientrando nelle associazioni tipicamente conosciute come la camorra o la 'ndrangheta, sono alle stesse accumunate ove si avvalgano del medesimo modus operandi per perseguire i propri scopi illeciti.

Si sottolinea ancora la maggiore ampiezza degli scopi riferibili all'associazione di tipo mafioso rispetto all'associazione prevista dall'art. 416 c.p., le finalità indicate dall'art. 416-bis c.p. sono tassative e alternative tra loro: commettere delitti, acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni, di autorizzazioni, appalti e servizi pubblici o realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali.

Infine, come per il delitto di cui all'art. 416 c.p., è configurabile il concorso esterno nella fattispecie associativa di stampo mafioso.

5.3. – SCAMBIO ELETTORALE POLITICO MAFIOSO (ART. 416-TER C.P.)

L'articolo prevede "*Chiunque accetta la promessa di procurare voti mediante le modalità di cui al terzo comma dell'articolo 416-bis in cambio dell'erogazione o della promessa di erogazione di denaro o di altra utilità è punito con la reclusione da sei a dodici anni. La stessa pena si applica a chi promette di procurare voti con le modalità di cui al primo comma.*"

La disposizione attribuisce penale rilevanza al fatto stesso dell'accordo tra il politico e colui che promette di procacciare i voti mediante modalità mafiose, ritenendo irrilevanti le successive condotte esecutive del patto stesso.

Si tratta di reato comune: sia con riferimento al soggetto del promissario, sia con riferimento a quello del promittente. Il promissario può essere lo stesso candidato in cerca di voti, ovvero un suo collaboratore o, più in generale, un qualsiasi soggetto che agisca per conto o anche solo nell'interesse del politico; dal canto suo, il promittente può essere un esponente di una cosca mafiosa, un mafioso agente *uti singulus,* oppure ancora un soggetto del tutto estraneo a una tale consorteria criminale.

Perché il reato possa dirsi integrato bisogna quindi accertare che il politico, o chi per lui, accetti la promessa di un suo interlocutore di procurargli, in cambio di denaro o di altra utilità, un certo numero di voti grazie al possibile ricorso, con modi espliciti o anche solo impliciti, alla forza di intimidazione di cui egli gode in ragione dell'appartenenza a un sodalizio mafioso.

5.4. - SEQUESTRO DI PERSONA A SCOPO DI ESTORSIONE (ART. 630 C.P.)

Ai sensi della norma in commento "*Chiunque sequestra una persona allo scopo di conseguire, per sé o per altri, un ingiusto profitto come prezzo della liberazione, è punito con la reclusione da venticinque a trenta.*

Se dal sequestro deriva comunque la morte, quale conseguenza non voluta dal reo, della persona sequestrata, il colpevole è punito con la reclusione di anni trenta. Se il colpevole cagiona la morte del sequestrato si applica la pena dell'ergastolo.

Al concorrente che, dissociandosi dagli altri, si adopera in modo che il soggetto passivo riacquisti la libertà, senza che tale risultato sia conseguenza del prezzo della liberazione, si applicano le pene previste dall'articolo 605. Se tuttavia il soggetto passivo muore, in conseguenza del sequestro, dopo la liberazione, la pena è della reclusione da sei a quindici anni.

Nei confronti del concorrente che, dissociandosi dagli altri, si adopera, al di fuori del caso previsto dal comma precedente, per evitare che l'attività delittuosa sia portata a conseguenze ulteriori ovvero aiuta concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di prove decisive per l'individuazione o la cattura dei concorrenti, la pena dell'ergastolo è sostituita da quella della reclusione da dodici a venti anni e le altre pene sono diminuite da un terzo a due terzi.

Quando ricorre una circostanza attenuante, alla pena prevista dal secondo comma è sostituita la reclusione da venti a ventiquattro anni; alla pena prevista dal terzo comma è sostituita la reclusione da ventiquattro a trenta anni. Se concorrono più circostanze attenuanti, la pena da applicare per effetto delle diminuzioni non può essere inferiore a dieci anni, nell'ipotesi prevista dal secondo comma, ed a quindici anni, nell'ipotesi prevista dal terzo comma.

I limiti di pena preveduti nel comma precedente possono essere superati allorché ricorrono le circostanze attenuanti di cui al quinto comma del presente articolo".

L'articolo è posto a tutela di un duplice interesse: quello della inviolabilità del patrimonio e quello della salvaguardia della libertà personale, in quanto nel delitto in questione la persona umana è strumentalizzata e oggetto di mercificazione. Il fatto tipico consiste nella privazione dell'altrui libertà personale e gli elementi costitutivi della fattispecie si realizzano non appena l'agente priva la vittima della libertà personale al fine di ottenere il prezzo della sua liberazione, non occorre – per la sussistenza del delitto – che sia richiesto anche il pagamento del riscatto.

L'elemento psicologico è il dolo specifico, che consiste nel fine dell'agente di conseguire con la sua condotta un ingiusto profitto (tale intendendosi qualsiasi vantaggio, non solo di tipo economico) che deve porsi in relazione finalistica rispetto alla liberazione della vittima.

5.5. - TRATTAMENTO SANZIONATORIO PER LE FATTISPECIE DI CUI ALL'ART. 24-TER DEL DECRETO

1. In relazione alla commissione di taluno dei delitti di cui agli articoli 416, sesto comma, 416-bis, 416-ter e 630 del codice penale, ai delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonchè ai delitti previsti dall'articolo 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, si applica la sanzione pecuniaria da quattrocento a mille quote.

2. In relazione alla commissione di taluno dei delitti di cui all'articolo 416 del codice penale, ad esclusione del sesto comma, ovvero di cui all'articolo 407, comma 2, lettera a), numero 5), del codice di procedura penale, si applica la sanzione pecuniaria da trecento a ottocento quote.

3. Nei casi di condanna per uno dei delitti indicati nei superiori punti 1 e 2, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2 del Decreto, per una durata non inferiore ad un anno.

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

6. – ATTIVITA' SENSIBILI A RISCHIO REATO ED I PRESIDI DI CONTROLLO

I reati sopra considerati trovano come presupposto l'instaurazione di rapporti a qualsiasi titolo, anche in forma indiretta, ovvero, con modalità transnazionale, con soggetti esterni all'ente che facciano parte di associazione criminose.

Al riguardo, è opportuno evidenziare che tali reati possono essere astrattamente commessi da tutti gli esponenti aziendali che abbiano contatti con soggetti esterni a qualsiasi titolo, in Italia o all'estero. Per converso, la strumentalizzazione della Società per finalità prevalentemente o esclusivamente illecite è suscettibile di essere realizzata principalmente da soggetti apicali, i soli in grado di modificare in modo così radicale l'oggetto sociale.

Con specifico riferimento al reato di associazione per delinquere di cui all'art. 416 c.p., occorre sottolineare che gli elementi costitutivi tipici del reato si fondano sulla stabilità del vincolo associativo,

desumibile da un certo livello di organizzazione dell'associazione e dal perseguimento di una finalità associativa consistente nella realizzazione di un programma delittuoso generico, di commettere cioè una serie indeterminata di delitti.

Sullo specifico punto, è intervenuta la Suprema Corte circoscrivendo l'operatività dell'art. 24-ter, negando la possibilità di recuperare indirettamente i delitti-scopo del reato associativo; a ragionare diversamente, infatti, "*la norma incriminatrice di cui all'art. 416 c.p. si trasformerebbe, in violazione del principio di tassatività del sistema sanzionatorio contemplato dal D. Lgs. n. 231 del 2001, in una disposizione "aperta", dal contenuto elastico, potenzialmente idoneo a ricomprendere nel novero dei reati-presupposto qualsiasi fattispecie di reato, con il pericolo di un'ingiustificata dilatazione dell'area di potenziale responsabilità dell'ente collettivo, i cui organi direttivi, peraltro, verrebbero in tal modo costretti ad adottare su basi di assoluta incertezza e nella totale assenza di oggettivi criteri di riferimento, i modelli di organizzazione e di gestione previsti dal citato D. Lgs., art. 6, scomparendone, di fatto, ogni efficacia in relazione agli auspicati fini di prevenzione*" (Cassazione penale, Sez. VI, 20 dicembre 2013, n. 3635).

Ebbene, esclusa la possibilità di immaginare nel caso della Società e, più in generale, di ogni impresa lecita, la realizzazione della condotta di costituzione di una associazione a ciò finalizzata, si tratta di vagliare il rischio che la struttura organizzativa societaria sia utilizzata da più persone al fine di realizzare una serie di delitti nell'interesse o a vantaggio della Società stessa; ipotesi che la giurisprudenza spesso riconduce alla figura dell'art. 416 c.p., piuttosto che al mero concorso di persone in più reati.

In quest'ottica, è evidente come il rischio che ciò accada non sia individuabile *ex ante* da parte della Società, ma si leghi a un fenomeno di devianza dipendente dalle determinazioni di alcuni suoi membri, nel caso in cui decidano di sfruttare l'organizzazione di persone e di mezzi, tipica di ogni impresa, per fini criminali.

Invero, con riferimento a tali reati, i principali processi sensibili ritenuti più specificatamente a rischio, in ambito IDRAGEST, sono i seguenti:

- ✓ Acquisti di beni e servizi;
- ✓ Affidamenti di incarichi di consulenza;
- ✓ Gestione dei flussi finanziari;
- ✓ Selezione, assunzione e gestione del personale;
- ✓ Partecipazione e gestione delle gare.

Le misure preventive immaginabili sono legate, in primo luogo, alla diffusione più ampia possibile della filosofia di impresa perseguita dalla Società, ribadendo a chiunque operi al suo interno che il

perseguimento di vantaggi per la Società, ottenuti attraverso il compimento di attività penalmente vietate, non è mai consentito e che la Società adotterà ogni misura, anche radicale, ritenuta utile a garantire immediatamente in quel settore organizzativo la situazione di legalità e trasparenza, nell'ipotesi in cui emerga il fondato sospetto che soggetti operanti nella Società siano dediti alla commissione di fatti delittuosi, seppure a vantaggio della Società stessa.

Tuttavia, al solo fine di scongiurare il pur remoto rischio che per la devianza di singoli soggetti operanti all'interno della Società, si possano in qualche modo agevolare dall'esterno, mediante il perfezionamento di rapporti contrattuali, organizzazioni di tipo criminale, si è ritenuto utile richiamare i principi di base e le regole della libera concorrenza - che hanno, peraltro, ispirato da sempre la filosofia di impresa della Società – per esigerne il rispetto.

Poiché i delitti di criminalità organizzata possono essere finalizzati anche alla commissione dei reati già analizzati nelle singole Parti Speciali, si ritiene opportuno specificare che le aree a rischio sopra menzionate devono intendersi integrate con le altre specificatamente individuate in relazione a ciascuna fattispecie oggetto di trattazione nelle altre Parti Speciali del presente Modello.

Tale precisazione si ritiene necessaria per ragioni strettamente legate alla formazione di un Modello quanto più efficace e in linea con il dettato normativo del Decreto.

In considerazione di tale natura peculiare dei reati associativi, non si ritiene possibile localizzare a specifiche aree aziendali il rischio della loro commissione.

LA PRESENTE PARTE SPECIALE HA LA FUNZIONE DI:

- fornire un elenco dei principi cui i destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandato.

Tali regole di condotta si applicano a tutti i destinatari del Modello e, in particolare, ai soggetti esterni alla Società, nonché a tutti coloro che svolgono le proprie mansioni nelle aree di rischio segnalate nel paragrafo che precede e in quelle delle altre Parti Speciali.

Occorre preliminarmente evidenziare che, in tutte le aree "a rischio reato" qui considerate, occorre osservare i seguenti Presidi di Controllo Generali (a cui si aggiungono Presidi di Controllo Specifici in relazione a singole attività sensibili o categorie di attività sensibili):

1) rispetto del Codice Etico;

2) formazione in ordine al Modello e alle tematiche di cui al D. Lgs. n. 231/2001, rivolta alle risorse operanti nell'ambito delle aree a rischio, con modalità di formazione appositamente pianificate in considerazione del ruolo svolto;

3) diffusione del Modello tra le risorse aziendali, mediante consegna di copia su supporto documentale o telematico e pubblicazione del Modello e dei protocolli maggiormente significativi (ad es., Codice Etico, Sistema Disciplinare, Procedure rilevanti, ecc.) sulla intranet della Società;

4) diffusione del Modello tra i Terzi Destinatari tenuti al rispetto delle relative previsioni (ad es., fornitori, appaltatori, consulenti) mediante pubblicazione dello stesso sul sito intranet della Società o messa a disposizione in formato cartaceo o telematico;

5) dichiarazione con cui i Destinatari del Modello, inclusi i Terzi Destinatari si impegnano a rispettare le previsioni del Decreto;

6) previsione e attuazione del Sistema Disciplinare volto a sanzionare la violazione del Modello e dei Protocolli ad esso connessi;

7) acquisizione di una dichiarazione, sottoscritta da ciascun destinatario del Modello della Società, di impegno al rispetto dello stesso, incluso il Codice Etico;

8) implementazione di un sistema di dichiarazioni periodiche (almeno semestrali) da parte dei Responsabili Interni con le quali si fornisce evidenza del rispetto e/o della inosservanza del Modello (o, ancora di circostanze che possono influire sull'adeguatezza ed effettività del Modello);

9) creazione di una "Sezione 231" all'interno della intranet aziendale, presso cui pubblicare tutti i documenti rilevanti nell'ambito del Modello della Società (ad es., Modello, Codice Etico, Protocolli aziendali in esso richiamati);

10) rispetto dell'organigramma aziendale.

Inoltre, si intendono qui richiamati i presidi di controllo adottati nelle altre Parti Speciali del Modello, in ragione del pericolo di commistione delle fattispecie di reato trattate, unitamente al fenomeno della criminalità organizzata.

Infine, l'Organo amministrativo della Società potrà prevedere ulteriori misure a maggiore tutela delle aree di rischio individuate e a integrazione dei comportamenti sopra elencati.

AREA A RISCHIO N. 1: ADEMPIMENTI IN MATERIA DI PERSONALE

ATTIVITÀ SENSIBILI:

A) GESTIONE DEL PROCESSO DI SELEZIONE, VALUTAZIONE, SCELTA E GESTIONE DEI CANDIDATI.

La selezione, assunzione e gestione del personale è tra le aree più sensibili al rischio di criminalità organizzata, poiché le condotte di associazione per delinquere o associazione di tipo mafioso potrebbero concretizzarsi, quantomeno nelle forme del concorso esterno, in un sistema di reclutamento del personale imposto o caldeggiato da gruppi criminali attraverso un sodalizio criminoso tra soggetti apicali, risorse umane ed esponenti della criminalità organizzata, in cambio di altri vantaggi illeciti conseguibili dalla società.

Reati ipotizzabili:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).

ULTERIORI PRESIDI DI CONTROLLO:

1) osservanza delle procedure e dei principi applicativi per la selezione e per la gestione del personale;

2) divieto per tutti i destinatari e collaboratori esterni alla Società - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di delitti di criminalità organizzata;

3) in relazione alle procedure per la selezione del personale i Destinatati sono tenuti ad applicare i seguenti criteri per scelta:

• professionalità rispetto all'incarico o le mansioni da ricoprire;

• parità di trattamento;

• esibizione del casellario giudiziario e dei carichi pendenti;

• assunzione di informazioni sulla professionalità, sulle competenze e sui ruoli precedentemente ricoperti dalla risorsa;

4) obbligo, per coloro che ricoprono posizioni apicali, limitatamente alle funzioni a loro affidate, di:

• non sottostare a qualsivoglia richiesta contraria alla legge o ai precetti contenuti nel presente Modello;

• informare tempestivamente l'Organo Amministrativo e l'Autorità Giudiziaria ove vengano a conoscenza di fatti o eventi che possano favorire infiltrazioni della criminalità organizzata, ovvero se sottoposti a ricatti o minacce, avvertendo altresì le Autorità competenti.

In ultimo, al fine di prevenire la commissione dei delitti di criminalità organizzata nella selezione, assunzione e gestione del personale, è necessario adottare i seguenti ed ulteriori presidi di controllo:

1. Esistenza di un'idonea segregazione di ruoli e funzioni coinvolti nel sistema di selezione del personale, alfine di assicurare un efficiente sistema di controlli e differenziazione tra chi segnala la necessità di assumere personale, chi seleziona il candidato, chi lo esamina e chi decide di assumerlo.

2. La selezione del personale deve essere effettuata sulla base di criteri selettivi che garantiscono la trasparenza della scelta e che prendono in considerazione la professionalità, le competenze e l'affidabilità del candidato dal rischio di infiltrazione criminale dello stesso

AREA A RISCHIO N. 2: STIPULA E GESTIONE DI CONTRATTI

ATTIVITÀ SENSIBILI:

a) gestione dei contratti di consulenza e di prestazione professionale;

b) gestione dell'anagrafica Consulenti;

c) selezione dei consulenti;

d) gestione degli acquisti e monitoraggio dei beni/servizi ricevuti.

Reati ipotizzabili:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).

ULTERIORI PRESIDI DI CONTROLLO:

1) osservanza delle procedure e dei principi applicativi per la selezione dei consulenti, dei fornitori, di partners o altri professionisti con cui la Società intenda intrattenere rapporti lavorativi;

2) divieto per tutti i destinatari e per i collaboratori esterni alla Società - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di delitti di criminalità organizzata;

3) in relazione alle procedure per la selezione di eventuali partners e/o fornitori e/o consulenti i Destinatati sono tenuti ad applicare i seguenti criteri per scelta:

• professionalità rispetto all'incarico o le mansioni da ricoprire;

• parità di trattamento;

• assunzione di informazioni sulla professionalità, sulle competenze e sui ruoli precedentemente ricoperti dalla risorsa.

4) con riferimento alla gestione di rapporti economici con i consulenti e/o altri partners esterni è imposto di:

• utilizzare specifici conti correnti bancari e/o postali sui quali effettuare i relativi pagamenti;

• imporre, quale unico metodo di pagamento, lo strumento del bonifico bancario o postale, nonché qualsiasi altro metodo che assicuri la piena tracciabilità;

5) obbligo per coloro che ricoprono posizioni apicali, limitatamente alle funzioni a loro affidate di:

• non sottostare a qualsivoglia richiesta contraria alla legge o ai precetti contenuti nel presente Modello;

• informare tempestivamente l'Organo Amministrativo e l'Autorità Giudiziaria ove vengano a conoscenza di fatti o eventi che possano favorire infiltrazioni della criminalità organizzata, ovvero se sottoposti a ricatti o minacce, avvertendo altresì le Autorità competenti;

6) creazione dell'anagrafica Consulenti, nella quale inserire i consulenti della Società, assicurandone la previa qualificazione mediante l'accertamento dei requisiti di professionalità ed onorabilità;

7) formalizzazione dei requisiti da richiedere ai consulenti e dei criteri da utilizzare nella relativa selezione, nonché delle ragioni che giustificano eventuali deroghe dai requisiti e criteri suddetti;

8) individuazione delle risorse deputate: a) a selezionare i potenziali nuovi consulenti b) a formalizzare l'accordo negoziale; c) a gestire l'anagrafica Consulenti; d) a gestire i pagamenti delle fatture emesse dai consulenti;

9) richiesta, ove possibile, di almeno due preventivi in sede di selezione dei consulenti;

10) archiviazione della documentazione inviata dai potenziali candidati e concernente il rispetto dei requisiti richiesti;

11) inserimento negli accordi con i consulenti di una clausola volta ad assicurare il rispetto del Modello e del Codice Etico della Società.

AREA A RISCHIO N. 3: CONTABILITÀ

ATTIVITÀ SENSIBILI:

a) contabilità generale, bilancio e altre comunicazioni sociali;

ULTERIORI PRESIDI DI CONTROLLO:

1) osservanza delle procedure e dei principi applicativi aziendali;

2) divieto per tutti i Destinatari e per i collaboratori esterni alla Società - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di delitti di criminalità organizzata;

3) obbligo per coloro che ricoprono posizioni apicali, limitatamente alle funzioni a loro affidate di:

• non sottostare a qualsivoglia richiesta contraria alla legge o ai precetti contenuti nel presente Modello;

• informare tempestivamente l'Organo Amministrativo e l'Autorità Giudiziaria ove vengano a conoscenza di fatti o eventi che possano favorire infiltrazioni della criminalità organizzata, ovvero se sottoposti a ricatti o minacce, avvertendo altresì le Autorità competenti.

AREA A RISCHIO N. 4: APPROVVIGIONAMENTO

ATTIVITÀ SENSIBILI:

a) approvvigionamento di beni, lavori e servizi;

b) selezione e scelta di fornitori e di vettori con cui intrattenere rapporti di natura contrattuale;

c) individuazione dei partners con cui la Società decida di intrattenere rapporti professionali per lo svolgimento della sua attività.

Reati ipotizzabili:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).

ULTERIORI PRESIDI DI CONTROLLO:

1) osservanza delle procedure e dei principi applicativi per la selezione dei consulenti, dei fornitori, di partners o altri professionisti con cui la Società intenda intrattenere rapporti lavorativi;

2) divieto per tutti i Destinatari e per i collaboratori esterni alla Società - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di delitti di criminalità organizzata;

3) in relazione alle procedure per la selezione di eventuali partners e/o fornitori e/o consulenti i Destinatati sono tenuti ad applicare i seguenti criteri per scelta:

• professionalità rispetto all'incarico o le mansioni da ricoprire;

• parità di trattamento;

• assunzione di informazioni sulla professionalità, sulle competenze e sui ruoli precedentemente ricoperti dalla risorsa.

4) con riferimento alla gestione di rapporti economici con i consulenti, e/o altri partners esterni è imposto di:

• utilizzare specifici conti correnti bancari e/o postali sui quali effettuare i relativi pagamenti;

• imporre, quale unico metodo di pagamento, lo strumento del bonifico bancario o postale, nonché qualsiasi altro metodo che assicuri la piena tracciabilità;

5) obbligo per coloro che ricoprono posizioni apicali, limitatamente alle funzioni a loro affidate di:

• non sottostare a qualsivoglia richiesta contraria alla legge o ai precetti contenuti nel presente Modello;

• informare tempestivamente l'Organo Amministrativo e l'Autorità Giudiziaria ove vengano a conoscenza di fatti o eventi che possano favorire infiltrazioni della criminalità organizzata, ovvero se sottoposti a ricatti o minacce, avvertendo altresì le Autorità competenti;

6) creazione dell'anagrafica Fornitori, nella quale inserire i fornitori della Società, assicurandone la previa qualificazione mediante l'accertamento dei requisiti di professionalità ed onorabilità;

7) formalizzazione dei requisiti da richiedere ai fornitori e dei criteri da utilizzare nella relativa selezione, nonché delle ragioni che giustificano eventuali deroghe dai requisiti e criteri suddetti;

8) individuazione delle risorse deputate: a) a selezionare i potenziali nuovi fornitori b) a formalizzare l'accordo negoziale; c) a gestire l'anagrafica Fornitori; d) a gestire i pagamenti delle fatture emesse dai fornitori;

9) richiesta, ove possibile, di almeno due preventivi in sede di selezione dei fornitori;

10) archiviazione della documentazione inviata dai potenziali candidati e concernente il rispetto dei requisiti richiesti;

11) sottoscrizione di un contratto con tutti i fornitori, con previsione, per quelli per i quali si prevede di procedere con l'Ordine di Acquisto, della previa consultazione ed accettazione delle proprie Condizioni Generali di Contratto;

12) inserimento nei contratti di fornitura di una clausola volta ad assicurare il rispetto del Modello e del Codice Etico della Società.

In ultimo, al fine di prevenire la commissione dei delitti di criminalità organizzata nella gestione degli acquisti di beni e servizi e per l'affidamento degli incarichi di consulenza, è necessario adottare i seguenti ed ulteriori presidi di controllo:

1. Definire i criteri qualitativi e quantitative di selezione dei fornitori;

2. Verificare, preventivamente, i requisiti di onorabilità e professionalità dei fornitori di beni e/o servizi, laddove si tratti di fornitori non già conosciuti da IDRAGEST e, dunque, non già fornitori della società;

3. Monitorare e aggiornare, periodicamente, i dati anagrafici e le coordinate bancarie di fornitori e consulenti e garantire la tracciabilità dei pagamenti anche relativamente a forniture/fatture occasionali;

4. Come su esposto, nei rinnovi e/o nei nuovi contratti con fornitori e consulenti deve essere contenuta un'apposita clausola con cui IDRAGEST informa gli stessi di avere adottato un Modello di Gestione

Organizzazione e Control lo ex D.Lgs n. 231/2001, chiedendo agli stessi di impegnarsi al rispetto del D.Lgs n. 231/2001.

AREA A RISCHIO N. 5: GESTIONE DEI FLUSSI FINANZIARI E DELLE SPONSORIZZAZIONI

ATTIVITÀ SENSIBILI:

A) gestione dei flussi finanziari;

B) gestione delle sponsorizzazioni, delle iniziative pubblicitarie e dei contributi ad associazioni ed Enti.

Reati ipotizzabili:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).

A) ULTERIORI PRESIDI DI CONTROLLO SULLA GESTIONE DEI FLUSSI FINANZIARI:

Al fine di prevenire la commissione dei delitti di criminalità organizzata nella gestione dei flussi finanziari, è necessario adottare i seguenti presidi di controllo:

1. Eseguire un controllo costante sull'effettività delle prestazioni rispetto alle fatture emesse;

2. Eseguire un controllo costante sulla veridicità delle dichiarazioni rispetto alle scritture contabili;

3. Eseguire un controllo costante che eventuali operazioni di investimento o sponsorizzazione siano preventivamente vagliate secondo modalità concrete di verifica della congruità economica e degli scopi.

B) ULTERIORI PRESIDI DI CONTROLLO SULLA GESTIONE DELLE SPONSORIZZAZIONI:

1) divieto per tutti i destinatari e per i collaboratori esterni alla Società - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di delitti di criminalità organizzata;

2) obbligo per coloro che ricoprono posizioni apicali, limitatamente alle funzioni a loro affidate di:

• non sottostare a qualsivoglia richiesta contraria alla legge o ai precetti contenuti nel presente Modello;

• informare tempestivamente l'Organo Amministrativo e l'Autorità Giudiziaria ove vengano a conoscenza di fatti o eventi che possano favorire infiltrazioni della criminalità organizzata, ovvero se sottoposti a ricatti o minacce, avvertendo altresì le Autorità competenti;

3) possibilità di sponsorizzare unicamente eventi o associazioni di comprovata affidabilità, con divieto di sponsorizzare eventi o associazioni riconducibili, direttamente o indirettamente, a PU o IPS che siano entrati in contatto (o che possano ragionevolmente entrare in contatto) con la Società per ragioni del loro ufficio (ad es., per il rilascio di una licenza o permesso).

AREA A RISCHIO N. 6: GESTIONE DEI SERVIZI FORNITI DALLA SOCIETÀ

ATTIVITÀ SENSIBILI:

a) gestione della clientela;

b) rapporti con eventuali intermediari, procacciatori di affari e simili;

c) offerta dei servizi forniti dalla Società.

Reati ipotizzabili:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).

ULTERIORI PRESIDI (SPECIFICI) DI CONTROLLO:

Poiché i delitti di criminalità organizzata possono essere finalizzati anche alla commissione dei reati già analizzati nelle singole Parti Speciali, si ritiene opportuno specificare che le aree a rischio sopra menzionate andranno integrate con le altre precedentemente individuate in relazione a ciascuna fattispecie oggetto di trattazione nelle altre Parti del presente Modello.

Tale precisazione si ritiene necessaria per ragioni strettamente legate alla formazione di un Modello quanto più efficace e in linea con il dettato normativo del Decreto.

Le aree indicate assumono rilevanza anche nell'ipotesi in cui le attività sopra elencate siano eseguite, in tutto o in parte, da persone fisiche o giuridiche in nome o per conto della Società, in virtù di apposite deleghe o per la sottoscrizione di specifici rapporti contrattuali, dei quali deve essere tempestivamente informato l'OdV.

7 PRINCIPI GENERALI DI COMPORTAMENTO E REGOLE DI CONDOTTA

I Destinatari del Modello sono tenuti ad osservare, nella fattispecie delle attività sensibili individuate nella presente procedura, nonché nella sfera dei rapporti con ogni stackeholder esterno, le seguenti regole di condotta:

- Garantire il rispetto dello Statuto e delle norme di legge applicabili nelle operazioni societarie;
- Interdire l'ingresso nella compagine societaria di soggetti (sia essi persone fisiche che giuridiche) dei quali sia conosciuta o sospetta l'appartenenza ad operazioni criminali o comunque operanti al di fuori della liceità quali, a titolo meramente esemplificativo ma non esaustivo, persone legate alla camorra, alla mafia, al traffico di sostanze stupefacenti, all'usura, al riciclaggio ecc.;

- Non utilizzare strumenti e conti anonimi o contanti per il compimento di operazioni di trasferimento di importi rilevanti;
- Rispettare tutti i requisiti relativi alla selezione dei fornitori, con particolare attenzione all'incensuratezza degli stessi e alla valutazione preventiva in ordine congruità dei prezzi richiesti rispetto ai valori di mercato
- Divieto di prestare qualsivoglia forma di collaborazione o anche solo semplice contatto con soggetti colpiti o indiziati da provvedimenti giudiziari legati alla criminalità organizzata;
- Divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti effettivi e/o potenziali che possano, in maniera diretta ed indiretta, favorire le condizioni per reati di criminalità organizzata;
- Divieto di porre in essere qualsiasi situazione e/o tenere qualsiasi comportamento in conflitto di interessi con la Pubblica Sicurezza;

IN PARTICOLARE È FATTO DIVIETO DI:

- Promuovere, costituire, organizzare, dirigere partecipare ovvero finanziare in alcuna forma le associazioni di cui agli artt. 416 e 416 bis c.p.;
- Effettuare donazioni o altra forma di erogazione di fondi, anche indirette, nei confronti di simili associazioni;
- Fornire supporto logistico e/o qualsivoglia altro tipo a persone che partecipano alle predette associazioni;
- Stipulare qualsiasi tipo di contratto o avere rapporti commerciali, di collaborazione o di diverso tipo con controparti che abbiano precedenti penali o carichi pendenti noti alla Società in materia di reati di criminalità organizzata, ovvero dei quali si presume il vincolo associativo e la finalità criminale, anche se non si ha la certezza tanto del vincolo quanto dello scopo illecito, purchè si disponga di elementi sufficienti a farne desumere l'esistenza e ciononostante non si desista dall'instaurazione dei predetti rapporti.

8 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, mettendo a disposizione dell'Organismo di Vigilanza – in un archivio digitale all'uopo preposto su apposita piattaforma informatica – tutta la documentazione necessaria.

L'Organismo di Vigilanza può effettuare periodicamente controlli a campione sulle attività connesse ai Processi Sensibili, al fine di verificare la corretta esplicazione delle stesse in relazione alle regole di cui al Modello.

A tal fine, all'Organismo di Vigilanza vengono garantiti autonomi poteri di iniziativa e controllo nonchè garantito libero accesso a tutta la documentazione aziendale rilevante.

L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute.

L'ODV DOVRÀ EFFETTUARE:

• il monitoraggio dell'efficacia delle procedure interne e delle regole di *corporate governance* per la prevenzione dei reati che la presente procedura è finalizzata a prevenire;

• l'esame d'eventuali segnalazioni provenienti dagli organi di controllo o da qualsiasi dipendente e disposizione degli accertamenti ritenuti necessari.

I dettagli in merito al contenuto ed alle modalità di comunicazione delle informazioni e segnalazioni verso l'Organismo di Vigilanza sono precisati nelle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e "Procedura di gestione del whistleblowing" cui si rimanda.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2023	ADOZIONE
Rev. 1	CDA DEL 9.05.2023	AGGIORNAMENTO
Rev. 2	CDA DEL 3.11.2023	AGGIORNAMENTO
Rev. 3	CDA DEL 01.08.2024	AGGIORNAMENTO
Rev. 4	CDA DEL 28.10.2024	AGGIORNAMENTO
Rev. 5	CDA DEL 9.07.2025	AGGIORNAMENTO
Rev. 6	CDA DEL 14.10.2025	AGGIORNAMENTO
Rev. 7	CDA DEL 22.07.2026	AGGIORNAMENTO

SOMMARIO

1 PREMESSA, SCOPO E FINALITA' 4

2 ACRONIMI AZIENDALI 5

3 RIFERIMENTI NORMATIVI 6

4 DESTINATARI DELLA PROCEDURA 6

5 I REATI CORRUTTIVI (ART. 25 e 25ter D.Lgs. 231/01) 7

6 PRINCIPI GENERALI DI COMPORTAMENTO 10

6.1 ALTRE CONDOTTE VIETATE 11

7. AREE SENSIBILI E PRESIDI DI CONTROLLO ANTICORRUZIONE 11

7.1 Rapporti con la Pubblica Amministrazione e altri Enti Pubblici 12

7.1.2. RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE PER L'OTTENIMENTO DI CONCESSIONI, LICENZE, AUTORIZZAZIONI E FINANZIAMENTI 12

7.2 Omaggi, Regalie, Spese di Rappresentanza e Sponsorizzazioni 14

7.3 Gestione delle Terze Parti (Fornitori, Consulenti, Partner) 14

7.4 Selezione del Personale e Prevenzione del "Pantouflage" 15

7.5 Conflitto di Interessi 15

7.6. Utilizzo di Sistemi di Intelligenza Artificiale 15

7.7. Trasparenza e Tracciabilità Contabile 15

7.7.1 PROCEDURE CONTABILI 16

8 RISORSE UMANE 16

9. COMUNICAZIONE E FORMAZIONE 17

10 VIOLAZIONI E PROVVEDIMENTI SANZIONATORI 18

10.1 AMBITO DI APPLICAZIONE 18

10.2 SANZIONI 19

11 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO 21

1 PREMESSA, SCOPO E FINALITA'

La presente Procedura per la Prevenzione della Corruzione (di seguito, "Procedura") formalizza l'impegno di IDRAGEST S.r.l. (di seguito, "Idragest" o la "Società") a condurre le proprie attività secondo i più elevati standard di integrità, onestà e trasparenza, in conformità con il principio di "tolleranza zero" verso qualsiasi forma di corruzione, sia essa attiva o passiva, pubblica o tra privati.

IDRAGEST, infatti, ripudia, coerentemente con i valori previsti nel proprio Codice Etico, ogni forma di corruzione, in quanto oltre ad essere un fenomeno illegale, rappresenta un ostacolo allo sviluppo sostenibile e altera la leale concorrenza, distruggendo, pertanto, la reputazione della società.

Pertanto, IDRAGEST, coerentemente con il principio di "zero tolleranza", vieta a tutti i Destinatari della presente Procedura (come i dipendenti, i lavoratori in somministrazione, i collaboratori e chiunque agisce in nome e per conto della società) ogni comportamento che possa facilitare o promuovere fenomeni corruttivi, dotandosi, per tale scopo, di un articolato sistema di regole, controlli e di presidi organizzativi volti alla prevenzione dei reati di corruzione.

Tale sistema, si basa sulle vigenti disposizioni normative nazionali e sovranazionali in materia di corruzione, tutte finalizzate a fissare gli strumenti di controllo che IDRAGEST mette a disposizione dei dipendenti, lavoratori in somministrazione, dei collaboratori e di tutti coloro che agiscono in nome e per conto della stessa, finalizzati a prevenire e contrastare il rischio di corruzione.

IDRAGEST, per assicurare il puntuale rispetto della presente Procedura, si impegna a svolgere attività di sensibilizzazione, formazione e aggiornamento periodico in materia, volte a fornire una chiara rappresentazione dei rischi di corruzione connessi alle attività di business della società, degli strumenti di prevenzione e contrasto che IDRAGEST ha adottato e attuato nel tempo e delle conseguenze che derivano dalla violazione di tali strumenti e delle disposizioni normative Anti-Corruzione. Inoltre, IDRAGEST si impegna a comunicare anche all'esterno (ovvero ai propri partner e ai terzi con i quali entra in relazione) i propri valori e principi etici, prevedendo nei relativi contratti adeguati impegni di compliance anti-corruzione e ciò anche allo scopo di promuovere e sensibilizzare tutti ad adottare delle misure finalizzate a prevenire il rischio della corruzione.

La presente Procedura, unitamente alla Politica Anti-corruzione adottata da IDRAGEST, rispecchia l'impegno puntuale e costante della Società finalizzato a contrastare i fenomeni corruttivi.

LE FINALITÀ DELLA PROCEDURA SONO:

1. Prevenire e contrastare la commissione dei reati di corruzione, concussione, traffico di influenze illecite e degli altri reati contro la Pubblica Amministrazione e tra privati rilevanti ai sensi del D.Lgs. 231/2001.
2. Garantire la piena conformità dell'operato aziendale alle normative anticorruzione applicabili.
3. Promuovere e diffondere una solida cultura dell'integrità e della legalità a tutti i livelli dell'organizzazione e nei rapporti con le terze parti.
4. Proteggere la reputazione, il patrimonio e la continuità operativa di Idragest, tutelandola dal rischio di applicazione delle sanzioni previste dal D.Lgs. 231/2001.

2 ACRONIMI AZIENDALI

CDA Consiglio di Amministrazione

PRES Presidente CDA

RSPP Responsabile del Servizio Prevenzione e Protezione

RSGQ Responsabile Sistema di Gestione Qualità

RTEC Responsabile Tecnico

RAM/RRU Responsabile Amministrazione - Risorse Umane

RCOM/APVG Responsabile Commerciale - Approvvigionamento

RFAM Responsabile Facility Management

RPROG Responsabile Progettazione

CDL Consulente del Lavoro

REC Responsabile Esterno Contabilità

RIA Responsabile IA

RIDC Responsabile interno di conformità

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

La presente Procedura è redatta in conformità al quadro normativo vigente e ai documenti interni che costituiscono i pilastri del sistema di controllo interno di IDRAGEST S.r.l. I principali riferimenti normativi ed organizzativi sono i seguenti:

- **D.LGS. 8 GIUGNO 2001, N. 231** e successive modifiche ed integrazioni, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*", con particolare riferimento all'art. 25 (Concussione, induzione indebita a dare o promettere utilità e corruzione) e all'art. 25-ter (Reati societari);
- **CODICE PENALE**, con specifico riferimento agli artt. 318 (Corruzione per l'esercizio della funzione), 319 (Corruzione per atto contrario ai doveri d'ufficio), 319-ter (Corruzione in atti giudiziari), 319-quater (Induzione indebita a dare o promettere utilità), 320 (Corruzione di persona incaricata di un pubblico servizio), 321 (Pene per il corruttore), 322 (Istigazione alla corruzione), 322-bis (Peculato, concussione, induzione indebita, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee), nonché all'art. 2635 c.c. (Corruzione tra privati) e all'art. 2635-bis c.c. (Istigazione alla corruzione tra privati);
- **CODICE ETICO DI IDRAGEST S.R.L.**, che definisce i valori fondamentali e i principi di condotta ai quali la Società improntа la propria attività nei confronti di tutti gli stakeholder;
- **MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO (MOG)** adottato dalla Società ai sensi del D.Lgs. 231/2001, quale strumento organizzativo volto a prevenire la commissione dei reati presupposto;
- **POLITICA ANTICORRUZIONE AZIENDALE**, che esplicita l'impegno della Società verso l'adozione di una politica di "zero tolleranza" rispetto a qualsiasi fenomeno corruttivo, sia nella dimensione pubblica che in quella privata;
- **D.LGS. 10 MARZO 2023, N. 24 (C.D. "DECRETO WHISTLEBLOWING");**
- **D.LGS. 31 MARZO 2023, N. 36 (NUOVO CODICE DEI CONTRATTI PUBBLICI).**

4 DESTINATARI DELLA PROCEDURA

La presente Procedura si applica a tutti coloro che agiscono in nome e per conto di IDRAGEST ed, in particolare ai componenti del Consiglio di Amministrazione e degli altri Organi Sociali, ai Dipendenti, ai lavoratori in somministrazione, ai collaboratori, ai consulenti, ai fornitori ed ai partner commerciali che, a qualsiasi titolo, operano in nome o per conto della Società. La presente Policy rappresenta, inoltre,

un'integrazione del Modello di Gestione Organizzazione e Controllo ex D.Lgs. n. 231/2001 adottato dalla Società, implementando in tal modo, unitamente ai principi contenuti nel Codice Etico, il sistema adottato da IDRAGEST per il contrasto dei fenomeni corruttivi.

5 I REATI CORRUTTIVI (ART. 25 E 25TER D.LGS. 231/01)

- **CONCUSSIONE (ART. 317 C.P.)**

Il reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

La concussione è un reato che può essere commesso solo da un soggetto agente che si qualifichi come esercente una pubblica funzione e si configura anche come un reato bilaterale, in quanto richiede la condotta di due distinti soggetti, il concussore e il concusso.

Nella fattispecie in esame solo il concussore è assoggettato a pena, in quanto il concusso è la vittima del reato.

- **CORRUZIONE PER UN ATTO D'UFFICIO O CONTRARIO AI DOVERI DI UFFICIO (ART. 318 - 319 E ART. 319-BIS C.P.)**

L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale per compiere un atto del suo ufficio riceve per sé o per altri in denaro o altra utilità, una retribuzione che non gli è dovuta o ne accetta la promessa.

L'art. 319 c.p. punisce il pubblico ufficiale che, per omettere o ritardare un atto del suo ufficio, ovvero per compiere o aver compiuto un atto contrario ai propri doveri d'ufficio, riceve per sé o per altri denaro o altra utilità o ne accetta la promessa.

L'art. 319-bis c.p. dispone un aumento di pena se il fatto della corruzione ha per oggetto il conferimento di pubblici impieghi, stipendi, pensione o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

La condotta del pubblico ufficiale potrà quindi estrinsecarsi nel compimento sia di un atto dovuto sia di un atto contrario ai propri doveri. Tali disposizioni valgono anche per l'incaricato di un pubblico servizio che rivesta la qualità di pubblico impiegato (art. 320 c.p.), oltre che per le persone indicate nell'art. 322-bis c.p.

Si ritiene opportuno, dal momento che il confine fra corruzione e concussione non è facilmente individuabile, riportare la differenza elaborata dalla giurisprudenza, la quale si fonda sul diverso

modo di rapportarsi del privato nei confronti del pubblico ufficiale: nella corruzione il privato e il pubblico ufficiale agiscono su un piano di parità, mentre nella concussione emerge una disparità, in cui il privato subisce le pressioni del pubblico ufficiale.

- **CORRUZIONE IN ATTI GIUDIZIARI (ART. 319-TER C.P.)**

Il reato si configura nel caso in cui i fatti di corruzione, di cui alle fattispecie che precedono, siano commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo.
È opportuno evidenziare che nella nozione di Pubblico Ufficiale sono sussumibili, oltre al magistrato, anche altri soggetti quali il cancelliere, i testi e qualsiasi altro funzionario pubblico operante nell'ambito di un contenzioso.

- **INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ (ART.319-QUATER C.P.)**

Tale ipotesi di reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, a lui o ad un terzo, denaro o altra utilità.
La norma, oltre a sanzionare la condotta del soggetto agente, punisce, al comma 2, anche il soggetto indotto (colui che dà o promette denaro o altra utilità) il quale, non avendo subito alcuna "costrizione" bensì "induzione", conserva un ampio margine di discrezionalità nella decisione di assecondare o meno la richiesta del soggetto qualificato, in tal modo potendo scegliere se qualificarsi vittima o coautore del reato. La condotta sanzionata è, dunque, attuata mediante un'attività di persuasione, di suggestione o di inganno, solo in questo modo esplicando modalità "induttive".

- **ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)**

Il reato si configura nel caso in cui, nei confronti di un Pubblico Ufficiale o di un Incaricato di Pubblico Servizio, sia formulata la promessa o l'offerta di una somma di denaro o di un'altra utilità, qualora la promessa o l'offerta non siano accettate e riguardino, in via alternativa:
- il compimento di un atto d'ufficio;
- l'omissione o il ritardo di un atto d'ufficio;
- il compimento di un atto contrario ai doveri d'ufficio.

E', inoltre, penalmente sanzionata anche la condotta del Pubblico Ufficiale (o Incaricato di Pubblico Servizio) che solleciti una promessa o dazione di denaro o altra utilità da parte di un privato per le medesime finalità.

È necessario, inoltre, che la promessa di denaro o di altra utilità non siano accettate dal Pubblico Ufficiale, poiché, in caso contrario, deve ritenersi integrata una delle fattispecie di corruzione previste dagli artt. 318 e 319 c.p.

Quanto alle possibili modalità di commissione del reato, si rinvia alle ipotesi previste, a titolo esemplificativo, per i reati di corruzione, fermo restando che, ai fini della configurabilità della fattispecie in esame, è necessario che l'offerta o la promessa non siano accettate.

- **CORRUZIONE TRA PRIVATI (ART.2635 C.C.)**

Il D.Lgs. 231/2001 all'art. 25-ter, c. 1, lettera s bis) rinvia al reato di corruzione tra privati, riferendosi però esclusivamente all'ipotesi contemplata al terzo comma dell'art. 2635 c.c. secondo la quale è punito chiunque dia o prometta denaro o altra utilità ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori o a soggetti sottoposti alla direzione o alla vigilanza di uno di questi ultimi.

Si configura la medesima fattispecie di reato se la condotta corruttiva è posta in essere da amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori dell'ente. Occorre, dunque, che la condotta sia posta nei confronti di soggetti, che abbiano con l'ente un rapporto, anche di carattere qualificato.

Il reato di corruzione tra privati punisce genericamente l'accettazione per sé o per altri di denaro o altra utilità, o la relativa promessa dei medesimi, con il compimento o la omissione di un atto contrario agli obblighi inerenti il proprio ufficio o obblighi di fedeltà, cagionando nocumento all'ente.

Si configura responsabilità per l'ente ai sensi del suddetto reato con la condotta del corruttore, nell'interesse dell'ente per il quale si svolge funzione e con danno per la società stessa.

- **INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 377-BIS C.P.)**

L'art. 377-bis c.p. sanziona le condotte poste in essere da chiunque, facendo ricorso ai mezzi della violenza, della minaccia o dell'offerta o promessa di denaro o di altra utilità, induca a non rendere dichiarazioni, ovvero a renderle mendaci, tutti coloro che sono chiamati a rendere, davanti alla autorità giudiziaria, dichiarazioni utilizzabili in un procedimento penale, nel caso in cui abbiano facoltà di non rispondere.

6 PRINCIPI GENERALI DI COMPORTAMENTO

IDRAGEST S.r.l. impronta la propria attività, a ogni livello organizzativo, ai principi di lealtà, correttezza, trasparenza e stretta legalità. La Società adotta e mantiene una politica di tolleranza zero nei confronti di qualsiasi forma di corruzione, intendendo per tale qualunque condotta volta a offrire, promettere, dare, accettare o sollecitare vantaggi indebiti – di natura economica o di altra utilità – allo scopo di influenzare le decisioni di un soggetto pubblico o privato o di ottenere benefici per sé o per terzi.

Tale politica si applica a tutti i Destinatari della presente Procedura, senza distinzione di ruolo o funzione, nei rapporti sia con la Pubblica Amministrazione sia tra soggetti privati, tanto in Italia quanto all'estero.

TUTTI I DESTINATARI SONO TENUTI A:

1. rispettare rigorosamente le norme di legge, le procedure interne e le prescrizioni del Modello 231 volte a prevenire condotte corruttive o illeciti affini;
2. evitare qualsiasi situazione che possa integrare, anche solo potenzialmente, un conflitto di interessi con la Società, dichiarandone tempestivamente l'esistenza qualora tale situazione dovesse insorgere;
3. assicurare che ogni operazione sia correttamente autorizzata, tracciabile e verificabile, nel rispetto dei livelli di delega e dei meccanismi di controllo previsti dal Modello;
4. effettuare adeguate verifiche preventive (due diligence) in merito all'integrità e alla reputazione delle controparti commerciali, in particolar modo quando queste operino in contesti ad elevato rischio di corruzione o in relazione con soggetti pubblici;
5. segnalare immediatamente all'OdV, attraverso i canali istituzionali previsti, qualsiasi richiesta, pressione o proposta ricevuta che possa configurare un tentativo di coinvolgimento in pratiche corruttive.

VIGE IL DIVIETO ASSOLUTO DI:

1. offrire, promettere, dare, pagare o autorizzare chicchessia a dare o pagare, direttamente o indirettamente, somme di denaro, regalie o altre utilità – a Pubblici Ufficiali, incaricati di pubblico servizio o a soggetti privati – per influenzare atti del loro ufficio, per ottenere un vantaggio indebito per la Società o per terzi, ovvero per conseguire qualsiasi altra forma di trattamento di favore;

2. sollecitare o accettare, per sé o per terzi, somme di denaro, regalie o altre utilità per compiere o aver compiuto atti contrari ai doveri d'ufficio, ai doveri di fedeltà verso la Società o agli obblighi previsti da legge o da contratto;
3. effettuare i cosiddetti "facilitating payments", ossia pagamenti di modesta entità erogati allo scopo di velocizzare o agevolare il compimento di pratiche burocratiche o procedimenti amministrativi che la Pubblica Autorità sarebbe tenuta a compiere nell'ordinario esercizio delle proprie funzioni;
4. erogare contributi, finanziamenti o altre forme di sostegno economico a favore di partiti politici, movimenti, comitati, organizzazioni politiche o candidati a cariche elettive, sia in Italia che all'estero, anche qualora ciò risultasse consentito dalla normativa applicabile.

6.1 ALTRE CONDOTTE VIETATE

Altre condotte vietate per contrastare e prevenire il fenomeno corruttivo riguardano:

- I **contributi politici** poiché presentano il rischio di poter essere usati come un mezzo improprio di corruzione per mantenere o ottenere un vantaggio di business. Infatti, IDRAGEST non eroga contributi a partiti, movimenti, comitati, organizzazioni politiche e sindacali, a loro rappresentanti e candidati.
- I **Facilitation Payment** sono espressamente vietati, poiché non è permesso accettare, offrire o promettere in nessun caso vantaggi economici o altre utilità allo scopo di velocizzare, favorire o facilitare lo svolgimento di un'attività in modo improprio.

7. AREE SENSIBILI E PRESIDI DI CONTROLLO ANTICORRUZIONE

IDRAGEST ha eseguito una mappatura di valutazione dei rischi finalizzata ad individuare le aree sensibili al rischio di corruzione nell'ambito delle proprie attività di business, adottando tutte le misure necessarie a mitigare i medesimi rischi.

Dunque, IDRAGEST ha definito e attuato uno strutturato processo di risk assessment volto a identificare, valutare e tracciare i rischi di corruzione nell'ambito delle proprie attività di business e a orientare la definizione e l'aggiornamento dei presidi di controllo contenuti nella presente procedura. Tra le attività a rischio individuate da IDRAGEST, attraverso tale risk assessment, rientrano a titolo esemplificativo:

- contratti con Terze Parti a Rischio corruzione - quali, a titolo esemplificativo, business associate, partner di joint venture (ovvero gli accordi di collaborazione tra due o più imprese che intendono sviluppare un progetto comune), fornitori, acquirenti/cessionari di crediti etc. -;
- operazioni di compravendita di partecipazioni societarie, aziende e rami d'azienda e contratti di joint venture ovvero associazione temporanea di imprese;
- iniziative non profit, progetti sociali e sponsorizzazioni;
- selezione, assunzione e gestione delle risorse umane;
- omaggi e ospitalità;
- Utilizzo di Sistemi di Intelligenza Artificiale: Impiego di strumenti di IA per l'analisi di dati, la redazione di documenti tecnici e il supporto decisionale.

Per ognuna di queste attività a rischio, IDRAGEST attua dei precisi presidi di controllo.

Di seguito verranno analizzati i controlli minimi previsti da IDRAGEST al fine di prevenire il fenomeno corruttivo.

7.1 RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E ALTRI ENTI PUBBLICI

Ogni interazione con Pubblici Ufficiali o Incaricati di Pubblico Servizio deve essere condotta da personale specificamente autorizzato, nel rispetto dei principi di trasparenza, correttezza e legalità. È obbligatoria la tracciabilità di ogni contatto significativo (es. tramite verbali di riunione, e-mail archiviate).

7.1.2. RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE PER L'OTTENIMENTO DI CONCESSIONI, LICENZE, AUTORIZZAZIONI E FINANZIAMENTI

La gestione dei rapporti con Enti Pubblici, Autorità di vigilanza e organismi istituzionali – finalizzata all'ottenimento di titoli abilitativi (concessioni, licenze, autorizzazioni, nulla osta) ovvero di benefici economici (finanziamenti pubblici, contributi, agevolazioni) – costituisce un'attività ad alto rischio corruttivo e richiede l'adozione di presidi specifici volti a garantire la massima trasparenza e tracciabilità.

LE FUNZIONI AZIENDALI COMPETENTI ALLA GESTIONE DI TALI RAPPORTI DEVONO:

1. assicurare che ogni istanza, domanda o comunicazione indirizzata alla Pubblica Amministrazione sia sottoscritta esclusivamente da soggetti aziendali dotati di idonei poteri di firma e rappresentanza, nel rispetto del sistema di deleghe e procure vigente;

2. verificare preventivamente la veridicità, la completezza e la correttezza di tutte le dichiarazioni, le autocertificazioni e la documentazione tecnica e amministrativa prodotte a supporto di richieste rivolte a soggetti pubblici, assumendo piena responsabilità del contenuto dei documenti trasmessi;
3. privilegiare, per ogni comunicazione e scambio di corrispondenza con funzionari e uffici pubblici, i canali di comunicazione formali e tracciabili (posta elettronica certificata – PEC, protocollo, raccomandata), evitando contatti informali che non consentano una piena tracciabilità;
4. registrare e documentare ogni contatto, incontro o comunicazione – anche informale – intercorso con rappresentanti della Pubblica Amministrazione nell'ambito dei procedimenti di cui al presente paragrafo, annotando data, oggetto, soggetti coinvolti ed esito del contatto;
5. archiviare in modo sistematico e ordinato, su piattaforma digitale aziendale o archivio fisico protetto, tutta la documentazione relativa ai procedimenti amministrativi, rendendola prontamente disponibile per eventuali verifiche da parte dell'OdV o delle Autorità competenti;
6. comunicare tempestivamente all'OdV l'avvio di procedimenti amministrativi di particolare rilevanza o complessità, nonché qualsiasi evento anomalo, richiesta insolita o pressione percepita nel corso dell'interlocuzione con la Pubblica Autorità;
7. inserire, nei contratti stipulati con consulenti, professionisti o intermediari esterni che supportano la Società nello svolgimento di pratiche amministrative, apposite clausole di conformità al Modello 231 e al Codice Etico, prevedendo espressamente la facoltà di risoluzione del contratto in caso di comportamenti contrari alle previsioni della presente Procedura.

VIGE IL DIVIETO DI:

1. ricorrere a intermediari non qualificati, soggetti privi di specifiche competenze professionali o figure il cui incarico non sia riconducibile a una genuina prestazione di servizi, al solo scopo di veicolare, anche indirettamente, risorse verso funzionari pubblici o di accelerare in modo improprio l'iter di procedimenti amministrativi;
2. promettere, offrire o concedere, sotto qualsiasi forma (denaro, regalie, utilità, promesse di assunzione, vantaggi per terzi), benefici di qualunque natura a funzionari o dipendenti di enti
3. pubblici per ottenere provvedimenti favorevoli, accelerare l'iter procedurale o evitare l'esercizio di controlli e ispezioni;

4. presentare dichiarazioni, documenti o dati non veritieri – ovvero omettere informazioni rilevanti – nell'ambito di procedimenti per il rilascio di autorizzazioni, concessioni o per l'ottenimento di finanziamenti pubblici;
5. instaurare, nell'ambito dei rapporti con la Pubblica Amministrazione, relazioni di tipo personale o informale che possano compromettere l'obiettività e l'imparzialità del funzionario pubblico o creare situazioni suscettibili di essere percepite come tentativi di condizionamento.

Ogni violazione – anche solo tentata – delle disposizioni del presente paragrafo dovrà essere immediatamente comunicata all'OdV attraverso i canali di segnalazione previsti, compresa la procedura di Whistleblowing aziendale.

7.2 Omaggi, Regalie, Spese di Rappresentanza e Sponsorizzazioni

È fatto divieto assoluto di offrire, promettere o dare, direttamente o indirettamente, denaro, regali o altre utilità a Pubblici Ufficiali o Incaricati di Pubblico Servizio al fine di influenzarne le decisioni.

Sono consentiti omaggi e spese di rappresentanza solo se di valore modico, non superiore a € 50,00 (cinquanta/00) su base annua per singolo destinatario, e solo se riconducibili a normali pratiche di cortesia e non interpretabili come un mezzo per ottenere un indebito vantaggio.

È comunque vietato offrire omaggi, anche di modico valore, a funzionari pubblici coinvolti in procedure di gara, negoziazioni contrattuali o processi decisionali di interesse per Idragest.

Ogni omaggio offerto o ricevuto deve essere autorizzato e registrato nell'apposito Registro Unico degli Omaggi (RUO).

Le attività di sponsorizzazione e le liberalità devono essere approvate dal CdA, formalizzate per iscritto e destinate a enti e iniziative di comprovata onorabilità, escludendo categoricamente partiti politici o soggetti ad essi riconducibili.

7.3 Gestione delle Terze Parti (Fornitori, Consulenti, Partner)

Nessuna terza parte può essere incaricata senza una preventiva e documentata attività di due diligence, volta a verificarne l'integrità, la reputazione e l'assenza di conflitti di interesse. I contratti con le terze parti devono contenere specifiche clausole anticorruzione che prevedano la risoluzione del rapporto in caso di violazione.

7.4 Selezione del Personale e Prevenzione del "Pantouflage"

Il processo di selezione deve basarsi su criteri oggettivi di merito e professionalità. Per prevenire il rischio di "pantouflage" (ex art. 53, co. 16-ter, D.Lgs. 165/2001), ogni candidato che abbia avuto precedenti rapporti di lavoro con la Pubblica Amministrazione negli ultimi tre anni deve sottoscrivere una Dichiarazione Anticorruzione dettagliata, specificando gli uffici di appartenenza e i poteri autoritativi o negoziali esercitati. La Società si riserva di effettuare verifiche e, in caso di dubbio, di consultare l'Organismo di Vigilanza (OdV).

7.5 Conflitto di Interessi

Tutti i Destinatari hanno l'obbligo di evitare e prevenire situazioni di conflitto di interesse. Qualsiasi potenziale conflitto, anche indiretto, deve essere immediatamente comunicato al proprio superiore e/o all'OdV. In particolare, il personale coinvolto in attività di consulenza per la selezione di fornitori per conto di clienti deve astenersi da ogni valutazione qualora sussista un interesse personale, diretto o indiretto, con uno dei fornitori in esame.

7.6. Utilizzo di Sistemi di Intelligenza Artificiale

L'utilizzo di sistemi di Intelligenza Artificiale deve avvenire nel rigoroso rispetto della "IDRAGEST - Policy IA.docx". In particolare, è fatto divieto assoluto di:

1. Inserire nei prompt di sistemi di IA dati personali, informazioni riservate di clienti, segreti industriali o qualsiasi dato coperto da obblighi di confidenzialità.
2. Utilizzare l'IA per elaborare strategie collusive, analizzare illecitamente dati di gara riservati o compiere qualsiasi attività finalizzata a turbare una gara d'appalto (art. 353 c.p.) o a commettere altri reati presupposto.

Qualsiasi uso improprio o sospetto deve essere segnalato al Responsabile IA e all'OdV.

7.7. Trasparenza e Tracciabilità Contabile

Tutte le operazioni e transazioni devono essere correttamente autorizzate, verificabili, legittime, coerenti e registrate in modo accurato e tempestivo nelle scritture contabili. È vietata la creazione di fondi neri o registrazioni fittizie. Per i contratti pubblici, deve essere garantita la piena tracciabilità dei flussi finanziari ai sensi della L. 136/2010.

7.7.1 PROCEDURE CONTABILI

Qualsiasi operazione economica e finanziaria è effettuata rispettando i principi di legalità, integrità e trasparenza e, per tale ragione, ogni operazione e transazione deve essere autorizzata dal datore di lavoro o dalla Funzione all'uopo preposta, e deve essere documentalmente riscontrabile, al fine di consentire i necessari controlli.

Invero, i costi, i pagamenti, le entrate, gli incassi e gli impegni di spesa sono tempestivamente inseriti tra le operazioni finanziarie e devono riflettere le informazioni contenute nei documenti di supporto, emessi in conformità alle leggi applicabili ed opportunamente archiviati.

Ancora, IDRAGEST si è dotata di un sistema organizzativo improntato al rispetto del principio di segregazione dei ruoli affinché vi sia separazione di responsabilità tra coloro che eseguono, controllano e autorizzano una specifica attività aziendale. La Società ha articolato il proprio sistema interno di conferimento dei poteri attribuendo specifiche deleghe operative in linea con le responsabilità organizzative assegnate.

IDRAGEST assicura la riservatezza delle informazioni in proprio possesso, stabilendo il divieto di utilizzare impropriamente notizie ed informazioni acquisite e/o elaborate in occasione dell'espletamento degli incarichi e delle attività svolte, attraverso l'adozione di apposite policy, procedure, regole e strumenti volti al raggiungimento di un adeguato livello di sicurezza nella gestione del patrimonio informativo aziendale, nel rispetto della normativa vigente applicabile, in termini di confidenzialità, integrità e disponibilità delle informazioni.

8 RISORSE UMANE

IDRAGEST assicura che il processo di selezione e assunzione del personale preveda specifiche verifiche dei candidati, con l'obiettivo di garantirne l'idoneità, la competenza e la professionalità, requisiti necessari per ricoprire la posizione lavorativa richiesta.

Il processo di selezione ed inserimento delle risorse deve essere gestito nel rispetto delle disposizioni e dei principi di seguito indicati:

- la responsabilità del processo è affidata a persone qualificate e all'uopo preposte;
- devono essere acquisite informazioni idonee ad identificare e gestire eventuali situazioni a potenziale

pregiudizio di indipendenza e/o di conflitto di interessi nel successivo svolgimento delle attività professionali, nonché raccolte informazioni riguardanti l'integrità, nel rispetto della vigente normativa;

● non sono ammesse segnalazioni, assunzioni, collaborazioni o attivazioni di stage finalizzate ad ottenere indebiti vantaggi;

● nel caso di assunzioni di personale che abbia lavorato presso Pubbliche Amministrazioni, che abbia ricoperto posizioni di livello apicale presso società clienti o persone con parenti e affini che ricoprono posizioni di responsabilità presso Pubbliche Amministrazioni o società clienti, devono essere espletati tutti i provvedimenti necessari ad evitare conflitti di interesse, problematiche di indipendenza e/o a rispettare vincoli o impedimenti di legge.

La selezione deve essere effettuata tenendo conto del ruolo e delle attività che la risorsa è chiamata a svolgere.

L'assunzione è finalizzata nel rispetto della normativa vigente applicabile e opportunamente formalizzata attraverso un contratto di lavoro sottoscritto dal datore di lavoro; tutta la documentazione deve essere debitamente conservata.

9. COMUNICAZIONE E FORMAZIONE

IDRAGEST, al fine di assicurare il puntuale rispetto della presente procedura garantisce la comunicazione e la formazione a tutti i Destinatari della medesima politica Anticorruzione.

Pertanto, la Società si impegna a diffondere a tutti i Destinatari la Politica Anticorruzione e a promuovere il rispetto dei principi in essa rappresentati.

LA COMUNICAZIONE ESTERNA PREVEDE:

● la pubblicazione della Politica Anticorruzione della Società nel sito web di IDRAGEST;

● l'inserimento di clausole contrattuali e/o disposizioni negli accordi con le Terze Parti relative all'accettazione dei principi anticorruzione adottati;

LA COMUNICAZIONE INTERNA PREVEDE:

● la pubblicazione della Politica Anticorruzione della Società nella sezione dedicata del portale aziendale;

● periodiche comunicazioni da parte della società sui principi etici da adottare e sui comportamenti vietati;

● l'organizzazione di specifiche iniziative di formazione in materia di anticorruzione;

● l'informativa al personale neo-assunto, attraverso la consegna della Politica Anticorruzione, oltre che del Codice Etico e del Modello 231.

La formazione ha la finalità principale di fornire adeguata conoscenza dei rischi, delle responsabilità e delle sanzioni applicabili in caso di violazioni delle normative anticorruzione adottate, nonché dei principi da osservare e dei comportamenti da adottare.

La formazione è obbligatoria per tutto il personale.

10 VIOLAZIONI E PROVVEDIMENTI SANZIONATORI

I Destinatari sono incoraggiati a segnalare atti di corruzione, tentata, presunta o effettiva, e/o di violazioni di disposizioni normative nazionali o dell'Unione Europea in materia di corruzione, nonché di violazioni tentate, presunte o effettive della Politica Anticorruzione, di cui siano venuti a conoscenza nell'esercizio della propria attività lavorativa.

Per le segnalazioni delle violazioni del D.Lgs. 231/2001 e del modello di organizzazione, gestione e controllo di IDRAGEST, si rappresenta che la stessa si è dotata di un'apposita procedura denominata "Procedura di gestione delle segnalazioni" ("Procedura interna di Whistleblowing"), alla quale si fa rinvia integralmente.

10.1 AMBITO DI APPLICAZIONE

La presente procedura si applica non soltanto a tutti destinatari del Modello e/o del Codice Etico della Società, ovvero ai soci, ai componenti dell'Organo Amministrativo, ai dipendenti e ai lavoratori in somministrazione, a tutti coloro che, pur non rientrando nella categoria dei dipendenti, operino per IDRAGEST e siano sotto il controllo e la direzione della società (es. stagisti, lavoratori a contratto ed a progetto) e coloro che, pur esterni alla Società, operino, direttamente o indirettamente, per IDRAGEST (es. professionisti, consulenti, agenti, fornitori, partner commerciali, clienti, ecc.).

Tale elenco include, oltre ai lavoratori dipendenti, anche i lavoratori autonomi ed in somministrazione; coloro che hanno un rapporto di collaborazione professionale con la Società, i liberi professionisti e i consulenti, i volontari, i tirocinanti, anche non retribuiti, oltre ai soci e alle persone con funzione di amministrazione, controllo, vigilanza o rappresentanza, anche solo in via di fatto.

Un ruolo particolare, viene svolto dall'Organismo di Vigilanza, istituito ai sensi del D. Lgs. 231/2001, la cui attività contempla la raccolta periodica di informazioni sensibili al fine di identificare comportamenti potenzialmente a rischio con riguardo ai reati di corruzione nei confronti sia di Pubbliche Amministrazioni italiane ed estere sia di soggetti privati.

Il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 e il quadro normativo aziendale sono assoggettati ad un processo di aggiornamento continuo per adeguarsi alle modifiche organizzative e legislative e rispondere adeguatamente ai possibili rischi di commissione di reati. Qualunque violazione, sospetta o nota, delle procedure anti-corruzione o di leggi in materia deve essere immediatamente segnalata, anche in forma anonima, tramite i canali di seguito riportati:

Sito internet aziendali	www.idragest.it attraverso la compilazione del modulo di segnalazione Whistleblowing
Indirizzo Postale	IDRAGEST S.R.L. Viale Andrea Doria 55 – 95123 Catania RISERVATO Organismo di Vigilanza

La gestione delle segnalazioni ed il relativo trattamento dei dati personali e delle informazioni raccolte è effettuato da IDRAGEST S.r.l., nel rispetto delle disposizioni di legge applicabili, ivi inclusa la normativa in materia di protezione dei dati personali ed in particolare nel rispetto del Decreto Legislativo 30/06/2003 n. 196 e s.m.i. e del Regolamento Europeo 2016/679 (GDPR).

10.2 SANZIONI

Il rispetto e l'osservanza della Politica Anticorruzione e delle normative Anticorruzione è parte integrante degli obblighi contrattuali dei dipendenti e delle Terze Parti con cui la Società intrattiene relazioni commerciali; pertanto, la loro violazione costituisce una inadempienza agli obblighi contrattuali e al rispetto delle regole aziendali.

Conseguentemente, la Società si impegna ad implementare ragionevoli controlli finalizzati a prevenire eventuali comportamenti illeciti, nonché ad applicare opportune sanzioni, che saranno gradati in base alla gravità e nel rispetto del quadro normativo e contrattuale di riferimento, prevedendo per il personale interno misure coerenti con quanto previsto dallo Statuto dei Lavoratori e dal CCNL di riferimento.

Mentre nel caso di soggetti esterni che lavorano per conto o con la Società (es. Fornitori, Collaboratori), l'inosservanza di quanto previsto nella presente Procedura sarà trattata attraverso previsioni contrattuali che possono includere anche la sospensione dell'esecuzione o la risoluzione del contratto e, laddove ve ne siano i presupposti, la richiesta di risarcimento danni.

Viene assicurata la riservatezza delle fonti e delle informazioni di cui si venga in possesso, fatti salvi gli obblighi di legge. Inoltre, IDRAGEST non effettuerà azioni ritorsive (ovvero sanzioni disciplinari, demansionamento, sospensione, licenziamento) o discriminerà in alcun modo in ambito lavorativo il personale della società che:

• abbia svolto in buona fede azioni mirate a riferire eventi o situazioni relative al rispetto di questa procedura o delle procedure anti-corruzione o comunque delle normative di legge in materia;

• si sia rifiutato di effettuare azioni contrarie a questa procedura o alle procedure anti-corruzione, anche se in conseguenza di tale rifiuto ci siano state conseguenze negative per il business della Società.

IN PARTICOLARE, I DESTINATARI DEVONO ASTENERSI DALL'INFLUENZARE LE DECISIONI DEI RAPPRESENTANTI DELLA PUBBLICA AMMINISTRAZIONE IN MANIERA IMPROPRIA O ILLECITA E DUNQUE È FATTO DIVIETO DI:

• promettere, offrire o corrispondere ai rappresentanti della Pubblica Amministrazione, anche su induzione di questi ultimi e direttamente o tramite terzi, somme di denaro o altre utilità in cambio di favori, compensi o altri vantaggi per la Società;

• effettuare pagamenti o riconoscere altre utilità a collaboratori, o altri soggetti terzi che operino per conto della Società, che non trovino adeguata giustificazione nel rapporto contrattuale;

• favorire, nei processi di assunzione o di acquisto dipendenti e collaboratori dietro specifica segnalazione dei Rappresentanti della Pubblica Amministrazione, in cambio di favori, compensi o altri vantaggi per sé e/o per la Società;

• concedere promesse di assunzione a favore di chiunque e, specificatamente, a favore di, rappresentanti della Pubblica Amministrazione, loro parenti e affini o soggetti da questi segnalati;

• distribuire ai rappresentanti della Pubblica Amministrazione italiana e straniera omaggi o regali, salvo che si tratti piccoli omaggi di modico o di simbolico valore, e tali da non compromettere l'integrità e la reputazione delle parti e da non poter essere considerati finalizzati all'acquisizione impropria di benefici. Eventuali richieste esplicite o implicite di benefici da parte di un pubblico ufficiale o di un incaricato di pubblico servizio, salvo omaggi d'uso commerciale e di modesto valore, debbono essere respinte ed immediatamente riferite al proprio superiore gerarchico;

• presentare ad o organismi pubblici nazionali o stranieri dichiarazioni non veritiere o prive delle informazioni dovute nell'ottenimento di finanziamenti pubblici, ed in ogni caso compiere qualsivoglia atto che possa trarre in inganno l'ente pubblico nella concessione di erogazioni o effettuazioni di pagamenti di qualsiasi natura;

• destinare somme ricevute da organismi pubblici nazionali o stranieri a titolo di contributo, sovvenzione o finanziamento a scopi diversi da quelli cui erano destinati;

• rappresentare, agli Enti finanziatori, informazioni non veritiere o non complete o eludere obblighi normativi, ovvero l'obbligo di agire nel più assoluto rispetto della legge e delle normative eventualmente applicabili in tutte le fasi del processo, evitando di porre in essere comportamenti scorretti, a titolo esemplificativo, al fine di ottenere il superamento di vincoli o criticità relative alla concessione del finanziamento, in sede di incontro con Funzionari degli Enti finanziatori nel corso dell'istruttoria;

• ricorrere a forme di pressione, inganno, suggestione o di captazione della benevolenza del pubblico funzionario, tali da influenzare le conclusioni dell'attività amministrativa;

• omettere gli obblighi ed i presidi di controllo previsti dalla Società in ambito della gestione dei flussi finanziari (i.e. limite impiego risorse finanziarie, procedura di firma congiunta per determinate tipologie di operazioni, espressa causale impiego di risorse, etc.), in conformità ai principi di correttezza professionale e contabile, al fine di orientare in proprio favore le decisioni in merito all'ottenimento di concessioni, licenze ed autorizzazioni dalla Pubblica Amministrazione;

I rapporti con la Pubblica Amministrazione nonché con le autorità giudiziarie sono gestiti esclusivamente dalle Funzioni Aziendali all'uopo preposte e/o delegate.

11 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

L'Organismo di Vigilanza (OdV) di IDRAGEST S.r.l. vigila sull'efficacia, sull'adeguatezza e sull'osservanza della presente Procedura nell'ambito del complessivo sistema di prevenzione dei reati previsto dal D.Lgs. 231/2001. A tal fine, l'OdV dispone di pieni e autonomi poteri di iniziativa e di controllo, esercitabili in ogni momento e senza necessità di preventiva autorizzazione da parte degli organi aziendali.

IN PARTICOLARE:

TRACCIABILITÀ E ARCHIVIAZIONE DOCUMENTALE: Ogni attività rientrante nelle aree sensibili individuate dalla presente Procedura deve essere adeguatamente documentata e archiviata su piattaforma digitale aziendale o in archivio fisico protetto. La documentazione deve essere conservata per un periodo idoneo a consentire le verifiche dell'OdV e, ove necessario, delle Autorità competenti, garantendo l'accessibilità immediata su richiesta dell'Organismo.

FLUSSI INFORMATIVI PERIODICI: Le Funzioni Aziendali interessate sono tenute a trasmettere all'OdV i flussi informativi periodici definiti dal Modello 231, nelle modalità e nei tempi ivi stabiliti. Tali flussi devono includere, a titolo esemplificativo: la reportistica sulle attività di due diligence effettuate sulle terze parti a rischio, le comunicazioni relative ad avvii di procedimenti amministrativi rilevanti, le eventuali segnalazioni di anomalie o criticità riscontrate nella gestione delle aree sensibili.

SEGNALAZIONI STRAORDINARIE: Fermi i flussi informativi periodici, ogni anomalia rilevante, ogni tentativo – anche non andato a buon fine – di ottenere o offrire vantaggi indebiti, nonché qualsiasi violazione o sospetto di violazione delle disposizioni della presente Procedura, deve essere segnalato immediatamente all'OdV, senza ritardo e indipendentemente dalla periodicità dei flussi ordinari.

WHISTLEBLOWING: Le segnalazioni di condotte illecite o di situazioni di rischio possono essere effettuate da chiunque ne venga a conoscenza attraverso i canali riservati previsti dalla Procedura di gestione del Whistleblowing adottata dalla Società. La riservatezza dell'identità del segnalante è garantita nei limiti consentiti dalla legge e dall'ordinamento interno; è assolutamente vietato porre in essere atti ritorsivi, discriminatori o penalizzanti nei confronti di chi abbia effettuato in buona fede una segnalazione.

POTERI ISPETTIVI DELL'ODV: L'OdV ha libero accesso a tutti i documenti, le informazioni, i sistemi informatici e le risorse aziendali necessari allo svolgimento della propria attività di vigilanza, potendo richiedere alle Funzioni competenti qualsiasi chiarimento, dato o documento ritenuto utile. L'OdV può avvalersi, nello svolgimento delle proprie funzioni, del supporto delle strutture aziendali competenti ovvero di consulenti esterni appositamente incaricati.

CONSEGUENZE DELLE VIOLAZIONI:

La violazione delle disposizioni contenute nella presente Procedura, accertata secondo le modalità previste dal Sistema Sanzionatorio interno, integra un illecito disciplinare e costituisce violazione del Modello di Organizzazione, Gestione e Controllo adottato dalla Società ai sensi del D.Lgs. 231/2001. La Società applicherà, nei confronti del soggetto responsabile, le sanzioni previste dal Sistema Sanzionatorio vigente, in coerenza con le previsioni del CCNL applicabile e con il quadro normativo di riferimento, ferma restando in ogni caso l'eventuale rilevanza penale e amministrativa delle condotte accertate.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO,

COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 22.07.2026	ADOZIONE

SOMMARIO

1 FINALITA' 5

2 ACRONIMI AZIENDALI 5

3 RIFERIMENTI NORMATIVI 6

4 DESTINATARI DELLA PROCEDURA 8

5. Definizioni 9

6. Principi generali di utilizzo 9

7. Usi consentiti 11

8. Divieti assoluti 13

9. Proprietà intellettuale, opere dell'ingegno e segreti commerciali 15

9.1 Principi generali 15

9.2 Titolarità degli output generati dall'IA 16

9.3 Obblighi operativi in materia di proprietà intellettuale 16

9.4 Divieti specifici in materia di proprietà intellettuale e IA 17

9.5 Tutela dei segreti commerciali e del know-how aziendale 18

9.6 Rapporti con fornitori e subfornitori 19

9.7 Reati presupposto e implicazioni 231 19

9.8 Controlli, segnalazioni e sanzioni 20

10. Sicurezza informatica e controlli tecnici 20

11. Valutazione preventiva e autorizzazione d'uso22

11.1 Finalità e ambito del paragrafo 22

11.2 Soggetti coinvolti nella valutazione preventiva e nell'autorizzazione 22

11.3 Riesame periodico delle autorizzazioni 23

11.4 Revoca e sospensione dell'autorizzazione 24

12. Validazione umana e qualità degli output 24

12.1 Obblighi di Protezione dei Dati e Anonimizzazione degli Input 25

13. Gare pubbliche e contratti 25

13-BIS. GESTIONE DELL'IA NELLE PROCEDURE DI GARA PUBBLICA E NEGLI APPALTI 26

13-bis.1 Ambito e finalità del capitolo 26

13-bis.2 Principi applicabili alle gare pubbliche26

13-bis.3 Attività consentite e attività vietate nella predisposizione dell'offerta 27

13-bis.4 Dichiarazioni obbligatorie in gara: schema operativo 28

13-bis.6 Obblighi di tracciabilità e conservazione 30

13-BIS.7 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA 30

13-bis.8 Sistema sanzionatorio specifico per le dichiarazioni ANAC 31

14. Incidenti, anomalie e segnalazioni 32

14.1 Incidenti di sicurezza e accesso 32

14.2 Incidenti privacy e confidenzialità 33

14.3 Incidenti tecnico-operativi 33

14.4 Incidenti giuridico-reputazionali 33

15. Formazione e consapevolezza 33

15.1 Differenziazione per ruolo 34

15.2 Verifica e autorizzazione 34

15.3 Tracciabilità e conservazione 34

16. Monitoraggio, audit e flussi verso OdV 34

16.1 Finalità e ambito 34

16.2 Governance del monitoraggio: ruoli e responsabilità 35

16.3 Controlli periodici: tipologia, contenuto e periodicità 36

16.3.1 Controlli sull'uso degli account e dei sistemi autorizzati 36

16.3.2 Verifiche sui log di sistema 36

16.3.3 Controlli a campione su prompt e output rilevanti 37

16.3.4 Audit su licenze, provenienza dati, divieti di scraping e data extraction 38

16.4 Registro Audit IA 39

16.5 Gestione delle anomalie e dei trigger di escalation 39

16.6 Reporting periodico verso l'OdV e il CDA 40

16.7 Conseguenze disciplinari, penali e amministrative delle violazioni 40

16.8 Rinvio alle procedure di flusso informativo e whistleblowing 41

16.9 Disposizioni finali del paragrafo 41

1 FINALITA'

La presente procedura disciplina la gestione, l'accesso, l'utilizzo, il controllo e il monitoraggio dei sistemi di intelligenza artificiale autorizzati da IDRAGEST, al fine di:

1. prevenire la commissione di reati rilevanti ai sensi del D.Lgs. 231/2001;
2. assicurare il rispetto della normativa su protezione dei dati, cybersecurity, proprietà intellettuale, segreti commerciali, appalti pubblici e trasparenza;
3. garantire che l'uso dell'IA avvenga in modo sicuro, tracciabile, proporzionato, umano-controllato e coerente con le finalità aziendali.

Con specifico riferimento alle procedure di affidamento di contratti pubblici, la procedura disciplina altresì gli obblighi dichiarativi, i controlli preventivi, la tracciabilità e i flussi informativi richiesti dalla Delibera ANAC n. 148 del 1° aprile 2026 e dal relativo aggiornamento del Bando tipo n. 1-2023. Tali disposizioni si applicano a tutto il personale coinvolto nelle attività di gara, indipendentemente dalla natura del rapporto con la società.

2 ACRONIMI AZIENDALI

CDA Consiglio di Amministrazione
PRES Presidente CDA
RSPP Responsabile del Servizio Prevenzione e Protezione
RSGQ Responsabile Sistema di Gestione Qualità
RTEC Responsabile Tecnico
RAM/RRU Responsabile Amministrazione - Risorse Umane
RCOM/APVG Responsabile Commerciale - Approvvigionamento
RFAM Responsabile Facility Management
RPROG Responsabile Progettazione
CDL Consulente del Lavoro
REC Responsabile Esterno Contabilità
RIA Responsabile IA
RIDC Responsabile interno di conformità

I SUDDETTI ACRONIMI AZIENDALI CORRISPONDONO ALLE FUNZIONI E AI RUOLI DEI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE DI IDRAGEST S.R.L..

3 RIFERIMENTI NORMATIVI

La presente Procedura è redatta in conformità al quadro normativo vigente e ai documenti interni che costituiscono i pilastri del sistema di controllo interno di IDRAGEST S.r.l.

A. FONTI PRIMARIE (EUROPEE)

- REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO (AI ACT): Costituisce la fonte principale per la regolamentazione dell'IA. È fondamentale richiamarne l'approccio basato sul rischio, i divieti (art. 5), gli obblighi per i sistemi ad alto rischio, gli obblighi specifici per i deployer (soggetti che utilizzano sistemi di IA come IDRAGEST) ai sensi dell'art. 26 e gli obblighi di trasparenza per determinati sistemi (art. 50);

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO (GDPR): Essenziale per tutti gli aspetti legati al trattamento di dati personali. Vanno richiamati i principi fondamentali (art. 5), le basi giuridiche (art. 6), i diritti degli interessati (artt. 15-22), gli obblighi di accountability del titolare, inclusa la valutazione d'impatto (DPIA, art. 35), e i principi di privacy by design e by default (art. 25);

- DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO (DIRETTIVA NIS 2): Stabilisce il quadro generale per un livello comune elevato di cibersicurezza nell'Unione. Costituisce la base per gli obblighi nazionali in materia di gestione dei rischi cyber, che sono essenziali per la sicurezza dei sistemi IA .

- REGOLAMENTO DI ESECUZIONE (UE) 2024/2690 DELLA COMMISSIONE: Specifica i requisiti tecnici e metodologici per le misure di gestione dei rischi di cibersicurezza ai sensi della Direttiva NIS 2. Fornisce indicazioni operative per le policy di sicurezza, la gestione degli incidenti e la sicurezza della catena di approvvigionamento.

B. NORMATIVA NAZIONALE DI RIFERIMENTO

- DELIBERA ANAC N. 148 DEL 1° APRILE 2026 – "*Aggiornamento Bando tipo n. 1-2023 in materia di dichiarazioni sull'uso dell'intelligenza artificiale nelle gare pubbliche*".

- LEGGE 23 SETTEMBRE 2025, N. 132 ("DISPOSIZIONI E DELEGHE AL GOVERNO IN MATERIA DI INTELLIGENZA ARTIFICIALE"): È la principale fonte nazionale in materia. Particolare rilevanza assumono l'art. 3 sui principi generali (trasparenza, proporzionalità, sorveglianza umana), l'art. 13 sull'uso dell'IA nelle professioni intellettuali

(ruolo strumentale, prevalenza del lavoro umano, obblighi informativi verso il cliente) e l'art. 14 sull'utilizzo da parte delle Pubbliche Amministrazioni.

- DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 ("DISCIPLINA DELLA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI"): È il fondamento stesso della procedura, in quanto strumento di prevenzione dei reati-presupposto .

- DECRETO LEGISLATIVO 4 SETTEMBRE 2024, N. 138 ("RECEPIMENTO DELLA DIRETTIVA (UE) 2022/2555"): Attua la Direttiva NIS 2 in Italia, definendo gli obblighi di cibersicurezza per soggetti come IDRAGEST, incluse le misure di gestione dei rischi e la notifica degli incidenti.

- DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196 ("CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI"): Da citare in coordinamento con il GDPR per la disciplina nazionale complementare.

- LEGGE 22 APRILE 1941, N. 633 ("LEGGE SUL DIRITTO D'AUTORE"): Fondamentale per la gestione della proprietà intellettuale sia dei dati di input (addestramento) che degli output. Si devono richiamare le disposizioni sul divieto di text and data mining non autorizzato (artt. 70-ter e 70-quater), nonché le norme a presidio dei programmi per elaboratore e delle banche dati.

- DECRETO LEGISLATIVO 10 FEBBRAIO 2005, N. 30 ("CODICE DELLA PROPRIETÀ INDUSTRIALE"): Da richiamare per la tutela dei segreti commerciali e del know-how aziendale, che devono essere protetti dall'inserimento improprio nei sistemi di IA.

- DECRETO LEGISLATIVO 31 MARZO 2023, N. 36 ("CODICE DEI CONTRATTI PUBBLICI"): Essenziale per le attività di Idragest. Vanno menzionati gli articoli sulla tutela dei segreti tecnici e commerciali contenuti nelle offerte (artt. 35, 98, 99) e sull'accesso agli atti (art. 36).

- DECRETO LEGISLATIVO 10 MARZO 2023, N. 24 ("DECRETO WHISTLEBLOWING"): Da richiamare per la gestione delle segnalazioni di illeciti o violazioni delle procedure, inclusa la PMOG16.

- LEGGE 20 MAGGIO 1970, N. 300 ("STATUTO DEI LAVORATORI"): Rilevante per i profili di controllo a distanza e per l'impatto degli strumenti di IA sull'attività lavorativa dei dipendenti [IDRAGEST

C. REATI PRESUPPOSTO (D.LGS. 231/2001 E CODICE PENALE)

La procedura deve mirare a prevenire la commissione dei seguenti reati:

- ART. 24-BIS D.LGS. 231/2001 (DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI): Include reati come accesso abusivo a sistema informatico (art. 615-ter c.p.), danneggiamento di sistemi (artt. 635-bis e ss. c.p.), frode informatica (art. 640-ter c.p.) ed estorsione informatica (art. 629, c. 3 c.p.).

- ART. 25-NOVIES D.LGS. 231/2001 (REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE): Include la duplicazione abusiva di software (art. 171-bis L.d.A.) e altre violazioni della legge sul diritto d'autore.

- ART. 612-QUATER C.P. (ILLECITA DIFFUSIONE DI CONTENUTI GENERATI O ALTERATI CON SISTEMI DI INTELLIGENZA ARTIFICIALE): Nuova fattispecie che punisce la creazione e diffusione di "deepfake" dannosi, da prevenire con specifici divieti procedurali.

Altri articoli del Codice Penale rilevanti richiamati nelle procedure esistenti, quali l'art. 491-bis (Documento informatico equiparato all'atto pubblico) e gli artt. 493-ter e 493-quater (Indebito utilizzo e falsificazione di strumenti di pagamento).

E. FONTI INTERNE AZIENDALI

La PMOG16 deve essere coordinata con e richiamare esplicitamente i seguenti documenti:

- Codice Etico di IDRAGEST S.r.l.
- Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/01 (Parte Generale e Speciale).
- IDRAGEST - Policy IA.

4 DESTINATARI DELLA PROCEDURA

La presente Procedura si applica a tutti coloro che agiscono in nome e per conto di IDRAGEST interagendo con sistemi di intelligenza artificiale, ed, in particolare ai componenti del Consiglio di Amministrazione e degli altri Organi Sociali, ai Dipendenti, ai lavoratori in somministrazione, ai collaboratori, ai consulenti, ai fornitori ed ai partner commerciali che, a qualsiasi titolo, operano in nome o per conto della Società. La presente Policy rappresenta, inoltre, un'integrazione del Modello di Gestione Organizzazione e Controllo ex D.Lgs. n. 231/2001 adottato dalla Società, implementando in tal modo, unitamente ai principi contenuti nel Codice Etico e alla Policy IA il sistema adottato da IDRAGEST per la prevenzione dei reati che potrebbero essere posti in essere a causa di un uso non consentito della piattaforma di intelligenza artificiale.

Con riferimento specifico alle procedure di gara pubblica, il RAM è il soggetto responsabile della correttezza delle dichiarazioni IA rese in offerta ai sensi della Delibera ANAC n. 148/2026. Prima della sottoscrizione e trasmissione dell'offerta, il RAM:

1. esegue la checklist di verifica pre-offerta di cui al § 13-bis.5;
2. raccoglie la conferma del Responsabile IA sulla conformità degli strumenti utilizzati;
3. raccoglie l'attestazione di validazione tecnica firmata dal professionista responsabile;
4. seleziona e inserisce nella documentazione di gara la dichiarazione ANAC applicabile (schema A, B, C o D);
5. archivia tutta la documentazione per almeno 5 anni;

6. trasmette le comunicazioni dovute all'OdV ai sensi del § 13-bis.7.

5. DEFINIZIONI

Ai fini della presente procedura si intendono per:

SISTEMA DI IA: sistema rientrante nella definizione aziendale e regolatoria adottata dalla Policy IA.

DEPLOYER: IDRAGEST, quale soggetto che utilizza sistemi di IA nell'esercizio della propria attività.

RESPONSABILE IA: soggetto designato dalla Società per la gestione degli account, il controllo di conformità, il monitoraggio, la formazione e la gestione degli incidenti.

UTENTE AUTORIZZATO: soggetto formalmente abilitato all'uso dei sistemi IA approvati.

DATI RISERVATI: dati personali, segreti industriali, planimetrie, dati tecnici di rete, credenziali, dati economici riservati, dati relativi a commesse pubbliche e ogni altra informazione classificata come non divulgabile.

VALIDAZIONE UMANA: verifica critica, tecnica, giuridica e documentata dell'output IA da parte del responsabile umano competente.

WEB SCRAPING / DATA SCRAPING: estrazione automatizzata di testi, dati, immagini, contenuti o metadati da siti, banche dati o altre fonti digitali.

OUTPUT IA: testo, codice, elaborato grafico, schema, analisi, traduzione, classificazione o altro contenuto generato dal sistema.

6. PRINCIPI GENERALI DI UTILIZZO

L'IA può essere utilizzata solo come strumento di supporto e mai come sostituto del giudizio professionale umano, pertanto, l'uso dei sistemi di IA è consentito solo come strumento di supporto all'attività lavorativa e non può sostituire la valutazione, il controllo e la responsabilità della persona fisica incaricata.

Inoltre, è vietato adottare decisioni vincolanti, tecniche, contrattuali o legali sulla sola base dell'output p

IN PARTICOLARE, I PRINCIPI CARDINE POSSONO ESSERE ARTICOLATI COME SEGUE:

1. PRINCIPIO DI SUPERVISIONE UMANA SIGNIFICATIVA E RESPONSABILITÀ PROFESSIONALE:

Questo è il principio fondamentale che governa l'intero ecosistema IA di IDRAGEST. L'IA è uno strumento di supporto, non un sostituto del giudizio e della competenza professionale umana.

Questo principio si allinea perfettamente con l'articolo 26 dell'AI Act, che impone ai deployer (come IDRAGEST) di affidare la sorveglianza umana a persone con la competenza e l'autorità necessarie, e con l'articolo 13 della Legge n. 132/2025, che sancisce la prevalenza del lavoro intellettuale nelle professioni.

Nelle procedure di affidamento di contratti pubblici, il principio di supervisione umana assume carattere di obbligo di legge, in virtù dell'art. 13 della Legge n. 132/2025 e delle prescrizioni della Delibera ANAC n. 148/2026, che richiedono la prevalenza del lavoro intellettuale umano, il controllo e la verifica dei risultati ottenuti. Qualsiasi output IA rilevante per la predisposizione dell'offerta tecnica è sempre subordinato alla revisione critica integrale e alla firma del professionista responsabile, che ne assume la piena paternità intellettuale e la responsabilità professionale.

IMPLICAZIONI OPERATIVE PER LE ATTIVITÀ DI IDRAGEST:

PROGETTAZIONE E INGEGNERIA (OPERE CIVILI, BILANCI IDRICI): Qualsiasi calcolo idraulico, dimensionamento strutturale, analisi delle perdite o schema di rete generato da un sistema di IA deve essere considerato una bozza preliminare. L'ingegnere o il progettista responsabile (RTEC, RPROG) ha l'obbligo di verificare, validare e, se necessario, ricalcolare autonomamente i dati prima di apporre la propria firma e assumerne la responsabilità professionale. L'output IA non può mai costituire l'elaborato tecnico definitivo.

SVILUPPO SOFTWARE E SIT: Il codice, gli script o le query generate da un'IA devono essere sottoposti a revisione, test e debug da parte degli sviluppatori. La responsabilità della sicurezza, dell'efficienza e della correttezza funzionale del software finale ricade interamente sul team di sviluppo e non può essere delegata all'IA.

2. PRINCIPIO DI RISERVATEZZA E TUTELA DEI SEGRETI COMMERCIALI

L'utilizzo di sistemi di IA, specialmente quelli basati su cloud e forniti da terze parti, introduce un rischio significativo di fuga di informazioni sensibili e, pertanto, è severamente vietato inserire credenziali o dati riservati/personali non anonimizzati.

La IDRAGEST - Policy IA elenca dettagliatamente le categorie di dati il cui inserimento nei prompt è "assolutamente vietato", tra cui segreti industriali, dati di clienti, informazioni relative a gare e credenziali.

3. PRINCIPIO DI RISPETTO DELLA PROPRIETÀ INTELLETTUALE E DEL DIRITTO D'AUTORE

L'IA opera su due fronti: utilizza dati in input e genera contenuti in output. Entrambe le fasi presentano rischi legati alla violazione del diritto d'autore.

IMPLICAZIONI OPERATIVE PER LE ATTIVITÀ DI IDRAGEST:

Web Scraping e Addestramento: È vietato utilizzare l'IA per estrarre massivamente dati da banche dati tecniche, pubblicazioni scientifiche o siti di concorrenti senza un'esplicita licenza che lo consenta. Questa pratica, oltre a violare i termini di servizio, può configurare un illecito ai sensi della legge sul diritto d'autore.

Verifica degli Output: Gli elaborati testuali, le immagini o il codice generati dall'IA possono contenere porzioni di opere protette da copyright. Il personale di IDRAGEST è tenuto a effettuare controlli anti-plagio e a garantire l'originalità degli elaborati finali, specialmente se destinati alla pubblicazione o alla consegna a un cliente.

Software e Licenze: Il codice generato dall'IA potrebbe includere snippet coperti da licenze open source (es. GPL) con obblighi di condivisione. Il personale tecnico deve verificare la compatibilità di tali licenze con gli obiettivi commerciali del software sviluppato per IDRAGEST o per i suoi clienti.

4. Principio di Trasparenza e Responsabilità Contrattuale

IDRAGEST opera in un settore, quello degli appalti pubblici, dove la trasparenza è un obbligo di legge e un requisito di fiducia.

La Delibera ANAC n. 148 del 1° aprile 2026 ha introdotto l'obbligo esplicito per gli operatori economici di dichiarare se si sono avvalsi di sistemi di IA per la redazione dell'offerta tecnica e se intendono utilizzarli in fase esecutiva.

IMPLICAZIONI OPERATIVE PER LE ATTIVITÀ DI IDRAGEST:

Procedure di Gara: Il Responsabile Amministrativo (RAM), in coordinamento con i responsabili tecnici (RTEC/RPROG), deve tracciare e documentare l'eventuale uso di IA nella preparazione dell'offerta. La dichiarazione resa all'ANAC deve essere veritiera e supportata da evidenze interne. Una dichiarazione mendace può comportare l'esclusione dalla gara e altre sanzioni.

Rapporti con i Clienti: In linea con il principio di trasparenza, qualora l'IA sia utilizzata in modo significativo nell'esecuzione di una commessa, specialmente per servizi di natura intellettuale, è opportuno informare il cliente, garantendo sempre la prevalenza del controllo e della validazione umana, come previsto dalla normativa.

In sintesi, per IDRAGEST l'utilizzo dell'IA è un'opportunità di efficienza che deve essere strettamente incardinata in un sistema di controlli che ponga al centro la responsabilità professionale del tecnico, la tutela del patrimonio informativo aziendale e dei clienti, e il rispetto rigoroso degli obblighi di legge e contrattuali.

7. USI CONSENTITI

L'utilizzo dei sistemi di intelligenza artificiale autorizzati dalla Società è consentito esclusivamente per finalità aziendali strettamente inerenti alle mansioni assegnate e nei limiti delle autorizzazioni nominative rilasciate, mediante uso dei soli strumenti, applicazioni, account e risorse approvati da IDRAGEST.

In coerenza con le attività svolte da IDRAGEST nei settori informatico, ingegneristico, topografico, cartografico, SIT, sviluppo software, progettazione, supporto tecnico-specialistico e predisposizione di offerte tecniche, i sistemi di IA possono essere utilizzati, quali strumenti meramente preparatori, organizzativi o di supporto, per le seguenti attività:

a) ricerche preliminari su fonti normative, standard tecnici, linee guida e documentazione pubblicamente disponibile, fermo l'obbligo di successiva verifica delle fonti originarie e della correttezza del contenuto utilizzato;

b) sintesi, riorganizzazione e schematizzazione non definitive di materiali di lavoro, appunti, testi interni e documentazione tecnica già predisposta dal personale aziendale, purché tali attività non comportino alterazione del contenuto tecnico-scientifico e siano comunque oggetto di revisione umana;

c) supporto alla strutturazione, impaginazione e organizzazione documentale di elaborati tecnici, relazioni metodologiche, offerte tecniche, specifiche funzionali, documentazione progettuale e atti interni, a condizione che i contenuti sostanziali siano integralmente elaborati, controllati e approvati dal personale tecnico competente;

d) revisione grammaticale, linguistica e stilistica di testi tecnici, amministrativi o commerciali già predisposti dai professionisti o dai responsabili aziendali, purché non venga modificato il contenuto sostanziale, tecnico, professionale o contrattuale del documento;

e) generazione di bozze non vincolanti di indici, sommari, strutture documentali, scalette, tracce redazionali, checklist, tabelle descrittive e modelli organizzativi da sottoporre a revisione integrale del responsabile di funzione o del professionista incaricato;

f) supporto allo sviluppo software, alla documentazione tecnica del codice, alla generazione di bozze di script, query, test, commenti e strutture logiche preliminari, fermo restando l'obbligo di verifica, collaudo, controllo di sicurezza, validazione tecnica e controllo di conformità licenziataria da parte del personale competente;

g) organizzazione e classificazione di informazioni e predisposizione di materiali di supporto interno, inclusa l'elaborazione preliminare di dati non riservati o previamente anonimizzati, nel rispetto delle regole aziendali in materia di sicurezza, riservatezza e protezione dei dati;

h) supporto alla traduzione di documentazione tecnica o amministrativa, con obbligo di controllo successivo da parte di un soggetto dotato delle competenze professionali adeguate;

i) attività preparatorie nelle gare pubbliche e nelle offerte tecniche, limitatamente a compiti di natura accessoria e strumentale, quali formattazione, strutturazione, revisione stilistica, sintesi di fonti pubbliche, predisposizione di indici e organizzazione espositiva, fermo il divieto di sostituzione del lavoro intellettuale del professionista e l'obbligo di dichiarazione nei casi previsti dalla disciplina ANAC.

L'utilizzo di cui sopra è ammesso solo ove il sistema di IA non sostituisca il giudizio tecnico, progettuale, professionale o organizzativo del personale di IDRAGEST e non influenzi autonomamente decisioni rilevanti, dovendo l'output costituire unicamente supporto a un'attività umana successivamente riesaminata, verificata e fatta propria dal soggetto competente.

In ogni caso, ogni output generato dal sistema di IA che possa incidere, anche indirettamente, su attività progettuali, tecniche, topografiche, software, amministrative, commerciali, contrattuali o di gara deve essere sottoposto a verifica, validazione e approvazione umana da parte del responsabile aziendale o del professionista competente, che ne assume integralmente la responsabilità.

Resta in ogni caso fermo che gli usi consentiti devono svolgersi nel rispetto delle regole aziendali in materia di sicurezza informatica, tutela delle opere dell'ingegno, licenze software, protezione dei dati, divieto di utilizzo di dati riservati o non anonimizzati, divieto di scraping e di estrazione non autorizzata di testi o dati da opere o banche dati protette, nonché degli obblighi di trasparenza previsti per l'impiego dell'IA nelle offerte e nell'esecuzione di contratti pubblici.

8. DIVIETI ASSOLUTI

È fatto assoluto divieto a tutti i Destinatari di utilizzare sistemi di intelligenza artificiale in modo contrario alla legge, al Modello 231, alla presente procedura, alla Policy IA aziendale, alla PMOG08 e alla PMOG11.

In particolare, è vietato:

a) utilizzare strumenti o account IA non autorizzati dalla Società ovvero impiegare versioni, applicazioni, API, estensioni, plug-in, ambienti cloud o dispositivi non previamente approvati secondo le regole aziendali;

b) inserire nei prompt, negli allegati o nei flussi di addestramento dati, informazioni o documenti aziendali, di clienti o di terzi che non siano preventivamente anonimizzati e autorizzati, inclusi, in particolare: dati personali identificativi, dati particolari, informazioni confidenziali di clienti, segreti

industriali, dati finanziari riservati, informazioni su contenziosi, credenziali, password, token, chiavi API e ogni altra informazione coperta da obblighi di riservatezza;

c) utilizzare dati aziendali per attività di fine-tuning, addestramento o riaddestramento di modelli senza preventiva autorizzazione scritta della Società e senza i necessari presidi di sicurezza, riservatezza e conformità;

d) trattare mediante sistemi di IA dati personali in violazione dei principi di liceità, correttezza, trasparenza, minimizzazione, limitazione della finalità e sicurezza, nonché trattare categorie particolari di dati in assenza dei relativi presupposti di legge;

e) impiegare tecniche subliminali, manipolative o ingannevoli, ovvero sistemi idonei a distorcere in modo apprezzabile il comportamento delle persone, in violazione dei divieti previsti dalla normativa vigente;

f) utilizzare sistemi di IA per inferire, monitorare o classificare emozioni, stati psicologici, attitudini o comportamenti dei lavoratori, fuori dai casi consentiti dalla legge e dalle procedure aziendali, nonché in modo lesivo della dignità, della riservatezza e dei diritti del personale;

g) utilizzare l'output generato dall'IA come elaborato definitivo, ufficiale o validato, senza preventiva verifica, revisione critica e approvazione del responsabile umano competente, specie se riferito a documenti tecnici, progettuali, software, relazioni, offerte, specifiche, comunicazioni a clienti o atti con rilevanza probatoria o contrattuale;

h) generare, diffondere o utilizzare contenuti falsi, alterati o artificialmente manipolati idonei a ingannare sulla loro genuinità, comprese immagini, video o voci, in violazione della normativa penale vigente;

i) violare diritti di proprietà intellettuale, licenze software, diritti d'autore o diritti su banche dati, anche mediante caricamento, riproduzione, estrazione, rielaborazione, condivisione o riutilizzo non autorizzato di contenuti protetti;

j) riprodurre o estrarre testo o dati da opere o altri materiali disponibili in rete o in banche dati in assenza di titolo legittimante, anche tramite sistemi di IA, nonché svolgere attività di scraping, file sharing, upload o download illecito di contenuti protetti;

k) installare, collegare o utilizzare programmi, codici, dispositivi o applicativi non autorizzati che possano compromettere la sicurezza dei sistemi aziendali, eludere controlli, alterare configurazioni, intercettare comunicazioni, acquisire credenziali, danneggiare dati o sistemi o consentire accessi abusivi;

l) aggirare le misure di sicurezza aziendali o utilizzare l'IA in combinazione con strumenti informatici o telematici in modo da esporre la Società a rischi di accesso abusivo, danneggiamento, intercettazione, diffusione illecita di dati o altri reati informatici rilevanti ai fini del D.Lgs. 231/2001;

m) inserire nei sistemi di IA dati o informazioni relativi a gare pubbliche, offerte economiche, strategie commerciali o documentazione riservata di commessa, salvo espressa autorizzazione e previa verifica di conformità alle regole interne e agli obblighi di riservatezza.

Ogni violazione dei presenti divieti costituisce illecito disciplinare e comporta l'applicazione delle misure previste dal sistema disciplinare aziendale, ferma restando ogni ulteriore responsabilità civile, penale, contrattuale e rilevante ai sensi del D.Lgs. 231/2001.

Nella predisposizione di offerte per procedure di affidamento di contratti pubblici, è vietato: **(i)** inserire nei prompt di sistemi IA informazioni relative alla stazione appaltante, ai criteri di aggiudicazione, ai dati economici dell'offerta o a qualsiasi dato classificabile come riservato ai sensi dell'art. 35 del D.Lgs. 36/2023; **(ii)** rendere dichiarazioni false o mendaci in ordine all'utilizzo o al mancato utilizzo dell'IA; **(iii)** generare tramite IA certificazioni, dichiarazioni sostitutive o attestazioni aventi valore giuridico-probatorio da inserire nella documentazione di gara senza validazione documentata del professionista responsabile.

9. PROPRIETÀ INTELLETTUALE, OPERE DELL'INGEGNO E SEGRETI COMMERCIALI

9.1 PRINCIPI GENERALI

L'utilizzo dei sistemi di intelligenza artificiale autorizzati dalla Società deve avvenire nel pieno rispetto della disciplina sulla proprietà intellettuale, sul diritto d'autore, sulla tutela dei programmi per elaboratore, delle banche dati e dei segreti commerciali, sia con riferimento ai contenuti forniti in input ai sistemi di IA, sia con riferimento agli output da questi generati.

Tutti i Destinatari della presente procedura sono tenuti a rispettare i diritti di proprietà intellettuale di IDRAGEST, dei suoi clienti e di terzi in ogni fase dell'attività lavorativa in cui vengano impiegati sistemi di IA, e sono personalmente responsabili delle conseguenze derivanti da un utilizzo non conforme alla normativa vigente e alle prescrizioni aziendali.

9.2 TITOLARITÀ DEGLI OUTPUT GENERATI DALL'IA

I diritti di proprietà intellettuale sugli output generati tramite i sistemi di IA autorizzati, nell'ambito delle attività lavorative di IDRAGEST, spettano alla Società nei limiti di quanto consentito dalla normativa vigente in materia di diritto d'autore e fatti salvi eventuali diritti di terzi.

TUTTAVIA, OCCORRE TENERE PRESENTE CHE:

a) gli output generati tramite IA sono tutelabili dal diritto d'autore solo in presenza di un apporto creativo umano significativo, ai sensi dell'art. 1 della Legge 22 aprile 1941, n. 633. In assenza di tale apporto, l'output non può essere considerato opera dell'ingegno originale tutelata dalla legge sul diritto d'autore e non può essere presentato come tale;

b) IDRAGEST non garantisce l'originalità degli output prodotti dai sistemi di IA. Prima di qualsiasi utilizzo in contesti ufficiali, ogni Utente Autorizzato ha l'obbligo di verificare l'originalità del contenuto generato, accertando l'assenza di violazioni dei diritti di terzi;

c) la titolarità degli output generati è altresì disciplinata dagli artt. 10 e 14.3 delle Condizioni Generali di Contratto di IDRAGEST, che regolano i rapporti con i clienti in ordine ai diritti sugli elaborati prodotti nell'ambito delle commesse.

9.3 OBBLIGHI OPERATIVI IN MATERIA DI PROPRIETÀ INTELLETTUALE

TUTTI I DESTINATARI SONO TENUTI A:

a) utilizzare esclusivamente opere dell'ingegno, banche dati e software nel rispetto dei titoli di licenza validi e delle autorizzazioni dei rispettivi titolari; è fatto divieto assoluto di installare, utilizzare o distribuire programmi privi di licenza valida, software pirata o banche dati senza autorizzazione;

b) verificare la compatibilità delle licenze dei contenuti e del codice eventualmente incorporati negli output generati dall'IA prima di qualsiasi utilizzo commerciale, distribuzione o consegna al cliente, con particolare attenzione ai contenuti protetti da licenze open source con obblighi di condivisione;

c) effettuare verifiche di originalità sugli output IA prima del loro impiego in documenti ufficiali, elaborati tecnici, relazioni, offerte, specifiche, pubblicazioni o qualsiasi atto in cui la paternità intellettuale sia rilevante, avvalendosi degli strumenti di controllo anti-plagio disponibili;

d) rendere apposita disclosure nei casi in cui la paternità intellettuale rilevi ai fini contrattuali o legali, quali, in via esemplificativa: gare d'appalto e offerte tecniche (in conformità alla Delibera ANAC n. 148/2026), pubblicazioni scientifiche o tecniche, deposito di brevetti, redazione di specifiche tecniche per la pubblica amministrazione;

e) proteggere il patrimonio informativo aziendale con misure ragionevolmente adeguate a mantenerlo segreto, in conformità ai requisiti previsti dagli artt. 98 e 99 del D.Lgs. 10 febbraio 2005, n. 30 (Codice della Proprietà Industriale) per la tutela dei segreti commerciali;

f) rispettare le misure tecnologiche di protezione (DRM, cifratura, controllo degli accessi) apposte da terzi titolari di diritti su opere, banche dati e programmi per elaboratore, astenendosi da qualsiasi condotta diretta a eludere, rimuovere o alterare tali misure.

9.4 DIVIETI SPECIFICI IN MATERIA DI PROPRIETÀ INTELLETTUALE E IA

SONO ESPRESSAMENTE VIETATI I SEGUENTI COMPORTAMENTI:

a) violazione delle condizioni di licenza di qualsiasi software, banca dati o strumento di IA, ivi inclusi i sistemi autorizzati dalla Società;

b) acquisto, installazione o utilizzo di software pirata per l'azienda o nell'ambito delle attività aziendali;

c) utilizzo di banche dati senza le necessarie autorizzazioni del titolare dei diritti sui contenuti;

d) condivisione o scambio di file in violazione del diritto d'autore (file sharing non autorizzato), nonché effettuazione di upload o download di contenuti protetti in assenza di titolo legittimante;

e) riproduzione o estrazione di testo o dati da opere o altri materiali disponibili in rete o in banche dati, in violazione degli artt. 70-ter e 70-quater della Legge n. 633/1941, anche attraverso sistemi di intelligenza artificiale. In particolare, è vietato effettuare attività di text and data mining (TDM) non autorizzato in violazione dei limiti di legge, nonché attività di web scraping dirette all'estrazione massiva di contenuti protetti;

f) utilizzo di contenuti protetti da diritto d'autore di terzi per attività di addestramento, fine-tuning o riaddestramento di modelli di IA senza il previo consenso del titolare dei diritti, in violazione degli artt. 70-ter e 70-quater della Legge n. 633/1941;

g) presentare output generati dall'IA come elaborati originali di IDRAGEST – o come opera personale del professionista – in contesti in cui la paternità intellettuale sia rilevante, senza adeguata revisione critica, validazione umana e, ove necessario, disclosure, in particolare nelle gare d'appalto pubbliche, nella consegna di elaborati progettuali, nelle offerte tecniche e nelle comunicazioni ufficiali al cliente;

h) porre in essere, mediante l'accesso alle reti informatiche, condotte illecite costituenti violazioni di diritti sulle opere dell'ingegno protette, quali:

- diffondere in qualsiasi forma opere dell'ingegno non destinate alla pubblicazione o usurparne la paternità;

- detenere qualsiasi mezzo diretto alla rimozione o elusione dei dispositivi di protezione dei programmi di elaborazione;
- rimuovere o alterare informazioni elettroniche inserite nelle opere protette o comparenti nelle loro comunicazioni al pubblico, circa il regime dei diritti sulle stesse gravanti;

i) generare, cedere, pubblicare o diffondere senza consenso, tramite sistemi di IA, immagini, video o voci falsificati o alterati, idonei a indurre in inganno sulla loro genuinità, in violazione dell'art. 612-quater del codice penale;

j) inserire dati riservati, segreti industriali, know-how aziendale, planimetrie tecniche, metodologie proprietarie o dati di clienti in sistemi di IA esterni privi di adeguate garanzie contrattuali di riservatezza, di sicurezza e di non riutilizzo per l'addestramento del modello, con conseguente rischio di esfiltrazione del patrimonio informativo tutelato come segreto commerciale.

9.5 TUTELA DEI SEGRETI COMMERCIALI E DEL KNOW-HOW AZIENDALE

Costituiscono segreti commerciali di IDRAGEST, soggetti a protezione ai sensi degli artt. 98 e 99 del D.Lgs. 30/2005 e della Direttiva (UE) 2016/943, le informazioni e le esperienze tecnico-industriali e commerciali che soddisfino congiuntamente i requisiti di segretezza, valore economico e adeguata segretazione. Rientrano in tale categoria, a titolo esemplificativo e non esaustivo:

1. le metodologie proprietarie di rilievo, restituzione e analisi delle reti idriche e fognarie;
2. gli algoritmi e gli strumenti software sviluppati internamente;
3. le specifiche tecniche dei sistemi SIT realizzati per i clienti;
4. i dati tecnici di rete e di consistenza delle infrastrutture gestite;
5. le strategie commerciali, le condizioni economiche delle offerte, i dati di gara;
6. le basi di dati clienti e le condizioni contrattuali praticate.

In nessun caso tali informazioni possono essere inserite in sistemi di IA non autorizzati o privi di adeguate clausole contrattuali di riservatezza e non-training. L'eventuale violazione di tale divieto può configurare una condotta illecita rilevante ai sensi dell'art. 99 del Codice della Proprietà Industriale, nonché ai fini della responsabilità degli enti ai sensi del D.Lgs. 231/2001.

9.6 RAPPORTI CON FORNITORI E SUBFORNITORI

Nei rapporti con fornitori di componenti software, dataset, modelli di IA o servizi cloud, IDRAGEST deve formalizzare per iscritto le condizioni di utilizzo dei dati e degli output, con particolare attenzione a:

1. titolarità e licenza degli output e dei modelli prodotti o sviluppati nell'ambito della commessa;
2. divieto di utilizzo dei dati aziendali per l'addestramento del modello del fornitore;
3. obblighi di riservatezza e di non-divulgazione dei segreti commerciali di IDRAGEST e dei suoi clienti;
4. audit rights e diritto di verifica del rispetto delle condizioni contrattuali;
5. clausole di responsabilità per violazioni del diritto d'autore o dei segreti commerciali imputabili al fornitore.

Tali clausole devono essere inserite nei contratti con i fornitori prima di qualsiasi attività di sviluppo, integrazione o utilizzo congiunto di sistemi di IA.

9.7 REATI PRESUPPOSTO E IMPLICAZIONI 231

Le condotte vietate dalla presente procedura in materia di proprietà intellettuale e segreti commerciali possono integrare reati rilevanti ai fini della responsabilità amministrativa della Società ai sensi del D.Lgs. 231/2001, e in particolare:

1. i delitti in materia di violazione del diritto d'autore previsti dagli artt. 171, 171-bis, 171-ter, 171-septies e 171-octies della Legge n. 633/1941, richiamati dall'art. 25-novies del D.Lgs. 231/2001, con applicazione all'ente della sanzione pecuniaria sino a cinquecento quote e delle sanzioni interdittive;
2. i delitti informatici di cui all'art. 24-bis del D.Lgs. 231/2001, ivi inclusi l'accesso abusivo a sistemi informatici (art. 615-ter c.p.) e il danneggiamento di sistemi informatici (artt. 635-bis e ss. c.p.);
3. la violazione del segreto industriale e gli atti di concorrenza sleale, rilevanti civilmente e penalmente ai sensi degli artt. 98, 99 del D.Lgs. 30/2005 e dell'art. 623 c.p.;
4. l'illecita diffusione di contenuti generati o alterati con sistemi di IA, prevista dall'art. 612-quater c.p., introdotto dalla Legge n. 132/2025.

9.8 CONTROLLI, SEGNALAZIONI E SANZIONI

Ogni violazione della presente procedura in materia di proprietà intellettuale costituisce illecito disciplinare e deve essere segnalata immediatamente al Responsabile IA, al Responsabile di funzione competente e all'Organismo di Vigilanza.

L'Organismo di Vigilanza effettua controlli periodici sul rispetto delle prescrizioni del presente paragrafo, con facoltà di accedere alla documentazione relativa a licenze, contratti con fornitori di IA, log di utilizzo e verifiche di originalità degli output. Le risultanze di tali controlli sono oggetto di flusso informativo periodico verso l'Organo Amministrativo.

10. SICUREZZA INFORMATICA E CONTROLLI TECNICI

L'utilizzo dei sistemi di intelligenza artificiale autorizzati dalla Società deve avvenire nel rispetto delle misure tecniche, organizzative e procedurali adottate da IDRAGEST a tutela della sicurezza dei sistemi informativi, della riservatezza delle informazioni, della disponibilità dei servizi, dell'integrità dei dati e della prevenzione dei reati informatici rilevanti ai sensi del D.Lgs. 231/2001.

In coerenza con la Policy IA aziendale e con la PMOG08, i sistemi di IA devono essere utilizzati esclusivamente all'interno dell'ecosistema tecnologico approvato dalla Società, mediante account aziendali nominativi, strumenti autorizzati e configurazioni conformi ai requisiti di sicurezza, tracciabilità e controllo definiti internamente.

Le misure di sicurezza applicabili ai sistemi di IA devono essere adeguate e proporzionate al rischio, tenendo conto della natura dei dati trattati, delle finalità d'uso, del contesto operativo e delle minacce ragionevolmente prevedibili, in conformità all'art. 24 del D.Lgs. 138/2024 e al Regolamento di esecuzione (UE) 2024/2690. **IN PARTICOLARE, TALI MISURE DEVONO INCLUDERE ALMENO:**

a) politiche di analisi e trattamento del rischio cyber, con specifica considerazione dei rischi connessi all'uso dell'IA, inclusi data poisoning, model poisoning, prompt injection, adversarial attacks, esfiltrazione dei dati, compromissione degli account, phishing, deepfake e utilizzo distorto degli output;

b) procedure formalizzate di gestione degli incidenti, comprensive di rilevazione, contenimento, analisi, eradicazione, ripristino, conservazione delle evidenze, escalation interna e flussi informativi verso le funzioni competenti e l'Organismo di Vigilanza;

c) misure di continuità operativa e disaster recovery, inclusi backup periodici, verifica dei ripristini, ridondanza ove necessaria e procedure di gestione delle crisi, in modo da garantire la resilienza dei processi aziendali anche in caso di incidente informatico o indisponibilità del fornitore del servizio IA;

d) misure di controllo degli accessi, basate su identità nominative, segregazione dei privilegi, principio del minimo privilegio, autenticazione forte o multifattore, disattivazione tempestiva delle utenze non più necessarie e revisione periodica dei profili autorizzativi;

e) misure di cifratura e protezione delle comunicazioni, sia in transito sia a riposo, nonché protezione degli endpoint, dei collegamenti remoti, delle reti wireless e delle interfacce applicative utilizzate per l'accesso ai sistemi IA;

f) logging, tracciabilità e conservazione delle evidenze, con registrazione degli accessi, delle sessioni, dei prompt, degli output rilevanti, dei file caricati, dell'identità dell'utente, della data, dell'ora, del modello utilizzato e della finalità dichiarata dell'uso, con conservazione dei log e delle conversazioni rilevanti per almeno 12 mesi, salvo maggiore durata necessaria per esigenze di audit, contenzioso o indagini interne;

g) monitoraggio continuo e controlli periodici di sicurezza, comprensivi di vulnerability assessment, penetration test, verifiche di configurazione, controlli sui log, test di backup e riesami di conformità almeno periodici e comunque in occasione di incidenti significativi o modifiche rilevanti del contesto operativo;

h) misure di sicurezza della supply chain, con preventiva valutazione dei fornitori di servizi IA, cloud, hosting, manutenzione o integrazione software, sotto il profilo della giurisdizione, delle garanzie contrattuali, della sicurezza dell'infrastruttura, delle certificazioni possedute, della gestione degli incidenti, dell'eventuale rischio di vendor lock-in e del divieto di riutilizzo dei dati aziendali per addestramento non autorizzato;

i) programmi di formazione e sensibilizzazione periodica, destinati a dipendenti, collaboratori e utenti autorizzati, in materia di cybersecurity, utilizzo sicuro dei sistemi di IA, protezione delle credenziali, riconoscimento di attacchi di social engineering e corretta gestione dei dati.

Resta fermo il divieto assoluto di inserire nei prompt, negli allegati o nei flussi di utilizzo dei sistemi IA dati riservati, credenziali, segreti industriali, dati personali non anonimizzati o informazioni di commessa non autorizzate, anche quando le piattaforme utilizzate offrano garanzie contrattuali di sicurezza, cifratura e controllo degli accessi, poiché tali garanzie non escludono l'obbligo di minimizzazione, anonimizzazione e stretta necessità del trattamento.

Ogni output generato dai sistemi di IA che sia destinato a incidere su attività tecniche, progettuali, software, documentali, amministrative, commerciali o contrattuali deve essere sottoposto a validazione umana preventiva, con verifica di accuratezza, coerenza, sicurezza, liceità dell'utilizzo dei dati e assenza

di anomalie tecniche o contenutistiche, restando vietato qualsiasi affidamento automatico o acritico sull'output prodotto.

In caso di incidente informatico, anomalia di sicurezza, fuga di dati, caricamento errato di informazioni riservate, compromissione di account, output anomali o sospetto abuso del sistema IA, l'utente deve darne immediata comunicazione al Responsabile IA, alla funzione IT/Cybersecurity e, ove pertinente, al DPO, attivando senza ritardo le procedure di contenimento e gestione previste dalla documentazione interna.

Tutte le attività di controllo, verifica, audit, manutenzione remota, gestione incidenti e riesame delle misure di sicurezza devono essere documentate e rese disponibili, per quanto di competenza, all'Organismo di Vigilanza, ai fini del monitoraggio sull'effettiva attuazione della presente procedura e della prevenzione dei reati-presupposto.

11. VALUTAZIONE PREVENTIVA E AUTORIZZAZIONE D'USO

11.1 FINALITÀ E AMBITO DEL PARAGRAFO

L'utilizzo di qualsiasi sistema di intelligenza artificiale da parte del personale di IDRAGEST è subordinato a una valutazione preventiva di ammissibilità, rischio e conformità e al rilascio di una autorizzazione nominativa formale, secondo le regole stabilite dalla presente procedura, dalla Policy IA aziendale.

La valutazione preventiva non costituisce un adempimento burocratico, ma uno strumento di controllo sostanziale finalizzato a:

1. prevenire la commissione di reati presupposto ai sensi del D.Lgs. 231/2001, in particolare quelli informatici (art. 24-bis) e quelli in materia di violazione del diritto d'autore (art. 25-novies);
2. garantire il rispetto della normativa sulla protezione dei dati personali (GDPR e D.Lgs. 196/2003) e della cybersecurity (D.Lgs. 138/2024 e Reg. (UE) 2024/2690);
3. assicurare la conformità all'AI Act (Reg. (UE) 2024/1689) in relazione agli obblighi specifici dei deployer;
4. tutelare il patrimonio informativo, i segreti commerciali, il know-how e la proprietà intellettuale di IDRAGEST e dei suoi clienti.

11.2 SOGGETTI COINVOLTI NELLA VALUTAZIONE PREVENTIVA E NELL'AUTORIZZAZIONE

La valutazione preventiva è condotta in modo integrato dal Responsabile IA. Il Responsabile IA il soggetto centrale della procedura autorizzativa.

1. riceve le richieste di accesso ai sistemi IA;
2. verifica la sussistenza dei requisiti tecnici, organizzativi e giuridici;
3. approva o rigetta la richiesta, anche su parere delle funzioni di controllo;
4. gestisce il registro degli utenti autorizzati;
5. revoca o sospende le autorizzazioni in caso di violazione, cessazione del rapporto o mutamento del contesto di rischio.

L'AUTORIZZAZIONE HA CARATTERE:

1. **personale:** non è cedibile né condivisibile con altri soggetti;
2. **limitato:** circoscritto alle finalità, agli strumenti e ai dati indicati nel documento di autorizzazione;
3. **revocabile:** può essere sospesa o revocata in qualsiasi momento al ricorrere dei presupposti;
4. **non trasferibile:** cessa automaticamente in caso di modifica delle mansioni, cessazione del rapporto o variazione significativa delle condizioni di rischio.

IL RILASCIO DELL'AUTORIZZAZIONE NON ESONERA L'UTENTE DAI PROPRI OBBLIGHI DI:

1. supervisione umana e validazione degli output;
2. rispetto dei divieti procedurali;
3. tutela della riservatezza e dei segreti commerciali;
4. osservanza della normativa sulla proprietà intellettuale;
5. segnalazione di anomalie, incidenti o violazioni.

11.3 RIESAME PERIODICO DELLE AUTORIZZAZIONI

Le autorizzazioni rilasciate devono essere soggette a riesame periodico, con cadenza almeno annuale, e comunque in occasione di:

1. variazione delle mansioni o del ruolo dell'utente;
2. aggiornamento degli strumenti IA autorizzati o modifica dei termini di servizio del fornitore;
3. variazione del contesto operativo o della commessa di riferimento;
4. rilevazione di un incidente di sicurezza o di una violazione della presente procedura;
5. aggiornamento normativo rilevante;
6. cessazione del rapporto lavorativo o di collaborazione.

Il riesame è condotto dal Responsabile IA, con il coinvolgimento delle funzioni competenti, e dà luogo a conferma, modifica, limitazione o revoca dell'autorizzazione. L'esito è documentato e archiviato nel registro utenti IA.

11.4 REVOCA E SOSPENSIONE DELL'AUTORIZZAZIONE

L'autorizzazione è revocata o sospesa con effetto immediato nei seguenti casi:

1. violazione accertata o anche solo sospettata della presente procedura o della Policy IA;
2. utilizzo dello strumento per finalità diverse da quelle autorizzate;
3. inserimento di dati vietati nei prompt del sistema IA;
4. incidente di sicurezza riconducibile all'uso del sistema;
5. cessazione del rapporto lavorativo o di collaborazione;
6. indisponibilità o revoca della formazione obbligatoria;
7. segnalazione dell'OdV o di un responsabile di funzione.

La revoca o sospensione è disposta dal Responsabile IA mediante comunicazione scritta all'utente, con contestuale disabilitazione dell'account, archiviazione del fascicolo e, ove pertinente, comunicazione all'OdV e attivazione del sistema disciplinare.

12. VALIDAZIONE UMANA E QUALITÀ DEGLI OUTPUT

In conformità ai principi di affidabilità, trasparenza e accountability previsti dal Modello 231, dalla normativa vigente (Reg. UE 2024/1689, L. 132/2025) e dalla giurisprudenza, nessun output generato, in tutto o in parte, da un sistema di IA può essere utilizzato per scopi professionali, integrato in elaborati finali, trasmesso a clienti o terzi, o impiegato in documenti di gara senza essere stato sottoposto a una procedura di validazione umana.

L'operatore che utilizza l'IA e il responsabile che approva l'output finale si assumono la piena responsabilità professionale, civile e penale del suo contenuto, come se fosse stato elaborato interamente con strumenti tradizionali.

La validazione è obbligatoria per tutti gli output che possono incidere su:

ELABORATI TECNICI: Calcoli idraulici, bilanci idrici, rilievi, planimetrie, schemi di rete, specifiche tecniche per SIT, progetti di opere civili.

SOFTWARE E SCRIPT: Codice sorgente, query per database, configurazioni di sistema.

DOCUMENTAZIONE DI GARA: Offerte tecniche, relazioni metodologiche, cronoprogrammi.

DOCUMENTI CONTRATTUALI E REPORTISTICA: Relazioni di collaudo, valutazioni tecnico-economiche, comunicazioni ufficiali.

L'utilizzatore autorizzato è, dunque, quel "centro di imputazione" all'interno di IDRAGEST: egli non è un mero tramite tra il sistema di IA e l'output finale, ma il soggetto che, attraverso la propria validazione, trasforma un elaborato automatico in un atto professionale di cui assume piena responsabilità.

L'utilizzatore assuma la responsabilità professionale e la paternità intellettuale dell'elaborato, in presenza di un apporto umano significativo, e non presenti output IA come opera originale senza adeguata revisione e disclosure quando rilevante.

12.1 Obblighi di Protezione dei Dati e Anonimizzazione degli Input

Prima ancora della validazione dell'output, l'utilizzatore ha precisi obblighi che attengono alla fase di generazione dell'output stesso:

1. Divieto assoluto di inserire nei prompt dati riservati, segreti industriali, credenziali di sistema o dati personali senza preventiva verifica di conformità interna;
2. Obbligo di anonimizzare i dati prima di inserirli nei sistemi di IA, sostituendo identificatori con valori generici o fittizi;
3. Obbligo di eliminazione immediata delle conversazioni contenenti informazioni sensibili o riservate dopo il loro utilizzo.

Questi obblighi attuano i principi di minimizzazione e limitazione della finalità del GDPR e prevengono la configurazione di reati informatici rilevanti ai sensi dell'art. 24-bis del D.Lgs. 231/2001, presidiati dalla PMOG 08.

13. Gare pubbliche e contratti

Per i servizi di natura intellettuale, la procedura deve recepire integralmente le dichiarazioni richieste da ANAC, distinguendo:

1. mancato uso dell'IA;
2. uso dell'IA nella redazione dell'offerta tecnica;
3. eventuale uso in fase esecutiva, con garanzia di conformità al Regolamento UE 2024/1689, alla legge n. 132/2025 e alla disciplina privacy.

DEVONO INOLTRE ESSERE PREVISTI:

1. conservazione della documentazione per almeno 5 anni;
2. tracciabilità dei prompt/output rilevanti;
3. prevalenza del lavoro umano;

4. divieto di generare certificazioni, dichiarazioni sostitutive o elaborati tecnici vincolanti senza validazione.

IL RISCHIO PRESIDIATO È DUPLICE E DI NATURA QUALITATIVA DIVERSA:

Rischio di illecito concorrenziale e reputazionale: presentare in gara output IA come elaborati originali del professionista, senza adeguata validazione, espone IDRAGEST all'esclusione dalla gara, alla risoluzione del contratto e all'iscrizione nel casellario ANAC;

Rischio di responsabilità 231: le condotte più gravi (dichiarazioni mendaci, uso non consentito di dati riservati, omissioni verso l'ODV) possono integrare reati presupposto rilevanti ai sensi del D.Lgs. 231/2001, con conseguente responsabilità amministrativa dell'ente.

13-BIS. GESTIONE DELL'IA NELLE PROCEDURE DI GARA PUBBLICA E NEGLI APPALTI

13-bis.1 Ambito e finalità del capitolo

Il presente capitolo disciplina le modalità operative con cui IDRAGEST S.r.l. gestisce l'utilizzo dei sistemi di IA autorizzati nell'ambito delle procedure di affidamento di contratti pubblici, sia nella fase di predisposizione dell'offerta che nella fase di esecuzione del contratto. Le disposizioni del presente capitolo si applicano a tutto il personale coinvolto nelle attività di gara e si coordinano con la Policy IA aziendale, con la PMOG11 e con la PMOG08, nonché con le Condizioni Generali di Contratto di IDRAGEST.

Il capitolo recepisce integralmente i contenuti della Delibera ANAC n. 148 del 1° aprile 2026 e del relativo aggiornamento del Bando tipo n. 1-2023, in materia di dichiarazioni sull'uso dell'IA nelle gare pubbliche.

13-bis.2 Principi applicabili alle gare pubbliche

In coerenza con la normativa vigente, l'uso dell'IA nelle attività di gara di IDRAGEST è governato dai seguenti principi inderogabili:

STRUMENTALITÀ: l'IA può essere utilizzata esclusivamente per svolgere attività di supporto nella predisposizione dell'offerta tecnica. Non può in nessun caso sostituire il giudizio professionale del tecnico responsabile.

PREVALENZA DEL LAVORO INTELLETTUALE UMANO: ogni elaborato tecnico, ogni relazione metodologica, ogni progetto, ogni proposta organizzativa e ogni documento valutativo deve essere frutto prevalente del

lavoro intellettuale del professionista responsabile (RPROG, RTEC, RSCM), che ne assume la piena responsabilità tecnica.

VALIDAZIONE UMANA DOCUMENTATA: prima della trasmissione dell'offerta, ogni parte del documento tecnico in cui sia stato impiegato un sistema di IA deve essere sottoposta a revisione critica integrale, con approvazione e firma del professionista responsabile.

TRASPARENZA: IDRAGEST dichiara in modo veridico, nella propria offerta, se ha utilizzato o meno sistemi di IA, specificando quali sistemi e per quali parti dell'offerta tecnica.

RISERVATEZZA ASSOLUTA DEI DATI DI GARA: è fatto divieto assoluto di inserire nei prompt di qualsiasi sistema di IA informazioni relative alla stazione appaltante, ai criteri di aggiudicazione, ai dati economici dell'offerta, alle strategie competitive, alle informazioni riservate del cliente o a qualsiasi altro dato classificabile come riservato ai sensi dell'art. 35 del D.Lgs. 36/2023.

CONFORMITÀ NORMATIVA: ogni utilizzo dell'IA nelle gare deve avvenire nel rispetto del Regolamento (UE) 2024/1689, della Legge n. 132/2025 e della normativa sul trattamento dei dati personali (Regolamento (UE) 2016/679 e D.Lgs. 196/2003).

13-BIS.3 ATTIVITÀ CONSENTITE E ATTIVITÀ VIETATE NELLA PREDISPOSIZIONE DELL'OFFERTA

13-BIS.3.1 ATTIVITÀ CONSENTITE

Nell'ambito della predisposizione dell'offerta tecnica, l'utilizzo dell'IA è consentito esclusivamente per le seguenti attività di natura strumentale e di supporto:

1. supporto redazionale e revisione stilistica di testi non tecnici;

2. generazione di bozze di struttura documentale, indici e sommari;

3. sintesi di fonti normative o tecniche di dominio pubblico;

4. traduzioni di documenti tecnici, soggette a revisione da parte del tecnico competente;

5. supporto nella formattazione, nell'impaginazione e nell'organizzazione visiva dei documenti;

6. ricerche preliminari su normativa tecnica, standard di settore e best practice, con verifica umana obbligatoria.

13-BIS.3.2 ATTIVITÀ VIETATE

È fatto espresso divieto di utilizzare l'IA per:

1. la generazione automatica di elaborati tecnici vincolanti (relazioni di calcolo, verifiche idrauliche, bilanci idrici, rilievi topografici, schemi di rete), anche parziale, senza revisione critica documentata del professionista responsabile;

2. l'inserimento nei prompt di dati economici dell'offerta, di informazioni sulla stazione appaltante o sui criteri di valutazione;

3. la presentazione di output IA come elaborati originali del professionista, in contesti in cui la paternità intellettuale sia rilevante o richiesta;

4. la generazione di certificazioni, dichiarazioni sostitutive, attestazioni di conformità o qualsiasi altro documento avente valore giuridico-probatorio;

5. la generazione o la manipolazione di immagini, video o elaborati grafici tecnici (planimetrie, schemi SIT, mappe di rete) senza validazione tecnica del professionista competente.

13-BIS.4 DICHIARAZIONI OBBLIGATORIE IN GARA: SCHEMA OPERATIVO

13-BIS.4.1 SCHEMA DICHIARATIVO PER L'OFFERTA

Nella domanda di partecipazione o nell'offerta tecnica, il Responsabile Amministrativo (RAM), previa verifica con il Responsabile IA e con i responsabili tecnici di progetto (RPROG/RTEC/RSCM), deve includere obbligatoriamente una delle seguenti dichiarazioni alternative, conformi alla Delibera ANAC n. 148/2026:

DICHIARAZIONE A – MANCATO USO DELL'IA:

«*IDRAGEST S.r.l. DICHIARA che nella predisposizione dell'offerta non si è avvalsa di sistemi di intelligenza artificiale.*»

DICHIARAZIONE B – USO DELL'IA (PER SERVIZI NON INTELLETTUALI):

«*IDRAGEST S.r.l. DICHIARA che nella predisposizione dell'offerta si è avvalsa di sistemi di intelligenza artificiale per la redazione dell'offerta tecnica e che l'utilizzo di tali sistemi è avvenuto nel rispetto del Regolamento UE 2024/1689, della legge n. 132 del 2025 e della vigente normativa sul trattamento e protezione dei dati (Regolamento UE 2016/679, decreto legislativo n. 196 del 2003).*»

DICHIARAZIONE C – USO DELL'IA PER SERVIZI DI NATURA INTELLETTUALE (SCHEMA RAFFORZATO):

«*IDRAGEST S.r.l. DICHIARA che nella predisposizione dell'offerta si è avvalsa dei seguenti sistemi di intelligenza artificiale [indicare il/i sistema/i utilizzato/i] per lo svolgimento di attività meramente strumentali e di supporto nella redazione della/e seguenti parte/i dell'offerta tecnica [indicare le parti], nel rispetto del Regolamento UE 2024/1689, della legge n. 132 del 2025 e della vigente normativa sul trattamento e protezione dei dati (Regolamento UE 2016/679, D.Lgs. 196/2003).*»

13-BIS.4.2 SCHEMA DICHIARATIVO PER LA FASE ESECUTIVA (POST-AGGIUDICAZIONE)

In caso di aggiudicazione del contratto, IDRAGEST deve altresì rendere la seguente dichiarazione in ordine all'utilizzo dell'IA nell'esecuzione delle prestazioni:

DICHIARAZIONE D – IMPEGNO IN FASE ESECUTIVA CON USO DELL'IA:

«*IDRAGEST S.r.l. DICHIARA che, ai fini dell'espletamento delle prestazioni oggetto del contratto, si avvarrà di sistemi di intelligenza artificiale al fine esclusivo di supportare ed efficientare il servizio, assicurando comunque la prevalenza del lavoro intellettuale, il controllo e la verifica dei risultati ottenuti e garantendo che l'uso di tali sistemi avverrà nel rispetto del Regolamento UE 2024/1689, della legge n. 132 del 2025 e della vigente normativa sul trattamento e protezione dei dati (Regolamento UE 2016/679, decreto legislativo n. 196 del 2003).*»

13-BIS.5 PROCEDURA DI VERIFICA PRE-OFFERTA: CHECKLIST OPERATIVA OBBLIGATORIA

Prima della sottoscrizione e trasmissione di qualsiasi offerta, il RAM, in coordinamento con il Responsabile IA e con i responsabili tecnici coinvolti, è tenuto a eseguire e documentare le seguenti verifiche:

NUMERO	ATTIVITÀ DI VERIFICA	RESPONSABILE	DOCUMENTAZIONE RICHIESTA
1	Identificare se e in quale misura è stato utilizzato l'IA nella predisposizione dell'offerta (quali parti, quali strumenti)	RPROG/RTEC/RSCM	Dichiarazione interna dell'uso IA
2	Verificare che gli strumenti utilizzati siano nella lista degli strumenti IA autorizzati dalla società	Responsabile IA	Estratto dal registro strumenti approvati
3	Verificare che i dati inseriti nei prompt non includano informazioni riservate della stazione appaltante o dell'offerta economica	Responsabile IA + RAM	Checklist anonimizzazione dati
4	Raccogliere la conferma scritta del professionista responsabile che gli output IA sono stati oggetto di revisione critica e validazione tecnica	RPROG/RTEC	Attestazione di validazione firmata
5	Raccogliere e archiviare i log dei prompt e degli output rilevanti	Responsabile IA	Log estratti dalla piattaforma IA

6	Selezionare la dichiarazione ANAC applicabile (A, B, C o D)	RAM	Dichiarazione selezionata nel modulo
7	Far approvare la dichiarazione dal legale rappresentante	PRES	Firma digitale/autografa sull'offerta

Tutta la documentazione raccolta nella checklist deve essere conservata per un periodo minimo di 5 anni dalla data di presentazione dell'offerta.

13-BIS.6 OBBLIGHI DI TRACCIABILITÀ E CONSERVAZIONE

13-BIS.6.1 REGISTRO GARE CON USO IA

Il RAM, con il supporto del Responsabile IA, mantiene un Registro delle gare con utilizzo dell'IA, aggiornato per ciascuna procedura, contenente almeno:

1. identificativo della gara (CIG, denominazione, stazione appaltante);

2. data di presentazione dell'offerta;

3. tipo di dichiarazione resa (A, B, C o D);

4. strumenti IA utilizzati e versione;

5. parti dell'offerta tecnica in cui è stato impiegato l'IA;

6. nome del professionista responsabile della validazione;

7. riferimenti ai log conservati.

13-BIS.6.2 CONSERVAZIONE DEI LOG DI PROMPT E OUTPUT

I log relativi all'utilizzo dell'IA nella predisposizione di offerte devono essere conservati per un periodo non inferiore a 12 mesi dalla presentazione dell'offerta, e in ogni caso per tutta la durata di eventuali contenziosi.

13-BIS.6.3 DOCUMENTAZIONE DI VALIDAZIONE TECNICA

L'attestazione di revisione critica e validazione tecnica degli output IA, firmata dal professionista responsabile, deve essere conservata per almeno 5 anni unitamente alla documentazione dell'offerta.

13-BIS.7 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Il RAM e il Responsabile IA sono tenuti a comunicare tempestivamente all'Organismo di Vigilanza i seguenti eventi:

1. ogni aggiudicazione di contratto in cui IDRAGEST abbia dichiarato di avvalersi dell'IA nella fase esecutiva;

2. ogni contestazione, rilievo o richiesta di chiarimento da parte della stazione appaltante in relazione alle dichiarazioni IA rese in offerta;

3. ogni uso dell'IA nella predisposizione di un'offerta che si discosti dalle prescrizioni del presente capitolo, anche se rilevato a posteriori;

4. ogni caso in cui la dichiarazione resa in offerta risulti non corrispondente all'effettivo utilizzo dell'IA

L'OdV include tali flussi nel proprio piano di vigilanza periodica e può richiedere in qualsiasi momento accesso al Registro gare con uso IA e alla documentazione di verifica pre-offerta.

CON RIFERIMENTO ALLE PROCEDURE DI GARA, L'ODV VERIFICA CON CADENZA SEMESTRALE:

1. la corretta tenuta del Registro gare con uso IA;
2. la conformità delle dichiarazioni rese nelle offerte rispetto all'effettivo utilizzo documentato dell'IA;
3. la completezza della documentazione di verifica pre-offerta e della documentazione di validazione tecnica;
4. la regolarità dei flussi informativi ricevuti dal RAM in ordine agli eventi rilevanti;
5. l'assenza di contestazioni ANAC o della stazione appaltante non comunicate.

In caso di audit da parte della stazione appaltante o di ANAC, il RAM e il Responsabile IA mettono immediatamente a disposizione dell'OdV tutta la documentazione rilevante.»

13-BIS.8 SISTEMA SANZIONATORIO SPECIFICO PER LE DICHIARAZIONI ANAC

Le seguenti condotte costituiscono illecito disciplinare di particolare gravità e possono determinare, in aggiunta alle sanzioni previste nel sistema disciplinare generale del Modello 231, la segnalazione all'OdV e, nei casi più gravi, la denuncia alle autorità competenti:

1. Rendere dichiarazioni false o mendaci in ordine all'uso o al non uso dell'IA nella predisposizione dell'offerta o nell'esecuzione del contratto. Tale condotta, oltre alle conseguenze disciplinari interne, può determinare l'esclusione dalla gara, la risoluzione del contratto e l'iscrizione nel casellario ANAC.

2. Inserire dati riservati della stazione appaltante o dell'offerta economica nei prompt di sistemi IA, in violazione del divieto di cui al § 13-bis.3.2.

3. Presentare come elaborato originale del professionista un output IA non sottoposto a revisione critica e validazione documentata.

4. Generare tramite IA certificazioni, dichiarazioni sostitutive o attestazioni aventi valore giuridico-probatorio.

5. Omettere di comunicare all'OdV eventi rilevanti ai sensi del § 13-bis.7.

14. INCIDENTI, ANOMALIE E SEGNALAZIONI

Costituisce incidente rilevante ogni anomalia, fuga di dati, accesso abusivo, uso improprio, output errato con impatto operativo, violazione della presente procedura, utilizzo non autorizzato di dati o opere protette, generazione o diffusione di contenuti alterati mediante IA, nonché ogni evento suscettibile di arrecare pregiudizio a IDRAGEST, ai clienti, ai terzi o di integrare rischio ai sensi del D.Lgs. 231/2001.

L'utilizzatore e ogni altro destinatario che rilevi l'evento deve darne immediata segnalazione al Responsabile IA, alla funzione IT/Sicurezza, al DPO se pertinente e all'OdV, trasmettendo tutte le evidenze disponibili.

Il Responsabile IA, con il supporto delle funzioni competenti, provvede alla classificazione dell'evento, all'attivazione delle misure di contenimento, all'eventuale sospensione del sistema o dell'account, alla conservazione dei log, dei prompt e degli output rilevanti, nonché all'apertura del fascicolo incidente.

Resta fermo il coordinamento con la PMOG 08 per gli incidenti di sicurezza, con la PMOG 11 per le violazioni in materia di opere dell'ingegno e con la Policy IA per i profili disciplinari, contrattuali e di protezione dei dati personali.

Ogni anomalia, fuga di dati, uso improprio, output errato con impatto operativo, sospetto accesso abusivo o violazione della presente procedura deve essere segnalato immediatamente al Responsabile IA, alla funzione IT/sicurezza, al DPO se pertinente e all'OdV. In particolare, si intende disciplinare la gestione degli eventi patologici connessi all'uso dei sistemi di IA: anomalie, fughe di dati, usi impropri, output errati con impatto operativo, sospetti accessi abusivi e violazioni della procedura.

LA PROCEDURA DEVE PREVEDERE:

1. escalation interna tempestiva;
2. sospensione dell'uso del sistema in caso di rischio;
3. gestione dell'incidente secondo i playbook cyber aziendali;
4. eventuale notifica al Garante entro 72 ore nei casi di data breach;
5. eventuale segnalazione al CSIRT Italia per incidenti significativi.

14.1 INCIDENTI DI SICUREZZA E ACCESSO

COMPRENDONO:

1. accessi abusivi o sospetti agli account IA;

2. utilizzo non autorizzato di credenziali;

3. compromissione di integrazioni API;

4. alterazione o perdita dei log;

5. output manipolati o non riconducibili ai prompt autorizzati.

14.2 INCIDENTI PRIVACY E CONFIDENZIALITÀ

COMPRENDONO:

1. inserimento nei prompt di dati personali o riservati non anonimizzati;
2. fuga di dati verso provider esterni;
3. output contenenti dati di clienti, dipendenti, reti infrastrutturali o informazioni tecniche riservate;

conservazione impropria di conversazioni o file allegati.

14.3 INCIDENTI TECNICO-OPERATIVI

COMPRENDONO:

1. output errati con impatto operativo;
2. calcoli, relazioni, script o specifiche tecniche inesatti;
3. documenti di gara o di commessa alterati da errori IA;
4. uso dell'output senza validazione umana, quando richiesta.

Per IDRAGEST questo punto è particolarmente critico, perché un output errato può incidere su rilievi, bilanci idrici, progettazione di opere civili, SIT, collaudi e specifiche tecniche.

14.4 INCIDENTI GIURIDICO-REPUTAZIONALI

COMPRENDONO:

1. utilizzo di materiale protetto da diritto d'autore senza verifica;
2. scraping non autorizzato;
3. generazione o uso di deepfake;
4. dichiarazioni non veritiere sull'uso dell'IA in gare pubbliche;
5. mancata conservazione della documentazione di validazione e dei log.

15. FORMAZIONE E CONSAPEVOLEZZA

La formazione in materia di utilizzo dei sistemi di intelligenza artificiale è obbligatoria per personale tecnico, personale amministrativo, responsabili di funzione e per ogni altro soggetto autorizzato all'uso degli strumenti IA aziendali. La formazione costituisce misura organizzativa essenziale ai fini della conformità al Regolamento (UE) 2024/1689. L'accesso agli strumenti IA aziendali è subordinato al completamento di una formazione iniziale obbligatoria. Successivamente devono essere erogati

aggiornamenti almeno annuali, nonché aggiornamenti straordinari in caso di modifiche normative, incidenti rilevanti, introduzione di nuovi strumenti o revisione delle procedure aziendali.

LA FORMAZIONE DEVE COMPRENDERE ALMENO:

1. AI Act e regole aziendali;
2. diritto d'autore, banche dati, anti-plagio e licenze;
3. segreti commerciali, riservatezza e limiti di utilizzo dei prompt;
4. cybersecurity, prompt injection, incident response, logging e protezione credenziali;
5. protezione dati, anonimizzazione, minimizzazione, DPIA e data breach;
6. deepfake, data leakage, bias, hallucinations e validazione umana degli output;
7. obblighi in gare pubbliche, dichiarazioni ANAC, checklist pre-offerta e conservazione documentale

15.1 DIFFERENZIAZIONE PER RUOLO

I contenuti formativi devono essere calibrati in funzione del ruolo, delle competenze tecniche, delle responsabilità e del contesto d'uso del sistema IA, con moduli specifici per funzioni tecniche, amministrative, gare, sicurezza informatica e supervisione.

15.2 VERIFICA E AUTORIZZAZIONE

La formazione deve prevedere verifica finale dell'apprendimento. Il completamento del percorso e il superamento della verifica costituiscono condizione per l'attivazione o il mantenimento dell'autorizzazione all'uso dei sistemi IA aziendali.

15.3 TRACCIABILITÀ E CONSERVAZIONE

La Società conserva evidenza dei programmi svolti, dei materiali didattici, delle presenze, degli esiti dei test e delle attestazioni rilasciate, in modo da garantire la tracciabilità del presidio formativo ai fini interni, di audit e delle verifiche dell'OdV.

16. MONITORAGGIO, AUDIT E FLUSSI VERSO ODV

16.1 FINALITÀ E AMBITO

Il presente paragrafo definisce il sistema di monitoraggio e controllo sull'utilizzo dei sistemi di Intelligenza Artificiale (IA) autorizzati in IDRAGEST S.r.l., con lo scopo di:

1. verificare il rispetto delle disposizioni della presente Procedura e della Policy IA aziendale;

2. garantire la tracciabilità degli accessi, dei prompt, degli output e delle validazioni effettuate;
3. assicurare flussi informativi strutturati e tempestivi verso l'Organismo di Vigilanza (OdV) e il Consiglio di Amministrazione (CDA);
4. prevenire e rilevare condotte suscettibili di integrare illeciti disciplinari, violazioni del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001, o fattispecie penalmente o amministrativamente rilevanti.

Il sistema di monitoraggio è parte integrante del Modello 231 e contribuisce, unitamente ai presidi sostanziali dei paragrafi precedenti, a dimostrare l'efficace attuazione del modello stesso ai sensi degli artt. 6 e 7 D.Lgs. 231/2001.

16.2 GOVERNANCE DEL MONITORAGGIO: RUOLI E RESPONSABILITÀ

Il sistema di monitoraggio è articolato nel modo seguente:

A) RESPONSABILE IA

Coordina l'intero sistema di controllo sull'uso dei sistemi IA. In particolare:

1. pianifica e supervisiona l'esecuzione dei controlli periodici di cui ai punti 16.3 e 16.4;
2. raccoglie e analizza gli esiti delle verifiche;
3. predispone il reporting periodico verso OdV e CDA;
4. gestisce le segnalazioni di anomalie, incidenti e non conformità;
5. funge da punto di contatto operativo per OdV e DPO in materia di sistemi IA;
6. propone misure correttive e ne monitora l'attuazione.

B) FUNZIONE IT/SICUREZZA INFORMATICA

Supporta il Responsabile IA nelle verifiche tecniche, assicurando in particolare:

1. estrazione e messa a disposizione dei log di sistema;
2. controllo sugli account attivi, sulle credenziali, sui privilegi e sull'autenticazione a più fattori (MFA);
3. segnalazione immediata di accessi anomali, alert di sicurezza o data breach.

C) RESPONSABILI DI FUNZIONE / RESPONSABILI DI PROGETTO

Collaborano ai controlli a campione su prompt e output rilevanti nell'ambito delle proprie commesse e aree di competenza. Segnalano tempestivamente al Responsabile IA qualsiasi anomalia rilevata nell'utilizzo dei sistemi IA all'interno dei propri team.

D) ORGANISMO DI VIGILANZA (ODV)

Riceve il reporting periodico e le segnalazioni urgenti. Può disporre in qualsiasi momento l'accesso ai registri, alle evidenze di controllo e ai fascicoli di audit. Può richiedere al Responsabile IA l'esecuzione di verifiche straordinarie.

16.3 CONTROLLI PERIODICI: TIPOLOGIA, CONTENUTO E PERIODICITÀ

16.3.1 CONTROLLI SULL'USO DEGLI ACCOUNT E DEI SISTEMI AUTORIZZATI

PERIODICITÀ: mensile (verifica operativa IT) e trimestrale (verifica formalizzata con reportistica).

CONTENUTO MINIMO:

1. verifica che gli account attivi corrispondano esclusivamente agli Utenti Autorizzati dall'elenco aggiornato;
2. verifica dell'attivazione e del corretto funzionamento dell'autenticazione a più fattori (MFA) per tutti gli utenti;
3. verifica dell'assenza di account condivisi, generici o non nominativi;
4. controllo delle abilitazioni e dei livelli di accesso attribuiti a ciascun utente, in coerenza con il ruolo aziendale;
5. verifica della tempestiva disabilitazione degli account di utenti cessati, trasferiti o privati dell'autorizzazione;
6. rilevazione di eventuali accessi in orari anomali, da indirizzi IP non autorizzati o con volumi anomali di utilizzo.

EVIDENZA DOCUMENTALE: verbale di controllo account/accessi, conservato nel Registro Audit IA.

16.3.2 VERIFICHE SUI LOG DI SISTEMA

PERIODICITÀ: trimestrale (verifica sistematica); immediata in caso di anomalie, incidenti o richieste dell'OdV.

CONTENUTO MINIMO DEI LOG DA VERIFICARE:

1. identità dell'utente (username nominativo);
2. data, ora e durata della sessione;
3. sistema IA utilizzato e versione del modello;
4. tipo di attività svolta (es. elaborazione testi, analisi dati, generazione di codice, elaborazione di documenti tecnici);
5. file o documenti caricati in input;
6. output generati e, ove tecnicamente possibile, loro traccia;

7. eventuali segnalazioni di errore o anomalie.

REQUISITI DI INTEGRITÀ E ACCESSO:

1. i log devono essere conservati in forma integra e inalterabile per almeno 12 mesi, salvo che specifiche commesse, contenziosi in corso o obblighi di legge richiedano un termine superiore;
2. l'accesso ai log è riservato esclusivamente al Responsabile IA, alla funzione IT/Sicurezza, al DPO per i profili di propria competenza e all'OdV;
3. ogni consultazione dei log deve essere essa stessa tracciata, con registrazione del soggetto, della data e della finalità della consultazione;
4. è fatto divieto a qualsiasi utente di cancellare, modificare o alterare i log; tale condotta integra violazione grave del presente Modello.

EVIDENZA DOCUMENTALE: scheda di verifica log, con indicazione degli elementi esaminati, degli esiti e delle eventuali anomalie rilevate; conservata nel Registro Audit IA.

16.3.3 CONTROLLI A CAMPIONE SU PROMPT E OUTPUT RILEVANTI

PERIODICITÀ: su base risk-based, con frequenza minima trimestrale per le aree ad alto rischio (commesse in appalto pubblico, elaborati tecnici destinati a clienti, documentazione di gara, sviluppo software, attività su infrastrutture critiche). Per le attività a rischio ordinario: semestrale.

CRITERI DI CAMPIONAMENTO:

Il campione è determinato dal Responsabile IA, con il supporto dei Responsabili di Funzione, tenendo conto dei seguenti fattori di rischio elevato:

1. output destinati a essere consegnati a clienti o stazioni appaltanti;
2. output impiegati in offerte tecniche o documenti di gara;
3. output che abbiano comportato il caricamento di file o dati in input;
4. output tecnici di rilievo (calcoli idraulici, bilanci idrici, schemi di rete, codice sorgente, relazioni di collaudo);
5. output generati da utenti per i quali siano stati rilevati utilizzi anomali nei log.

CONTENUTO DEL CONTROLLO A CAMPIONE:

PER CIASCUN CAMPIONE SELEZIONATO, IL CONTROLLO DEVE VERIFICARE:

1. che il prompt non contenga dati personali non anonimizzati, dati riservati di clienti, segreti industriali, informazioni su infrastrutture di terzi, credenziali o dati di accesso a sistemi;

2. che il prompt non sia stato strutturato con finalità di data/web scraping illecito;
3. che l'output sia stato sottoposto alla procedura di validazione umana prevista al paragrafo 12, con relativa registrazione nel Registro delle Validazioni IA;
4. che l'output non presenti elementi di potenziale violazione del diritto d'autore (es. riproduzione integrale di testi protetti), verificando, ove necessario, con strumenti anti-plagio;
5. che l'output tecnico, ove utilizzato all'esterno, sia coerente con le norme tecniche di settore e non contenga errori gravi o allucinazioni non corrette in sede di validazione.

EVIDENZA DOCUMENTALE: scheda di controllo campione prompt/output (con check-list standardizzata), conservata nel Registro Audit IA.

16.3.4 AUDIT SU LICENZE, PROVENIENZA DATI, DIVIETI DI SCRAPING E DATA EXTRACTION

PERIODICITÀ: almeno annuale; straordinaria in caso di rinnovo o modifica di contratti con provider IA, introduzione di nuovi sistemi, o richiesta dell'OdV.

CONTENUTO MINIMO DELL'AUDIT:

1. verifica della regolarità e validità delle licenze d'uso dei sistemi IA autorizzati (abbonamenti attivi, condizioni d'uso aggiornate, eventuali limitazioni per uso professionale);
2. verifica delle clausole dei contratti con i provider IA in relazione a: (i) no-training dei dati inseriti dall'utente; (ii) no-retention dei dati; (iii) eventuali restrizioni per utilizzo in appalti pubblici o in settori regolamentati;
3. verifica della provenienza e della liceità dei dataset o delle basi di dati utilizzate dall'utente in input al sistema IA, con particolare riguardo alle attività di SIT, elaborazione dati territoriali, sviluppo software e integrazione di basi di conoscenza;
4. verifica del rispetto del divieto assoluto di web scraping e data extraction tramite IA in violazione delle condizioni d'uso dei siti web e delle banche dati, nonché degli artt. 70-ter e 70-quater L. 633/1941 come vigenti;
5. verifica della conformità delle licenze d'uso di eventuali porzioni di codice open source generate o integrate tramite IA nello sviluppo software;
6. verifica del rispetto delle limitazioni di utilizzo delle cartografie, ortofoto e banche dati tecniche eventualmente caricate nei sistemi IA nell'ambito delle attività di rilievo e di SIT.

EVIDENZA DOCUMENTALE: verbale di audit licenze/dati, con check-list e documentazione contrattuale allegata; conservato nel Registro Audit IA.

16.4 REGISTRO AUDIT IA

Il Responsabile IA istituisce e aggiorna il Registro Audit IA, che costituisce la principale evidenza documentale dell'attività di monitoraggio e controllo.

Il Registro è tenuto in forma strutturata (cartacea o digitale, con accesso controllato) e raccoglie:

1. i verbali dei controlli account/accessi;
2. le schede di verifica log;
3. le schede di controllo campione prompt/output;
4. i verbali di audit licenze/dati;
5. le segnalazioni di anomalie, incidenti e non conformità;
6. le misure correttive adottate e il relativo stato di attuazione;
7. i report periodici trasmessi a OdV e CDA.

Il Registro Audit IA è conservato per almeno 5 anni, salvo termini superiori imposti da specifiche commesse, contenziosi o obblighi di legge. L'OdV ha accesso al Registro in qualsiasi momento.

16.5 GESTIONE DELLE ANOMALIE E DEI TRIGGER DI ESCALATION

Indipendentemente dalla periodicità dei controlli ordinari, il Responsabile IA, i Responsabili di Funzione, la funzione IT/Sicurezza, il DPO e ogni Utente Autorizzato sono tenuti a effettuare segnalazione immediata al Responsabile IA e, nei casi previsti, all'OdV, al DPO e al CDA, al verificarsi di uno dei seguenti eventi:

1. Data breach o sospetta fuga di dati riservati
2. Accessi abusivi o non autorizzati a sistemi IA Responsabile IA, IT/Sicurezza, OdV
3. Inserimento accertato o sospettato di dati riservati di clienti, infrastrutture o dati personali in prompt
4. Output tecnici errati o privi di validazione impiegati in commesse o gare
5. Violazione accertata o sospettata del diritto d'autore (scraping, plagio, data extraction)
6. Mancata o falsa dichiarazione sull'uso dell'IA in gare d'appalto
7. Anomalie rilevanti nei log (cancellazione, alterazione, volumi anomali)
8. Uso improprio dell'IA con possibile rilevanza penale o 231
9. Mancata collaborazione o ostacolo agli audit da parte di utenti

Le segnalazioni urgenti sono effettuate con le modalità operative indicate nella procedura aziendale "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01" e, per i profili di segnalazione degli illeciti, nella "Procedura di gestione del whistleblowing".

16.6 REPORTING PERIODICO VERSO L'ODV E IL CDA

Il Responsabile IA predispone un report periodico sull'utilizzo dei sistemi IA, da trasmettere all'OdV e al CDA con frequenza semestrale, fatta salva la facoltà dell'OdV di richiedere report straordinari in qualsiasi momento.

IL REPORT PERIODICO CONTIENE ALMENO:

1. numero e tipologia dei controlli eseguiti nel periodo di riferimento;
2. esiti dei controlli account e dei log (anomalie rilevate e risolte, utenti disabilitati, accessi anomali);
3. esiti dei controlli a campione su prompt e output (non conformità rilevate, misure correttive);
4. esiti dell'audit licenze/provenienza dati;
5. numero e sintesi degli incidenti e delle non conformità segnalate;
6. misure correttive adottate e relativo stato di attuazione;
7. aggiornamenti sullo stato della formazione degli Utenti Autorizzati;
8. eventuali segnalazioni ricevute attraverso il canale whistleblowing rilevanti ai fini della presente Procedura;
9. indicazioni su variazioni nel parco sistemi IA autorizzati, nuovi contratti con provider, aggiornamenti rilevanti delle condizioni d'uso.

16.7 CONSEGUENZE DISCIPLINARI, PENALI E AMMINISTRATIVE DELLE VIOLAZIONI

La violazione delle disposizioni contenute nella presente Procedura – inclusi gli obblighi di controllo, tracciabilità, segnalazione e reporting di cui al presente paragrafo 16 – costituisce:

(a) Illecito disciplinare, soggetto alle sanzioni previste dal sistema disciplinare aziendale e dal CCNL applicabile, graduate in funzione della gravità della condotta, del grado di intenzionalità, del danno cagionato o potenzialmente cagionabile e del ruolo rivestito nell'organizzazione.

INTEGRANO, IN PARTICOLARE, VIOLAZIONE DISCIPLINARE GRAVE:

1. la cancellazione, l'alterazione o la manomissione non autorizzata dei log di sistema o delle evidenze di audit;

2. l'omissione dolosa di segnalazione di anomalie o incidenti rilevanti;
3. l'ostacolo, anche mediante condotta omissiva, agli audit interni o alle verifiche dell'OdV;
4. la mancata esecuzione dei controlli periodici di propria competenza;
5. la falsa rappresentazione degli esiti dei controlli nei report a OdV o CDA;
6. la mancata dichiarazione dell'uso dell'IA in gare d'appalto in violazione dei criteri stabiliti dalla Delibera ANAC n. 148/2026 e successive.

(b) Violazione del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001, con conseguente possibile compromissione dell'efficacia esimente del Modello stesso e attivazione delle procedure di accertamento e contestazione previste dallo Statuto dell'OdV.

(c) Possibile rilevanza penale o amministrativa, in ragione della condotta concretamente accertata, con particolare riferimento a:

1. reati informatici ex art. 24-bis D.Lgs. 231/2001 (accesso abusivo a sistemi informatici ex art. 615-ter c.p., danneggiamento informatico ex artt. 635-bis ss. c.p., trattamento illecito di dati ex art. 167 D.Lgs. 196/2003);

2. violazioni del diritto d'autore ex art. 25-novies D.Lgs. 231/2001 (scraping illecito, riproduzione non autorizzata di opere protette);

diffusione illecita di contenuti deepfake ex art. 612-quater c.p.;

violazioni della normativa in materia di protezione dei dati personali ai sensi del Reg. UE 2016/679 e del D.Lgs. 196/2003;

3. illeciti connessi a false dichiarazioni in gare d'appalto pubblico.

16.8 RINVIO ALLE PROCEDURE DI FLUSSO INFORMATIVO E WHISTLEBLOWING

Per le modalità operative di comunicazione e segnalazione all'OdV si rinvia alle procedure aziendali:

1. "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01";
2. "Procedura di gestione del whistleblowing".

Il rinvio a tali procedure non elimina né sospende gli obblighi di reporting periodico e di segnalazione urgente previsti dal presente paragrafo 16, che si applicano cumulativamente e in modo autonomo rispetto ai canali di segnalazione generali del Modello.

16.9 DISPOSIZIONI FINALI DEL PARAGRAFO

Il presente paragrafo è soggetto a revisione periodica, con cadenza almeno annuale o in occasione di:

1. aggiornamenti normativi rilevanti (AI Act, D.Lgs. 231/2001, normativa sul diritto d'autore, normativa sulla protezione dei dati);
2. introduzione di nuovi sistemi IA o modifica dei sistemi autorizzati;
3. variazioni organizzative significative;
4. esiti degli audit o delle verifiche OdV che evidenzino criticità nei presidi esistenti.

LA VIOLAZIONE DELLA PRESENTE PROCEDURA E DEI SUOI OBBLIGHI DI COMUNICAZIONE, INTEGRA UNA VIOLAZIONE DEL PRESENTE MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO E, PERTANTO, COSTITUISCE UN ILLECITO DISCIPLINARE PASSIBILE DI SANZIONE AI SENSI DELLA LEGGE VIGENTE IN MATERIA, DELLO STESSO MODELLO 231, NONCHÉ DEL CONTRATTO COLLETTIVO NAZIONALE DI LAVORO APPLICATO.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

ELENCO ALLEGATI

ALLEGATO 1: Codice Etico

ALLEGATO 2: Clausola contrattuale

ALLEGATO 3: Elenco reati sanzionati dal Decreto

ALLEGATO 4: Composizione dell'Organismo di Vigilanza

ALLEGATO 5: Costituzione, compensi, cause di (in)eleggibilità, decadenza e sospensione dei componenti dell'Organismo di Vigilanza

ALLEGATO 6: procedura WHISTLEBLOWING

IDRAGEST

IDRAGEST water engineering	**CODICE ETICO**			
		Rev. 1	22.07.2026	Pag. 1 di 59

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 24.03.2024	ADOZIONE
Rev. 1	CDA DEL 22.07.2026	AGGIORNAMENTO

IDRAGEST S.R.L.

CODICE ETICO

PRINCIPI ETICI E VALORI CHE ISPIRANO LA CULTURA E LA CONDOTTA AZIENDALE DI IDRAGEST S.R.L.

Il presente Codice Etico è stato approvato dal Consiglio di Amministrazione di IDRAGEST S.R.L.

Sommario

1. LA CULTURA DELL'INTEGRITÀ DI IDRAGEST S.R.L. 5
1.1 LA MISSION DI IDRAGEST 6
1.2 LA VISION 6
1.3 FINALITÀ DEL CODICE ETICO 7
1.4 SISTEMA INTEGRATO DI COMPLIANCE 7
ESSO SI COORDINA CON: 7
1.5 DESTINATARI 8
1.6 IMPEGNO DELLA SOCIETÀ 8
ART. 1 – LEGALITÀ 9
ART. 2 – INTEGRITÀ, ONESTÀ E BUONA FEDE 9
ART. 3 – TRASPARENZA E ACCOUNTABILITY 10
ART. 4 – CENTRALITÀ DELLA PERSONA 10
ART. 5 – PARI OPPORTUNITÀ, INCLUSIONE E NON DISCRIMINAZIONE 10
ART. 6 – PROFESSIONALITÀ, COMPETENZA E MIGLIORAMENTO CONTINUO 11
ART. 7 – INNOVAZIONE RESPONSABILE 11
ART. 8 – RISERVATEZZA E TUTELA DELLE INFORMAZIONI 12
ART. 9 – TUTELA DEL PATRIMONIO AZIENDALE E DELLA PROPRIETÀ INTELLETTUALE 12
ART. 10 – SOSTENIBILITÀ E RESPONSABILITÀ SOCIALE 13
ART. 11 – CULTURA DELLA COMPLIANCE 13
ART. 12 – PRINCIPI DI GOVERNANCE 14
ART. 13 – SISTEMA INTEGRATO DI COMPLIANCE 14
ART. 14 – ORGANI AZIENDALI E RESPONSABILITÀ 15
ART. 15 – ORGANISMO DI VIGILANZA 15
ART. 16 – RESPONSABILE DELLA CONFORMITÀ 16
ART. 17 – GOVERNANCE DELL'INTELLIGENZA ARTIFICIALE 16
ART. 18 – SISTEMA DEI CONTROLLI INTERNI 17
ART. 19 – COLLABORAZIONE AI CONTROLLI 17
ART. 20 – CULTURA DELLA PREVENZIONE E DEL MIGLIORAMENTO CONTINUO 17
ART. 21 – CENTRALITÀ DELLE PERSONE 18
ART. 22 – SELEZIONE E VALORIZZAZIONE DELLE RISORSE UMANE 18
ART. 23 – PARI OPPORTUNITÀ, INCLUSIONE E RISPETTO DELLA PERSONA 19
ART. 24 – TUTELA DELLA DIGNITÀ E CONTRASTO ALLE MOLESTIE 19
ART. 25 – REGOLARITÀ DEI RAPPORTI DI LAVORO 20
ART. 26 – FORMAZIONE CONTINUA 20

ART. 27 – UTILIZZO CORRETTO DEGLI STRUMENTI AZIENDALI 21
ART. 28 – UTILIZZO RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE 21
ART. 29 – RISERVATEZZA E PROTEZIONE DEI DATI 22
ART. 30 – SALUTE, SICUREZZA E BENESSERE ORGANIZZATIVO 22
ART. 31 – DOVERE DI COLLABORAZIONE E DI SEGNALAZIONE 23
ART. 32 – PRINCIPI GENERALI 23
ART. 33 – RAPPORTI ISTITUZIONALI 24
ART. 34 – GARE PUBBLICHE, AFFIDAMENTI E CONTRATTI PUBBLICI 24
ART. 35 – RAPPORTI CON PUBBLICI UFFICIALI E INCARICATI DI PUBBLICO SERVIZIO 25
ART. 36 – OMAGGI, OSPITALITÀ E SPESE DI RAPPRESENTANZA 25
ART. 37 – ISPEZIONI, VERIFICHE E CONTROLLI 26
ART. 38 – CONTRIBUTI, FINANZIAMENTI E AGEVOLAZIONI PUBBLICHE 26
ART. 39 – RAPPORTI CON LE AUTORITÀ INDIPENDENTI E L'AUTORITÀ GIUDIZIARIA 27
ART. 40 – TRACCIABILITÀ DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE 27
ART. 41 – PREVENZIONE DELLA CORRUZIONE 28
ART. 42 – PRINCIPIO DI INTEGRITÀ NEI RAPPORTI COMMERCIALI 28
ART. 43 – PRINCIPIO DI TOLLERANZA ZERO VERSO LA CORRUZIONE 28
ART. 44 – CORRUZIONE PUBBLICA E PRIVATA 29
ART. 45 – OMAGGI, LIBERALITÀ, OSPITALITÀ E SPESE DI RAPPRESENTANZA 29
ART. 46 – PAGAMENTI DI FACILITAZIONE 30
ART. 47 – CONFLITTO DI INTERESSI 30
ART. 48 – SELEZIONE DI FORNITORI, CONSULENTI E PARTNER 31
ART. 49 – DUE DILIGENCE E VERIFICA DELLE CONTROPARTI 31
ART. 50 – RAPPORTI CON INTERMEDIARI E CONSULENTI 31
ART. 51 – RAPPORTI CON FORNITORI E SUBAPPALTATORI 32
ART. 52 – DONAZIONI, SPONSORIZZAZIONI E CONTRIBUTI 32
ART. 53 – TUTELA DELLA CONCORRENZA 32
ART. 54 – OBBLIGO DI SEGNALAZIONE 33
ART. 55 – PRINCIPI GENERALI 33
ART. 56 – RAPPORTI CON I CLIENTI 34
ART. 57 – QUALITÀ DEI SERVIZI 34
ART. 58 – RAPPORTI CON FORNITORI E PROFESSIONISTI 34
ART. 59 – RAPPORTI CON CONSULENTI E COLLABORATORI ESTERNI 35
ART. 60 – RAPPORTI CON PARTNER COMMERCIALI, RTI E RETI D'IMPRESA 35
ART. 61 – CONCORRENZA LEALE 36
ART. 62 – TUTELA DELLA PROPRIETÀ INTELLETTUALE E DEL KNOW-HOW 36
ART. 63 – COMUNICAZIONI COMMERCIALI E PUBBLICITÀ 37

ART. 64 – TUTELA DELLA REPUTAZIONE AZIENDALE 37
ART. 65 – TUTELA DEGLI STAKEHOLDER 37
ART. 66 – CLAUSOLE ETICHE E DIRITTO DI REAZIONE 38
ART. 67 – PRINCIPI GENERALI 38
ART. 68 – TUTELA DELLE INFORMAZIONI AZIENDALI 38
ART. 69 – PROTEZIONE DEI DATI PERSONALI 39
ART. 70 – SICUREZZA INFORMATICA 39
ART. 71 – UTILIZZO DEGLI STRUMENTI INFORMATICI 40
ART. 72 – PROPRIETÀ INTELLETTUALE E TUTELA DEL KNOW-HOW 40
ART. 73 – PRINCIPI PER L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE 41
ART. 74 – SUPERVISIONE UMANA 41
ART. 75 – UTILIZZI VIETATI 41
ART. 76 – VERIFICA DEGLI OUTPUT 42
ART. 77 – TRASPARENZA NELL'UTILIZZO DELL'IA 42
ART. 78 – FORMAZIONE E AGGIORNAMENTO 43
ART. 79 – PRINCIPI GENERALI 43
ART. 80 – TUTELA DELL'AMBIENTE 43
ART. 81 – USO EFFICIENTE DELLE RISORSE 44
ART. 82 – INNOVAZIONE PER LA SOSTENIBILITÀ 44
ART. 83 – RESPONSABILITÀ SOCIALE D'IMPRESA 44
ART. 84 – DIRITTI UMANI 45
ART. 85 – SALUTE E SICUREZZA NEI LUOGHI DI LAVORO 45
ART. 86 – RAPPORTI CON LA COLLETTIVITÀ 46
ART. 87 – SOSTENIBILITÀ NELLA CATENA DI FORNITURA 46
ART. 88 – IMPEGNO AL MIGLIORAMENTO CONTINUO 46
ART. 89 – PRINCIPI GENERALI 47
ART. 90 – VERIDICITÀ DELLE REGISTRAZIONI CONTABILI 47
ART. 91 – BILANCIO E COMUNICAZIONI SOCIALI 48
ART. 92 – TRACCIABILITÀ DEI FLUSSI FINANZIARI 48
ART. 93 – GESTIONE DELLE RISORSE FINANZIARIE 48
ART. 94 – PREVENZIONE DEI REATI TRIBUTARI 49
ART. 95 – PREVENZIONE DEI REATI SOCIETARI 49
ART. 96 – PREVENZIONE DEL RICICLAGGIO, AUTORICICLAGGIO E FINANZIAMENTO DEL TERRORISMO 50
ART. 97 – CONSERVAZIONE DELLA DOCUMENTAZIONE 50
ART. 98 – RAPPORTI CON GLI ORGANI DI CONTROLLO 50
ART. 99 – RESPONSABILITÀ INDIVIDUALE 51

ART. 100 – CULTURA DELLA SEGNALAZIONE E DELLA PREVENZIONE 51
ART. 101 – OBBLIGO DI SEGNALAZIONE 51
ART. 102 – PROCEDURA WHISTLEBLOWING 52
ART. 103 – TUTELA DEL SEGNALANTE 53
ART. 104 – SEGNALAZIONI IN MALA FEDE 53
ART. 105 – ORGANISMO DI VIGILANZA 53
ART. 106 – DOVERE DI COLLABORAZIONE 53
ART. 107 – SISTEMA DISCIPLINARE 54
ART. 108 – MISURE NEI CONFRONTI DEI SOGGETTI TERZI 54
ART. 109 – MONITORAGGIO E AGGIORNAMENTO DEL CODICE ETICO 54
ART. 110 – ADOZIONE ED ENTRATA IN VIGORE 55
ART. 111 – DIFFUSIONE DEL CODICE ETICO 55
ART. 112 – FORMAZIONE E SENSIBILIZZAZIONE 56
ART. 113 – COORDINAMENTO CON IL SISTEMA DI COMPLIANCE 56
ART. 114 – INTERPRETAZIONE DEL CODICE ETICO 57
ART. 115 – REVISIONE E AGGIORNAMENTO 57
ART. 117 – IMPEGNO DEI DESTINATARI 57
DISPOSIZIONE FINALE 58
APPENDICE DI DETTAGLIO AI FINI DEL D.LGS. 231/2001 58

PREMESSA

1. LA CULTURA DELL'INTEGRITÀ DI IDRAGEST S.R.L.

Il presente Codice Etico rappresenta la Carta dei Valori di IDRAGEST S.r.l. e costituisce il documento fondamentale attraverso il quale la Società definisce i principi etici, i valori e le regole di comportamento che devono orientare l'attività aziendale e l'operato di tutti coloro che agiscono, a qualsiasi titolo, nell'interesse o per conto della Società.

IDRAGEST considera l'etica, la legalità, la trasparenza e la responsabilità sociale elementi imprescindibili per lo svolgimento della propria attività imprenditoriale e fattori essenziali per la creazione di valore nel lungo periodo.
La Società è consapevole che la propria reputazione rappresenta un patrimonio strategico costruito attraverso comportamenti improntati all'integrità, alla correttezza, alla competenza professionale e al rispetto della persona, dell'ambiente e del mercato.
Per tale ragione, ogni decisione aziendale deve essere assunta nel rispetto non soltanto della normativa vigente, ma anche dei principi etici contenuti nel presente Codice, nella consapevolezza che nessun vantaggio economico o competitivo può giustificare comportamenti contrari alla legge, ai valori aziendali o ai principi di correttezza e buona fede.
Il Codice Etico costituisce parte integrante del sistema di governo societario e del sistema di controllo interno adottato da IDRAGEST e rappresenta il principale strumento di diffusione della cultura della compliance all'interno dell'organizzazione.

1.1 LA MISSION DI IDRAGEST

IDRAGEST S.r.l. opera nel settore dell'ingegneria applicata ai servizi idrici, della progettazione, del rilievo, della digitalizzazione delle infrastrutture e dell'ottimizzazione delle reti idriche e fognarie, perseguendo l'obiettivo di contribuire allo sviluppo di infrastrutture efficienti, resilienti e sostenibili.
Attraverso l'impiego delle migliori competenze professionali, delle tecnologie più avanzate e di processi organizzativi orientati alla qualità, IDRAGEST realizza soluzioni innovative capaci di generare valore per i propri clienti, per la collettività e per il territorio.
La Società promuove un modello di crescita fondato sull'innovazione tecnologica, sulla tutela delle risorse naturali, sulla sicurezza delle infrastrutture, sulla valorizzazione del capitale umano e sul rispetto dei principi di sviluppo sostenibile.

1.2 LA VISION

IDRAGEST intende consolidare il proprio ruolo quale operatore di riferimento nel settore dell'ingegneria applicata alle infrastrutture idriche, distinguendosi per affidabilità, competenza tecnica, innovazione, integrità e responsabilità sociale.

La Società considera la trasformazione digitale, l'impiego responsabile dell'intelligenza artificiale, la prevenzione della corruzione, la sicurezza delle informazioni e la sostenibilità ambientale fattori strategici per il proprio sviluppo e per la creazione di valore durevole nei confronti di clienti, istituzioni, dipendenti, partner commerciali e dell'intera collettività.

1.3 FINALITÀ DEL CODICE ETICO

Il presente Codice Etico ha lo scopo di:

a) definire i valori fondamentali cui deve ispirarsi l'attività della Società;

b) stabilire i principi di comportamento vincolanti per tutti i Destinatari;

c) rafforzare la cultura della legalità e dell'integrità aziendale;

d) prevenire comportamenti illeciti o contrari ai principi di correttezza, trasparenza e buona fede;

e) contribuire all'efficace attuazione del Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D.Lgs. 231/2001;

f) promuovere una gestione responsabile dei rischi aziendali, anche attraverso il coordinamento con le procedure interne e con le politiche di compliance adottate dalla Società;

g) tutelare la reputazione, l'affidabilità e la credibilità di IDRAGEST nei confronti di tutti gli stakeholder;

h) favorire una cultura organizzativa improntata alla responsabilità individuale, alla trasparenza, alla sostenibilità e al miglioramento continuo.

1.4 SISTEMA INTEGRATO DI COMPLIANCE

Il presente Codice costituisce il documento di riferimento dell'intero sistema etico e di compliance di IDRAGEST.

Esso si coordina con:

1. il Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D.Lgs. 231/2001;
2. il Codice Disciplinare;
3. la Procedura Whistleblowing adottata ai sensi del D.Lgs. 24/2023;
4. la Politica Anticorruzione;
5. la Politica sull'uso corretto e responsabile dell'Intelligenza Artificiale;
6. le procedure aziendali in materia di salute e sicurezza sul lavoro;

7. le procedure in materia di protezione dei dati personali, sicurezza informatica e gestione delle informazioni;
8. ogni altra procedura o regolamento aziendale adottato dal Consiglio di Amministrazione.

Le politiche aziendali costituiscono strumenti attuativi dei principi contenuti nel presente Codice e ne disciplinano gli aspetti operativi e specialistici. In caso di contrasto, trova applicazione la disposizione maggiormente idonea a garantire il rispetto della legge, dei principi etici aziendali e del sistema di controllo interno.

1.5 DESTINATARI

Il presente Codice Etico è vincolante per:

- componenti del Consiglio di Amministrazione;
- Organismo di Vigilanza;
- dirigenti;
- dipendenti;
- lavoratori somministrati;
- collaboratori;
- consulenti;
- professionisti incaricati;
- partner commerciali;
- RTI, joint venture e reti di imprese;
- fornitori e subappaltatori;
- clienti, ove contrattualmente richiamato;
- ogni altro soggetto che operi, direttamente o indirettamente, nell'interesse o per conto della Società.

Tutti i Destinatari sono tenuti a conoscere, osservare e promuovere i principi contenuti nel presente Codice, collaborando attivamente alla diffusione della cultura della legalità e della compliance aziendale.

1.6 IMPEGNO DELLA SOCIETÀ

IDRAGEST si impegna a:

- diffondere il presente Codice a tutti i Destinatari;
- garantire adeguati programmi di formazione periodica;
- assicurare il coordinamento tra il Codice Etico, il Modello 231 e le politiche aziendali;

- promuovere un ambiente di lavoro improntato al rispetto, all'inclusione e alla valorizzazione delle persone;
- favorire la segnalazione, in buona fede, di comportamenti contrari ai principi del presente Codice, garantendo la tutela dei segnalanti da qualsiasi forma di ritorsione;
- aggiornare periodicamente il Codice al fine di recepire l'evoluzione normativa, organizzativa e tecnologica.

CAPITOLO I

PRINCIPI ETICI FONDAMENTALI

ART. 1 – LEGALITÀ

IDRAGEST S.r.l. opera nel rigoroso rispetto della Costituzione della Repubblica Italiana, della normativa dell'Unione Europea, delle leggi nazionali, dei regolamenti, delle disposizioni emanate dalle Autorità competenti e delle procedure interne adottate dalla Società.

Il rispetto della legalità costituisce il principio imprescindibile dell'attività aziendale e rappresenta il presupposto fondamentale per la tutela della reputazione della Società e per la creazione di valore nel lungo periodo.

Tutti i Destinatari sono tenuti ad osservare le disposizioni normative applicabili alle attività svolte e ad aggiornare costantemente le proprie competenze professionali mediante la partecipazione alle iniziative formative promosse dalla Società.

Nessun risultato economico, commerciale o competitivo può giustificare comportamenti contrari alla legge, al presente Codice Etico o alle procedure aziendali.

ART. 2 – INTEGRITÀ, ONESTÀ E BUONA FEDE

Ogni attività aziendale deve essere svolta con onestà, correttezza, trasparenza, imparzialità e buona fede.

I Destinatari devono assumere decisioni esclusivamente nell'interesse della Società e degli stakeholder, evitando qualsiasi comportamento idoneo a compromettere l'indipendenza, l'obiettività o l'affidabilità dell'azione aziendale.

Ogni rapporto interno ed esterno deve essere improntato al rispetto reciproco, alla lealtà, alla collaborazione e alla correttezza professionale.
La Società promuove una cultura organizzativa fondata sull'esempio, sulla responsabilizzazione individuale e sulla fiducia reciproca.

ART. 3 – TRASPARENZA E ACCOUNTABILITY

IDRAGEST impronta la propria attività ai principi di trasparenza, tracciabilità e responsabilità.
Ogni operazione deve essere:

- preventivamente autorizzata ove previsto;
- adeguatamente documentata;
- verificabile;
- ricostruibile;
- registrata in modo completo e veritiero.

Ogni Destinatario è responsabile delle decisioni assunte nell'ambito delle proprie competenze e deve essere in grado di dimostrare la correttezza del proprio operato.
La Società promuove il principio dell'accountability quale elemento fondamentale del proprio sistema di governance e di controllo interno.

ART. 4 – CENTRALITÀ DELLA PERSONA

IDRAGEST riconosce la persona quale valore fondamentale dell'organizzazione aziendale.
La Società tutela la dignità, la libertà, la salute, la sicurezza, la riservatezza e lo sviluppo professionale di ogni individuo, promuovendo un ambiente di lavoro inclusivo, collaborativo e rispettoso delle diversità.
Ogni forma di discriminazione, molestia, intimidazione, violenza, abuso di potere, sfruttamento o comportamento lesivo della dignità personale è vietata.
Le relazioni professionali devono essere improntate al rispetto reciproco, alla collaborazione e alla valorizzazione delle competenze individuali.

ART. 5 – PARI OPPORTUNITÀ, INCLUSIONE E NON DISCRIMINAZIONE

La Società garantisce pari opportunità nello svolgimento dell'attività lavorativa, nei processi di selezione, assunzione, formazione, valutazione, sviluppo professionale e progressione di carriera.

Non sono ammesse discriminazioni fondate, a titolo esemplificativo, su:

- sesso;
- identità di genere;
- orientamento sessuale;
- età;
- origine etnica;
- nazionalità;
- lingua;
- religione;
- convinzioni personali;
- opinioni politiche;
- condizioni di salute;
- disabilità;
- appartenenza sindacale;
- qualsiasi altra condizione tutelata dalla normativa vigente.

La Società favorisce politiche organizzative orientate all'inclusione, alla valorizzazione del merito e allo sviluppo delle competenze.

ART. 6 – PROFESSIONALITÀ, COMPETENZA E MIGLIORAMENTO CONTINUO

IDRAGEST considera il capitale umano il principale fattore di sviluppo aziendale.

Ogni Destinatario è tenuto ad operare con la massima diligenza professionale, aggiornando costantemente le proprie competenze tecniche, organizzative, digitali e normative.

La Società promuove programmi di formazione continua finalizzati ad accrescere:

- le competenze tecniche;
- la cultura della sicurezza;
- la cultura della compliance;
- la prevenzione della corruzione;
- la protezione dei dati personali;
- la sicurezza informatica;
- l'utilizzo consapevole delle tecnologie digitali e dell'intelligenza artificiale.

ART. 7 – INNOVAZIONE RESPONSABILE

L'innovazione rappresenta un elemento strategico per la crescita della Società.

IDRAGEST promuove l'impiego delle tecnologie digitali e dell'intelligenza artificiale quale strumento di supporto alle attività aziendali, nel rispetto dei principi di legalità, trasparenza, sicurezza, supervisione umana, tutela dei diritti fondamentali e protezione dei dati personali.

L'utilizzo dei sistemi di intelligenza artificiale deve sempre avvenire nel rispetto della Policy aziendale sull'uso corretto e responsabile dell'Intelligenza Artificiale e non può sostituire il giudizio professionale umano nelle decisioni aventi rilevanza tecnica, economica, contrattuale o giuridica.

Ogni Destinatario è responsabile della verifica critica degli output generati dai sistemi di intelligenza artificiale prima del loro utilizzo nell'ambito delle attività aziendali.

ART. 8 – RISERVATEZZA E TUTELA DELLE INFORMAZIONI

Le informazioni aziendali costituiscono un patrimonio strategico della Società.

I Destinatari sono tenuti a garantire la massima riservatezza relativamente a dati, documenti, informazioni tecniche, commerciali, economiche, progettuali e organizzative acquisiti nello svolgimento della propria attività.

È vietata qualsiasi divulgazione non autorizzata di informazioni riservate o di know-how aziendale.

Le informazioni devono essere trattate nel rispetto:

- del GDPR;
- della normativa nazionale in materia di protezione dei dati personali;
- delle procedure aziendali;
- delle misure di sicurezza informatica;
- della Policy IA;
- delle procedure di cybersecurity adottate dalla Società.

ART. 9 – TUTELA DEL PATRIMONIO AZIENDALE E DELLA PROPRIETÀ INTELLETTUALE

Ogni Destinatario è responsabile della corretta conservazione e dell'utilizzo diligente dei beni aziendali materiali e immateriali.

Rientrano nel patrimonio della Società, a titolo esemplificativo:

- infrastrutture informatiche;
- software;
- banche dati;

- documentazione tecnica;
- modelli progettuali;
- algoritmi;
- elaborazioni sviluppate mediante sistemi di intelligenza artificiale;
- segreti commerciali;
- know-how;
- marchi;
- brevetti;
- informazioni riservate.

Tali beni devono essere utilizzati esclusivamente per finalità aziendali e nel rispetto delle procedure interne.

ART. 10 – SOSTENIBILITÀ E RESPONSABILITÀ SOCIALE

IDRAGEST considera la sostenibilità un principio trasversale della propria attività. La Società promuove uno sviluppo economico compatibile con la tutela dell'ambiente, l'uso efficiente delle risorse naturali, la sicurezza delle infrastrutture idriche e la creazione di valore per la collettività.

Nello svolgimento delle proprie attività, IDRAGEST orienta le proprie decisioni ai principi di:

- sostenibilità ambientale;
- responsabilità sociale;
- innovazione tecnologica;
- tutela del territorio;
- economia circolare;
- uso efficiente delle risorse;
- miglioramento continuo.

ART. 11 – CULTURA DELLA COMPLIANCE

La compliance rappresenta un elemento essenziale della governance aziendale.

IDRAGEST promuove una cultura organizzativa fondata sulla prevenzione dei rischi, sull'osservanza delle regole e sulla collaborazione tra tutte le funzioni aziendali.

Ogni Destinatario è tenuto a conoscere e rispettare:

- il presente Codice Etico;

- il Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001;
- la Politica Anticorruzione;
- la Policy sull'uso corretto e responsabile dell'Intelligenza Artificiale;
- la Procedura Whistleblowing;
- il Codice Disciplinare;
- tutte le procedure aziendali applicabili alle attività svolte.

L'osservanza di tali documenti costituisce parte integrante degli obblighi contrattuali e professionali di ciascun Destinatario.

CAPITOLO II

GOVERNO SOCIETARIO, COMPLIANCE E SISTEMA DEI CONTROLLI INTERNI

ART. 12 – PRINCIPI DI GOVERNANCE

IDRAGEST S.r.l. adotta un sistema di governo societario improntato ai principi di legalità, trasparenza, responsabilità, indipendenza delle funzioni di controllo, separazione dei poteri, tracciabilità delle decisioni e adeguatezza degli assetti organizzativi, amministrativi e contabili, ai sensi dell'art. 2086 del Codice Civile.

La governance aziendale è orientata alla prevenzione dei rischi, alla tutela della continuità aziendale, alla corretta gestione delle risorse, alla protezione degli stakeholder e alla creazione di valore sostenibile.

Tutte le decisioni devono essere assunte nel rispetto della normativa vigente, del presente Codice Etico, del Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D.Lgs. 231/2001 e delle procedure aziendali.

ART. 13 – SISTEMA INTEGRATO DI COMPLIANCE

IDRAGEST ha adottato un sistema integrato di compliance finalizzato a prevenire la commissione di illeciti, assicurare il rispetto della normativa vigente e promuovere una cultura aziendale fondata sull'etica e sull'integrità.

Il sistema di compliance comprende, tra gli altri:

- il Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001;
- il presente Codice Etico;
- la Politica Anticorruzione;

- la Policy sull'uso corretto e responsabile dell'Intelligenza Artificiale;
- la Procedura Whistleblowing;
- il Codice Disciplinare;
- le procedure speciali del Modello 231;
- le procedure aziendali in materia di sicurezza delle informazioni, protezione dei dati personali, salute e sicurezza sul lavoro e gestione dei processi aziendali.

I predetti documenti costituiscono un sistema unitario e coordinato di prevenzione dei rischi e devono essere interpretati in modo coerente tra loro.

ART. 14 – ORGANI AZIENDALI E RESPONSABILITÀ

Gli organi societari esercitano le rispettive funzioni nel rispetto della legge, dello Statuto sociale e dei principi contenuti nel presente Codice.

Ciascun componente degli organi societari è tenuto ad agire con indipendenza di giudizio, diligenza professionale, lealtà e correttezza, perseguendo esclusivamente l'interesse della Società.

Ogni decisione deve essere adottata secondo criteri di trasparenza, documentabilità, proporzionalità e tracciabilità.

ART. 15 – ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza esercita le proprie funzioni con autonomia, indipendenza, continuità di azione e professionalità, nel rispetto delle disposizioni del D.Lgs. 231/2001.

L'Organismo di Vigilanza:

- vigila sull'efficace attuazione del Modello 231;
- verifica l'osservanza del presente Codice Etico;
- riceve e valuta i flussi informativi previsti dal Modello;
- riceve le segnalazioni di violazioni di propria competenza;
- propone eventuali aggiornamenti del Modello e del Codice Etico;
- promuove la diffusione della cultura della compliance.

Tutte le funzioni aziendali sono tenute a collaborare con l'Organismo di Vigilanza, fornendo tempestivamente le informazioni richieste e garantendo il pieno accesso alla documentazione necessaria allo svolgimento delle attività di controllo.

ART. 16 – RESPONSABILE DELLA CONFORMITÀ

La Società individua una Funzione di Conformità quale presidio operativo del sistema di prevenzione dei rischi di compliance.

La Funzione di Conformità opera in coordinamento con la Direzione aziendale e con l'Organismo di Vigilanza, assicurando:

- il monitoraggio dell'attuazione della Politica Anticorruzione;
- il supporto nell'aggiornamento delle procedure aziendali;
- il coordinamento delle attività di compliance;
- il monitoraggio dei rischi emergenti;
- la promozione della cultura della legalità e dell'integrità.

La Funzione di Conformità opera nel rispetto dei principi di autonomia tecnica, indipendenza funzionale, imparzialità e riservatezza.

ART. 17 – GOVERNANCE DELL'INTELLIGENZA ARTIFICIALE

La Società riconosce l'importanza dell'innovazione tecnologica e dell'utilizzo responsabile dei sistemi di Intelligenza Artificiale.

L'impiego di tali strumenti è disciplinato dalla specifica Policy aziendale e deve rispettare i principi di:

- supervisione umana;
- trasparenza;
- affidabilità;
- sicurezza;
- protezione dei dati personali;
- non discriminazione;
- proporzionalità;
- responsabilità.

L'adozione di sistemi di Intelligenza Artificiale non può in alcun caso sostituire le valutazioni professionali, tecniche, economiche, contrattuali o giuridiche che devono rimanere affidate alle competenti funzioni aziendali.

Ogni utilizzatore è responsabile della verifica dell'affidabilità, correttezza e completezza dei risultati prodotti dai sistemi di Intelligenza Artificiale prima del loro utilizzo.

ART. 18 – SISTEMA DEI CONTROLLI INTERNI

IDRAGEST considera il sistema dei controlli interni uno strumento essenziale per garantire la corretta gestione aziendale.

Il sistema dei controlli interni è finalizzato a:

- assicurare l'efficacia e l'efficienza dei processi aziendali;
- garantire l'affidabilità delle informazioni;
- tutelare il patrimonio aziendale;
- prevenire frodi e comportamenti illeciti;
- assicurare il rispetto della normativa vigente;
- monitorare i rischi aziendali;
- favorire il miglioramento continuo.

I controlli devono essere proporzionati ai rischi, adeguatamente documentati e periodicamente verificati.

ART. 19 – COLLABORAZIONE AI CONTROLLI

Tutti i Destinatari sono tenuti a collaborare attivamente con le funzioni di controllo interno, con l'Organismo di Vigilanza, con la Funzione di Conformità, con i revisori e con le Autorità competenti.

È fatto obbligo di:

- fornire informazioni complete, corrette e tempestive;
- mettere a disposizione la documentazione richiesta;
- evitare comportamenti ostruzionistici;
- non alterare o distruggere documenti o evidenze rilevanti;
- segnalare tempestivamente eventuali anomalie o criticità riscontrate.

Ogni comportamento volto ad ostacolare le attività di vigilanza, controllo o audit costituisce violazione del presente Codice Etico e può comportare l'applicazione delle misure disciplinari previste dalla normativa vigente e dal sistema disciplinare aziendale.

ART. 20 – CULTURA DELLA PREVENZIONE E DEL MIGLIORAMENTO CONTINUO

IDRAGEST promuove un approccio preventivo alla gestione dei rischi aziendali, fondato sul miglioramento continuo dei processi, sull'analisi periodica dei rischi e sull'aggiornamento costante del sistema di compliance.

La Società favorisce la diffusione di una cultura organizzativa nella quale ogni Destinatario contribuisce, nell'ambito delle proprie competenze, all'individuazione delle aree di miglioramento, alla prevenzione dei rischi e alla tutela dell'integrità aziendale.

Le esperienze maturate, gli audit, le attività dell'Organismo di Vigilanza, le segnalazioni ricevute, gli aggiornamenti normativi e l'evoluzione tecnologica costituiscono elementi fondamentali per il progressivo rafforzamento del sistema di controllo interno.

CAPITOLO III

LE PERSONE DI IDRAGEST

ART. 21 – CENTRALITÀ DELLE PERSONE

Le persone rappresentano il principale patrimonio di IDRAGEST S.r.l. e costituiscono il fattore determinante per il raggiungimento degli obiettivi aziendali.

La Società promuove un ambiente di lavoro fondato sul rispetto reciproco, sulla collaborazione, sulla valorizzazione delle competenze e sulla responsabilizzazione individuale.

Ogni lavoratore contribuisce, con il proprio comportamento, alla diffusione della cultura della legalità, dell'integrità, della sicurezza e della qualità.

La Società favorisce la crescita professionale delle proprie risorse umane attraverso percorsi di formazione continua, aggiornamento professionale e sviluppo delle competenze tecniche, organizzative, digitali e manageriali.

ART. 22 – SELEZIONE E VALORIZZAZIONE DELLE RISORSE UMANE

La selezione del personale è effettuata esclusivamente sulla base di criteri oggettivi di competenza, professionalità, esperienza, capacità e attitudine al ruolo da ricoprire.

La Società garantisce processi di selezione trasparenti, imparziali e coerenti con le esigenze organizzative, evitando qualsiasi forma di favoritismo, clientelismo o discriminazione.

Ogni decisione relativa all'assunzione, all'inquadramento, alla formazione, alla retribuzione, alla valutazione delle prestazioni e alla progressione professionale è fondata esclusivamente sul merito e sulle capacità individuali.

ART. 23 – PARI OPPORTUNITÀ, INCLUSIONE E RISPETTO DELLA PERSONA

IDRAGEST garantisce pari opportunità a tutti i lavoratori e promuove una cultura organizzativa inclusiva.

La Società vieta qualsiasi discriminazione fondata, a titolo esemplificativo, su:

- sesso;
- identità di genere;
- orientamento affettivo e sessuale;
- età;
- origine etnica;
- nazionalità;
- lingua;
- religione;
- opinioni politiche;
- appartenenza sindacale;
- condizioni personali o familiari;
- stato di salute;
- disabilità;
- qualsiasi altra condizione tutelata dalla legge.

Ogni persona deve essere trattata con dignità, correttezza e rispetto.

ART. 24 – TUTELA DELLA DIGNITÀ E CONTRASTO ALLE MOLESTIE

La Società non tollera alcuna forma di:

- molestia;
- molestia sessuale;
- intimidazione;
- abuso di autorità;
- violenza psicologica;
- violenza verbale;
- violenza fisica;
- mobbing;
- stalking;
- comportamenti offensivi;
- isolamento intenzionale;
- ritorsione.

Ogni comportamento lesivo della dignità personale costituisce grave violazione del presente Codice Etico.
Chiunque sia vittima o venga a conoscenza di tali comportamenti è invitato a segnalarli attraverso i canali aziendali previsti, con garanzia della massima riservatezza e della tutela contro qualsiasi forma di ritorsione.

ART. 25 – REGOLARITÀ DEI RAPPORTI DI LAVORO

IDRAGEST instaura esclusivamente rapporti di lavoro conformi alla normativa vigente.

La Società:

- rifiuta ogni forma di lavoro irregolare;
- vieta qualsiasi forma di sfruttamento del lavoro;
- contrasta il lavoro forzato;
- vieta il lavoro minorile nei casi previsti dalla legge;
- garantisce il rispetto della normativa previdenziale, contributiva e fiscale;
- applica il contratto collettivo di riferimento.

Ogni collaboratore riceve informazioni chiare circa:

- mansioni;
- responsabilità;
- diritti;
- obblighi;
- procedure aziendali;
- sistema disciplinare.

ART. 26 – FORMAZIONE CONTINUA

La formazione rappresenta uno strumento fondamentale di crescita personale e aziendale.

La Società promuove programmi periodici di aggiornamento riguardanti:

- normativa di settore;
- Modello 231;
- Codice Etico;
- prevenzione della corruzione;
- salute e sicurezza;
- protezione dei dati personali;
- sicurezza informatica;

- intelligenza artificiale;
- qualità;
- sostenibilità;
- procedure aziendali.

I Destinatari sono tenuti a partecipare ai programmi formativi organizzati dalla Società quando previsti per la funzione ricoperta.

ART. 27 – UTILIZZO CORRETTO DEGLI STRUMENTI AZIENDALI

Le attrezzature, i dispositivi informatici, i software, gli strumenti tecnologici, gli indirizzi di posta elettronica, gli account aziendali e ogni altro bene aziendale devono essere utilizzati esclusivamente per finalità lavorative.

È vietato:

- utilizzare strumenti aziendali per attività illecite;
- installare software non autorizzati;
- eludere le misure di sicurezza informatica;
- condividere credenziali personali;
- utilizzare dispositivi aziendali in modo da compromettere la sicurezza della rete;
- utilizzare risorse aziendali per fini personali incompatibili con l'attività lavorativa.

L'utilizzo degli strumenti informatici è disciplinato anche dalle specifiche procedure aziendali.

ART. 28 – UTILIZZO RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

L'utilizzo di sistemi di Intelligenza Artificiale costituisce un'opportunità di innovazione e di miglioramento dell'efficienza aziendale, purché avvenga nel rispetto della normativa vigente e delle procedure interne.

I Destinatari devono:

- utilizzare esclusivamente gli strumenti autorizzati dalla Società;
- verificare criticamente ogni contenuto prodotto dall'IA prima del suo utilizzo;
- mantenere sempre il controllo umano sulle decisioni;
- evitare l'inserimento nei sistemi di IA di dati riservati o informazioni la cui comunicazione non sia autorizzata;
- rispettare la Policy aziendale sull'uso dell'Intelligenza Artificiale;

- segnalare eventuali anomalie, errori o utilizzi impropri dei sistemi impiegati.

È vietato utilizzare sistemi di IA per alterare documenti, produrre informazioni false, eludere controlli aziendali o porre in essere comportamenti contrari alla legge o ai principi del presente Codice.

ART. 29 – RISERVATEZZA E PROTEZIONE DEI DATI

Ogni lavoratore è tenuto a mantenere la massima riservatezza sulle informazioni acquisite nello svolgimento della propria attività.

Devono essere tutelati, in particolare:

- dati personali;
- dati dei clienti;
- dati dei fornitori;
- informazioni economiche;
- progetti;
- banche dati;
- documentazione tecnica;
- know-how;
- segreti commerciali;
- credenziali di accesso.

Le informazioni devono essere trattate esclusivamente per finalità aziendali e nel rispetto della normativa vigente e delle procedure interne.

ART. 30 – SALUTE, SICUREZZA E BENESSERE ORGANIZZATIVO

La tutela della salute e della sicurezza costituisce un valore fondamentale della Società.

Ogni Destinatario è tenuto a:

- osservare la normativa vigente;
- rispettare le procedure aziendali;
- utilizzare correttamente le attrezzature;
- impiegare i dispositivi di protezione individuale;
- segnalare tempestivamente situazioni di rischio;
- collaborare alle attività di prevenzione.

La Società promuove altresì il benessere organizzativo quale elemento essenziale per il miglioramento della qualità del lavoro, della produttività e della soddisfazione delle persone.

ART. 31 – DOVERE DI COLLABORAZIONE E DI SEGNALAZIONE

Ogni Destinatario è tenuto a collaborare attivamente con la Società nell'attuazione del sistema di compliance.

Chiunque venga a conoscenza di:

- violazioni del presente Codice;
- comportamenti contrari alla legge;
- situazioni di rischio;
- condotte corruttive;
- utilizzi impropri dei sistemi informatici o dell'Intelligenza Artificiale;
- violazioni delle procedure aziendali;

ha il dovere di effettuare tempestivamente una segnalazione attraverso i canali previsti dalla Procedura Whistleblowing adottata dalla Società.

La Società garantisce la tutela della riservatezza dell'identità del segnalante e vieta qualsiasi forma di ritorsione, discriminazione o penalizzazione nei confronti di chi effettua una segnalazione in buona fede.

CAPITOLO IV

RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE, LE AUTORITÀ E GLI ENTI PUBBLICI

ART. 32 – PRINCIPI GENERALI

I rapporti con la Pubblica Amministrazione, con gli enti pubblici, con i concessionari di pubblici servizi, con le Autorità amministrative indipendenti, con gli organismi di controllo e con ogni altro soggetto che eserciti pubbliche funzioni devono essere improntati ai principi di:

1. legalità;
2. imparzialità;
3. correttezza;
4. trasparenza;
5. collaborazione;

6. buona fede;
7. tracciabilità;
8. integrità.

Tutti i Destinatari sono tenuti ad operare nel pieno rispetto della normativa vigente, del Modello di Organizzazione, Gestione e Controllo, della Politica Anticorruzione e delle procedure aziendali applicabili.

ART. 33 – RAPPORTI ISTITUZIONALI

I rapporti con le Pubbliche Amministrazioni sono riservati esclusivamente ai soggetti formalmente autorizzati in ragione delle rispettive deleghe, procure o responsabilità organizzative.

Ogni interlocuzione deve essere:

1. preventivamente autorizzata, ove previsto;
2. correttamente documentata;
3. improntata alla massima trasparenza;
4. coerente con gli interessi legittimi della Società.

È vietato assumere iniziative personali nei confronti di pubblici funzionari al di fuori delle competenze attribuite.

ART. 34 – GARE PUBBLICHE, AFFIDAMENTI E CONTRATTI PUBBLICI

Nella partecipazione a procedure di evidenza pubblica, affidamenti diretti, concessioni, partenariati e ogni altra procedura disciplinata dalla normativa sui contratti pubblici, IDRAGEST opera secondo i principi di:

1. concorrenza leale;
2. trasparenza;
3. correttezza;
4. imparzialità;
5. buona fede;
6. parità di trattamento;
7. integrità.

Ogni documento presentato alla stazione appaltante deve essere completo, veritiero, aggiornato e conforme alla normativa vigente.

È fatto divieto di:

1. alterare informazioni o documenti;

2. produrre dichiarazioni false o incomplete;
3. occultare informazioni rilevanti;
4. influenzare impropriamente l'esito delle procedure;
5. utilizzare informazioni riservate acquisite illegittimamente.

ART. 35 – RAPPORTI CON PUBBLICI UFFICIALI E INCARICATI DI PUBBLICO SERVIZIO

Nei rapporti con pubblici ufficiali o incaricati di pubblico servizio è fatto assoluto divieto di:

1. offrire, promettere o corrispondere denaro;
2. offrire beni o utilità non consentite;
3. promettere vantaggi personali;
4. concedere favori indebiti;
5. effettuare pagamenti non dovuti;
6. influenzare impropriamente decisioni amministrative;
7. ottenere trattamenti preferenziali contrari alla legge.

Sono vietate anche le condotte poste in essere tramite intermediari, consulenti, professionisti, partner commerciali o altri soggetti terzi.
Ogni comportamento deve essere conforme ai principi di imparzialità e trasparenza.

ART. 36 – OMAGGI, OSPITALITÀ E SPESE DI RAPPRESENTANZA

Gli omaggi, gli atti di cortesia commerciale e le spese di rappresentanza sono consentiti esclusivamente quando:

1. siano conformi alla legge;
2. abbiano un valore economico non superiore ad euro 150,00 per singola utilità e, comunque, tale da non compromettere, neppure apparentemente, l'indipendenza, l'imparzialità o l'autonomia di giudizio del destinatario;
3. rientrino nelle ordinarie pratiche di cortesia istituzionale o commerciale;
4. non siano finalizzati ad ottenere vantaggi indebiti o trattamenti di favore;
5. siano preventivamente autorizzati secondo le procedure aziendali, ove previsto;
6. siano adeguatamente documentati e tracciati.

È in ogni caso vietato offrire, promettere o accettare omaggi, utilità, ospitalità o altre forme di beneficio che, per valore, frequenza, circostanze o modalità di erogazione, possano anche solo apparire idonei ad influenzare l'indipendenza decisionale del destinatario o ad ottenere un vantaggio indebito.

Nei rapporti con la Pubblica Amministrazione, con i pubblici ufficiali e con gli incaricati di pubblico servizio è consentita esclusivamente l'offerta di omaggi di carattere meramente simbolico e di valore non superiore ad euro 50,00, nel rispetto della normativa vigente e delle procedure aziendali, fermo restando il divieto assoluto di offrire qualsiasi utilità idonea ad influenzare l'esercizio delle funzioni pubbliche.

Restano ferme le eventuali disposizioni più restrittive previste dalla Politica Anticorruzione adottata dalla Società.

ART. 37 – ISPEZIONI, VERIFICHE E CONTROLLI

La Società collabora con le Autorità pubbliche, gli organi ispettivi e gli organismi di controllo.

Durante ispezioni, verifiche, audit o richieste istruttorie, tutti i Destinatari devono:

1. collaborare con correttezza;
2. fornire informazioni veritiere e complete;
3. mettere tempestivamente a disposizione la documentazione richiesta;
4. evitare comportamenti ostruzionistici;
5. segnalare immediatamente alla Direzione eventuali criticità emerse.

È vietato:

1. occultare documenti;
2. alterare registrazioni;
3. distruggere evidenze;
4. rendere dichiarazioni false o fuorvianti.

ART. 38 – CONTRIBUTI, FINANZIAMENTI E AGEVOLAZIONI PUBBLICHE

La Società utilizza contributi, finanziamenti, incentivi, sovvenzioni e agevolazioni pubbliche esclusivamente per le finalità per le quali sono stati concessi.

È fatto divieto di:

7. presentare documentazione non veritiera;
8. omettere informazioni rilevanti;
9. utilizzare fondi pubblici per finalità diverse da quelle autorizzate;

10. rendicontare costi inesistenti;
11. ottenere indebitamente erogazioni pubbliche.

La documentazione relativa all'utilizzo delle risorse pubbliche deve essere completa, verificabile e conservata secondo le procedure aziendali.

ART. 39 – RAPPORTI CON LE AUTORITÀ INDIPENDENTI E L'AUTORITÀ GIUDIZIARIA

La Società mantiene rapporti improntati alla massima collaborazione con:

1. Autorità Giudiziaria;
2. Autorità Nazionale Anticorruzione (ANAC);
3. Autorità Garante della Concorrenza e del Mercato (AGCM);
4. Garante per la Protezione dei Dati Personali;
5. Autorità di regolazione;
6. Autorità fiscali;
7. Autorità di vigilanza;
8. ogni altro organismo pubblico competente.

Le richieste provenienti dalle Autorità devono essere gestite tempestivamente, con correttezza e trasparenza.

ART. 40 – TRACCIABILITÀ DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Ogni rapporto con la Pubblica Amministrazione deve essere adeguatamente documentato e tracciabile.

Devono essere conservati, secondo le procedure aziendali:

1. corrispondenza;
2. verbali;
3. richieste;
4. autorizzazioni;
5. offerte;
6. dichiarazioni;
7. documentazione di gara;
8. provvedimenti;
9. comunicazioni ufficiali.

La tracciabilità costituisce elemento essenziale del sistema di controllo interno e del Modello di Organizzazione, Gestione e Controllo.

ART. 41 – PREVENZIONE DELLA CORRUZIONE

IDRAGEST adotta una politica di assoluta intolleranza nei confronti di qualsiasi forma di corruzione, sia nel settore pubblico sia nei rapporti tra privati.

Tutti i Destinatari sono tenuti a:

1. rispettare integralmente la Politica Anticorruzione adottata dalla Società;
2. astenersi da qualsiasi comportamento idoneo a integrare anche solo il rischio di fenomeni corruttivi;
3. segnalare tempestivamente eventuali richieste indebite, tentativi di corruzione o situazioni di rischio;
4. collaborare con l'Organismo di Vigilanza e con la Funzione di Conformità nell'attuazione delle misure di prevenzione.

La violazione delle disposizioni contenute nel presente articolo costituisce grave inosservanza del Codice Etico e comporta l'applicazione delle misure disciplinari e contrattuali previste dall'ordinamento e dal sistema disciplinare aziendale.

CAPITOLO V

INTEGRITÀ NEI RAPPORTI COMMERCIALI E PREVENZIONE DELLA CORRUZIONE

ART. 42 – PRINCIPIO DI INTEGRITÀ NEI RAPPORTI COMMERCIALI

IDRAGEST svolge la propria attività imprenditoriale secondo criteri di correttezza, trasparenza, lealtà, professionalità e reciproca fiducia.

Ogni rapporto commerciale deve essere fondato sul rispetto della legge, delle regole di mercato e dei principi contenuti nel presente Codice Etico.

La Società rifiuta qualsiasi pratica commerciale scorretta, ingannevole o idonea ad alterare il corretto funzionamento del mercato.

ART. 43 – PRINCIPIO DI TOLLERANZA ZERO VERSO LA CORRUZIONE

IDRAGEST adotta una politica di assoluta intolleranza ("Zero Tolerance") nei confronti di qualsiasi forma di corruzione, concussione, induzione indebita, traffico di influenze illecite, corruzione tra privati, frode, appropriazione indebita, abuso d'ufficio ove applicabile, nonché di qualsiasi comportamento finalizzato ad ottenere vantaggi illeciti.

Il divieto riguarda tanto i rapporti con soggetti pubblici quanto quelli con soggetti privati.

È vietato, direttamente o indirettamente, anche tramite terzi:

1. offrire;
2. promettere;
3. richiedere;
4. accettare;
5. autorizzare;
6. ricevere;
7. denaro, beni, servizi, utilità, favori o altri vantaggi non dovuti, allo scopo di ottenere o mantenere un indebito vantaggio economico o commerciale.

ART. 44 – CORRUZIONE PUBBLICA E PRIVATA

I Destinatari devono astenersi da qualsiasi comportamento che possa integrare o favorire, anche solo potenzialmente, fattispecie di:

1. corruzione nei confronti della Pubblica Amministrazione;
2. corruzione tra privati;
3. induzione indebita;
4. traffico di influenze illecite;
5. turbata libertà degli incanti;
6. turbata libertà del procedimento di scelta del contraente;
7. frode nelle pubbliche forniture;
8. ogni altra fattispecie prevista dalla normativa vigente.

Sono vietati accordi occulti, pagamenti non documentati, retrocessioni di compensi, compensi non proporzionati alle prestazioni rese e qualsiasi altra utilità priva di giustificazione economica.

ART. 45 – OMAGGI, LIBERALITÀ, OSPITALITÀ E SPESE DI RAPPRESENTANZA

Gli omaggi, le spese di rappresentanza, le forme di ospitalità e le liberalità devono essere improntati ai principi di trasparenza, correttezza, proporzionalità e tracciabilità.

Essi sono consentiti esclusivamente quando:

1. siano conformi alla normativa vigente;
2. perseguano finalità esclusivamente istituzionali o commerciali lecite;
3. siano occasionali;

4. siano preventivamente autorizzati, ove previsto;
5. siano adeguatamente documentati.

Fermo restando quanto previsto dalla Politica Anticorruzione:

1. nei rapporti tra soggetti privati non possono essere offerti o accettati omaggi o utilità di valore superiore ad € 150,00 per singola utilità;
2. nei rapporti con la Pubblica Amministrazione, pubblici ufficiali o incaricati di pubblico servizio possono essere esclusivamente offerti omaggi di carattere simbolico e di valore non superiore ad € 50,00, purché consentiti dalla normativa applicabile.

In ogni caso resta vietato qualsiasi omaggio, beneficio o utilità che possa anche soltanto apparire idoneo ad influenzare l'autonomia decisionale del destinatario.

ART. 46 – PAGAMENTI DI FACILITAZIONE

IDRAGEST vieta i cosiddetti pagamenti di facilitazione ("facilitation payments"), intendendosi per tali qualsiasi pagamento, anche di modesto importo, effettuato allo scopo di accelerare, agevolare o influenzare l'esecuzione di attività dovute da parte di pubblici funzionari o soggetti privati.

Nessuna eccezione è consentita, salvo i casi di pericolo grave e imminente per l'incolumità delle persone, che dovranno essere tempestivamente comunicati alla Direzione aziendale e all'Organismo di Vigilanza.

ART. 47 – CONFLITTO DI INTERESSI

Ogni Destinatario deve evitare situazioni, anche solo potenziali, nelle quali interessi personali, familiari, patrimoniali o professionali possano interferire con l'interesse della Società.

Costituiscono, a titolo esemplificativo, situazioni di conflitto:

1. interessi economici personali in imprese concorrenti, clienti o fornitori;
2. rapporti di parentela o affinità con soggetti coinvolti nei processi decisionali;
3. incarichi esterni incompatibili;
4. utilizzo della posizione aziendale per ottenere vantaggi personali;
5. partecipazione a decisioni riguardanti soggetti con i quali esistano interessi privati.

Ogni situazione di conflitto deve essere tempestivamente comunicata alla Direzione aziendale, che adotterà le misure ritenute opportune.

ART. 48 – SELEZIONE DI FORNITORI, CONSULENTI E PARTNER

La selezione dei fornitori, dei consulenti, dei professionisti e dei partner commerciali avviene secondo criteri oggettivi di:

1. competenza;
2. affidabilità;
3. capacità tecnica;
4. solidità economica;
5. reputazione;
6. qualità;
7. sostenibilità;
8. conformità normativa.

La Società promuove rapporti commerciali esclusivamente con soggetti che condividano principi etici coerenti con quelli contenuti nel presente Codice.

I contratti possono prevedere specifiche clausole di integrità, di rispetto del Modello 231 e del presente Codice Etico, la cui violazione può costituire causa di risoluzione del rapporto.

ART. 49 – DUE DILIGENCE E VERIFICA DELLE CONTROPARTI

Prima dell'instaurazione di rapporti commerciali significativi, la Società può svolgere verifiche preventive finalizzate ad accertare:

1. l'identità della controparte;
2. la struttura proprietaria;
3. l'affidabilità economico-finanziaria;
4. l'assenza di situazioni di incompatibilità;
5. eventuali precedenti giudiziari o reputazionali rilevanti;
6. l'adeguatezza dei presidi di compliance adottati.

L'intensità delle verifiche è commisurata alla natura del rapporto, al rischio connesso e alla rilevanza economica dell'operazione.

ART. 50 – RAPPORTI CON INTERMEDIARI E CONSULENTI

L'affidamento di incarichi a consulenti, intermediari, agenti o professionisti deve essere motivato da effettive esigenze aziendali.

I compensi devono essere:

1. congrui;

2. proporzionati;
3. documentati;
4. coerenti con le prestazioni effettivamente svolte.

È vietato conferire incarichi aventi finalità elusive della normativa o finalizzati ad occultare pagamenti indebiti.

ART. 51 – RAPPORTI CON FORNITORI E SUBAPPALTATORI

I rapporti con fornitori e subappaltatori devono essere improntati ai principi di correttezza, collaborazione, trasparenza e reciproco rispetto.

La Società richiede ai propri fornitori il rispetto della normativa vigente in materia di:

1. lavoro;
2. salute e sicurezza;
3. ambiente;
4. tutela dei dati personali;
5. anticorruzione;
6. responsabilità amministrativa degli enti;
7. diritti umani.

La Società si riserva di effettuare verifiche sulla permanenza dei requisiti richiesti durante l'intero rapporto contrattuale.

ART. 52 – DONAZIONI, SPONSORIZZAZIONI E CONTRIBUTI

Donazioni, sponsorizzazioni e contributi sono consentiti esclusivamente quando:

1. siano conformi alla legge;
2. perseguano finalità lecite;
3. siano coerenti con i valori della Società;
4. siano preventivamente autorizzati;
5. siano adeguatamente documentati e contabilizzati.

È vietata qualsiasi erogazione finalizzata ad ottenere vantaggi indebiti o ad influenzare decisioni di soggetti pubblici o privati.

ART. 53 – TUTELA DELLA CONCORRENZA

IDRAGEST riconosce il valore della libera concorrenza quale elemento fondamentale del mercato.

Sono vietati:

1. accordi anticoncorrenziali;
2. pratiche collusive;
3. scambi illeciti di informazioni sensibili;
4. abuso di posizione dominante;
5. qualsiasi comportamento idoneo ad alterare il normale funzionamento del mercato.

I rapporti con concorrenti devono svolgersi nel pieno rispetto della normativa nazionale ed europea in materia di tutela della concorrenza.

ART. 54 – OBBLIGO DI SEGNALAZIONE

Ogni Destinatario che venga a conoscenza di:

1. richieste indebite;
2. tentativi di corruzione;
3. conflitti di interesse non dichiarati;
4. anomalie nei processi di acquisto;
5. violazioni della Politica Anticorruzione;
6. violazioni del presente Capitolo;
7. è tenuto a effettuare tempestivamente una segnalazione attraverso i canali previsti dalla Procedura Whistleblowing, collaborando con la Società e con l'Organismo di Vigilanza nell'accertamento dei fatti.

CAPITOLO VI

RAPPORTI CON CLIENTI, FORNITORI, PARTNER COMMERCIALI E MERCATO

ART. 55 – PRINCIPI GENERALI

IDRAGEST instaura i propri rapporti commerciali secondo criteri di correttezza, trasparenza, professionalità, reciproca fiducia, buona fede e responsabilità.

Ogni attività deve essere svolta perseguendo la soddisfazione del cliente, la qualità delle prestazioni, la tutela della reputazione aziendale e il rispetto della normativa vigente.

La Società opera affinché ogni rapporto commerciale sia improntato al rispetto dei principi del presente Codice Etico e del proprio sistema di compliance.

ART. 56 – RAPPORTI CON I CLIENTI

La Società considera il cliente un interlocutore fondamentale per il proprio sviluppo.

Nei rapporti con i clienti IDRAGEST garantisce:

1. correttezza e trasparenza nelle trattative;
2. chiarezza delle offerte economiche;
3. qualità delle prestazioni professionali;
4. rispetto degli impegni contrattuali;
5. tempestività delle comunicazioni;
6. tutela della riservatezza;
7. assistenza tecnica qualificata.

I clienti devono ricevere informazioni veritiere, complete, comprensibili e non ingannevoli.

È vietato formulare promesse o assumere impegni che la Società non sia ragionevolmente in grado di rispettare.

ART. 57 – QUALITÀ DEI SERVIZI

IDRAGEST persegue il miglioramento continuo della qualità dei servizi offerti.

Ogni attività tecnica, progettuale, informatica, topografica, di rilievo, monitoraggio, digitalizzazione e supporto specialistico deve essere eseguita secondo elevati standard professionali, nel rispetto:

1. della normativa vigente;
2. delle regole tecniche applicabili;
3. delle specifiche contrattuali;
4. delle procedure aziendali;
5. dei sistemi di gestione adottati dalla Società.

Gli errori devono essere tempestivamente comunicati e corretti, adottando ogni misura utile a limitarne gli effetti.

ART. 58 – RAPPORTI CON FORNITORI E PROFESSIONISTI

I fornitori rappresentano partner essenziali per il perseguimento degli obiettivi aziendali.

La loro selezione avviene secondo criteri oggettivi di:

1. qualità;

2. competenza;
3. affidabilità;
4. esperienza;
5. sostenibilità;
6. solidità economica;
7. rispetto della normativa.

La Società garantisce pari opportunità di accesso alle procedure di selezione e vieta qualsiasi forma di favoritismo.

ART. 59 – RAPPORTI CON CONSULENTI E COLLABORATORI ESTERNI

I rapporti con consulenti, professionisti e collaboratori esterni devono essere fondati su:

1. competenza;
2. indipendenza;
3. professionalità;
4. correttezza;
5. trasparenza.

Gli incarichi devono essere formalizzati per iscritto, descrivere chiaramente le prestazioni richieste e prevedere compensi proporzionati alle attività effettivamente svolte.

La Società richiede ai propri consulenti il rispetto del presente Codice Etico e del Modello di Organizzazione, Gestione e Controllo.

ART. 60 – RAPPORTI CON PARTNER COMMERCIALI, RTI E RETI D'IMPRESA

Nei rapporti con partner commerciali, raggruppamenti temporanei di imprese, consorzi, joint venture e reti d'impresa, IDRAGEST promuove rapporti fondati sulla collaborazione, sulla trasparenza e sulla condivisione di principi etici comuni.

La Società verifica, in relazione alla natura del rapporto, l'affidabilità e la reputazione dei partner e richiede il rispetto dei principi di legalità, integrità e correttezza.

Ogni partner è tenuto a cooperare nel rispetto delle norme di legge, delle obbligazioni contrattuali e delle procedure concordate.

ART. 61 – CONCORRENZA LEALE

IDRAGEST riconosce il valore della libera concorrenza e opera nel pieno rispetto della normativa nazionale ed europea in materia di concorrenza e mercato.

È fatto divieto di:

1. porre in essere pratiche anticoncorrenziali;
2. diffondere informazioni denigratorie nei confronti dei concorrenti;
3. appropriarsi indebitamente di informazioni riservate;
4. utilizzare mezzi illeciti per acquisire commesse o clienti;
5. concordare prezzi, condizioni contrattuali o ripartizioni di mercato con imprese concorrenti.

La Società compete esclusivamente attraverso la qualità delle proprie prestazioni, l'innovazione tecnologica e la competenza professionale.

ART. 62 – TUTELA DELLA PROPRIETÀ INTELLETTUALE E DEL KNOW-HOW

IDRAGEST tutela il proprio patrimonio intellettuale, tecnologico e informativo.

Costituiscono patrimonio della Società, tra l'altro:

1. metodologie operative;
2. software;
3. banche dati;
4. documentazione progettuale;
5. modelli digitali;
6. algoritmi;
7. rilievi;
8. elaborazioni tecniche;
9. studi;
10. procedure;
11. know-how aziendale.

I Destinatari sono tenuti a:

1. utilizzare tali beni esclusivamente per finalità aziendali;
2. impedirne la divulgazione non autorizzata;
3. rispettare i diritti di proprietà intellettuale di terzi;
4. evitare qualsiasi utilizzo abusivo di opere dell'ingegno protette.

ART. 63 – COMUNICAZIONI COMMERCIALI E PUBBLICITÀ

Le comunicazioni commerciali devono essere improntate ai principi di correttezza, trasparenza e veridicità.

La Società vieta qualsiasi forma di pubblicità:

1. ingannevole;
2. denigratoria;
3. comparativa illecita;
4. suscettibile di alterare la libera concorrenza.

Ogni informazione relativa ai servizi offerti deve essere verificabile e coerente con le effettive capacità aziendali.

ART. 64 – TUTELA DELLA REPUTAZIONE AZIENDALE

La reputazione rappresenta un patrimonio strategico della Società.

Tutti i Destinatari devono evitare comportamenti che possano arrecare pregiudizio all'immagine di IDRAGEST.

Particolare attenzione deve essere prestata:

1. nelle relazioni con clienti e fornitori;
2. nelle comunicazioni pubbliche;
3. nell'utilizzo dei social network;
4. nella partecipazione a convegni, eventi e manifestazioni;
5. nelle dichiarazioni rese a terzi.

Le comunicazioni esterne effettuate in nome della Società possono essere rilasciate esclusivamente dai soggetti espressamente autorizzati.

ART. 65 – TUTELA DEGLI STAKEHOLDER

IDRAGEST riconosce il valore del dialogo con tutti gli stakeholder.

La Società favorisce rapporti improntati a:

1. ascolto;
2. trasparenza;
3. collaborazione;
4. affidabilità;
5. responsabilità.

Le osservazioni, i reclami e le segnalazioni provenienti dagli stakeholder costituiscono un'opportunità di miglioramento dei processi aziendali e sono gestiti con tempestività, imparzialità e tracciabilità.

ART. 66 – CLAUSOLE ETICHE E DIRITTO DI REAZIONE

La Società promuove l'inserimento nei contratti di clausole che richiamino l'obbligo di rispettare il presente Codice Etico, il Modello di Organizzazione, Gestione e Controllo, la Politica Anticorruzione e le altre procedure di compliance applicabili.
La violazione grave o reiterata di tali obblighi può costituire motivo di sospensione, risoluzione del rapporto contrattuale o esclusione da future collaborazioni, fatto salvo il risarcimento dell'eventuale danno subito dalla Società.

CAPITOLO VII

GESTIONE DELLE INFORMAZIONI, SICUREZZA INFORMATICA E UTILIZZO RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

ART. 67 – PRINCIPI GENERALI

Le informazioni costituiscono un patrimonio strategico della Società e rappresentano un elemento essenziale per lo svolgimento delle attività aziendali.
IDRAGEST assicura che la gestione delle informazioni avvenga nel rispetto dei principi di:

1. riservatezza;
2. integrità;
3. disponibilità;
4. autenticità;
5. tracciabilità;
6. protezione dei dati;
7. sicurezza informatica.

Ogni Destinatario è responsabile della corretta gestione delle informazioni di cui venga a conoscenza nello svolgimento della propria attività.

ART. 68 – TUTELA DELLE INFORMAZIONI AZIENDALI

Devono essere protette tutte le informazioni aventi natura:

1. tecnica;
2. commerciale;

3. economica;
4. finanziaria;
5. progettuale;
6. amministrativa;
7. organizzativa;
8. strategica;
9. informatica.

Le informazioni aziendali devono essere utilizzate esclusivamente per finalità connesse all'attività lavorativa e secondo il principio del "need to know", limitando l'accesso ai soli soggetti autorizzati.

È vietata qualsiasi divulgazione non autorizzata, anche dopo la cessazione del rapporto di lavoro o di collaborazione.

ART. 69 – PROTEZIONE DEI DATI PERSONALI

La Società tratta i dati personali nel rispetto del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018, nonché delle procedure interne adottate in materia di protezione dei dati.

Ogni Destinatario è tenuto a:

1. trattare esclusivamente i dati necessari allo svolgimento delle proprie mansioni;
2. garantire l'esattezza e l'aggiornamento delle informazioni trattate;
3. adottare le misure di sicurezza previste dalla Società;
4. evitare accessi non autorizzati;
5. segnalare tempestivamente eventuali violazioni dei dati personali (data breach).

È vietato utilizzare dati personali per finalità estranee alle attività aziendali.

ART. 70 – SICUREZZA INFORMATICA

IDRAGEST considera la sicurezza informatica un elemento essenziale della continuità operativa e della tutela del patrimonio aziendale.

Tutti i Destinatari sono tenuti a:

1. rispettare le procedure di sicurezza informatica;
2. utilizzare esclusivamente dispositivi e software autorizzati;
3. custodire con diligenza le proprie credenziali di accesso;
4. adottare password robuste e riservate;

5. non condividere account personali;
6. proteggere i dispositivi aziendali da accessi non autorizzati;
7. segnalare immediatamente incidenti informatici, tentativi di phishing, malware, violazioni di sicurezza o altri eventi anomali.

È vietato eludere o compromettere i sistemi di sicurezza predisposti dalla Società.

ART. 71 – UTILIZZO DEGLI STRUMENTI INFORMATICI

Le risorse informatiche della Società costituiscono beni aziendali destinati esclusivamente allo svolgimento delle attività lavorative.

I Destinatari devono utilizzare gli strumenti informatici con diligenza, evitando comportamenti idonei a:

1. compromettere la sicurezza della rete;
2. danneggiare sistemi informatici;
3. introdurre software non autorizzati;
4. diffondere virus o altri programmi dannosi;
5. utilizzare piattaforme non autorizzate;
6. effettuare copie abusive di software o banche dati.

L'utilizzo degli strumenti aziendali deve essere conforme alle politiche interne adottate dalla Società.

ART. 72 – PROPRIETÀ INTELLETTUALE E TUTELA DEL KNOW-HOW

La Società tutela il proprio patrimonio di conoscenze, esperienze, metodologie, software, banche dati, algoritmi, elaborazioni progettuali e ogni altra opera dell'ingegno sviluppata nell'ambito dell'attività aziendale.

Ogni Destinatario è tenuto a:

1. salvaguardare il know-how aziendale;
2. rispettare i diritti di proprietà intellettuale della Società e di terzi;
3. non utilizzare software o contenuti in violazione della normativa sul diritto d'autore;
4. non divulgare informazioni riservate senza autorizzazione.

ART. 73 – PRINCIPI PER L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

IDRAGEST riconosce il valore dell'Intelligenza Artificiale quale strumento di supporto all'innovazione, all'efficienza dei processi aziendali e alla qualità delle prestazioni professionali.

L'utilizzo dei sistemi di Intelligenza Artificiale deve essere conforme ai principi di:

1. legalità;
2. trasparenza;
3. affidabilità;
4. supervisione umana;
5. responsabilità;
6. sicurezza;
7. proporzionalità;
8. protezione dei dati personali;
9. non discriminazione;
10. rispetto dei diritti fondamentali.

Ogni utilizzo deve essere coerente con la Policy aziendale sull'uso corretto e responsabile dell'Intelligenza Artificiale.

ART. 74 – SUPERVISIONE UMANA

I sistemi di Intelligenza Artificiale costituiscono esclusivamente strumenti di supporto alle decisioni.

Essi non possono sostituire:

1. il giudizio tecnico;
2. le valutazioni professionali;
3. le decisioni gestionali;
4. le valutazioni giuridiche;
5. le decisioni economiche;
6. le responsabilità dei soggetti aziendali.

Ogni output generato da sistemi di Intelligenza Artificiale deve essere verificato criticamente da personale competente prima del suo utilizzo.

La responsabilità delle decisioni rimane sempre in capo alla persona fisica competente.

ART. 75 – UTILIZZI VIETATI

È vietato utilizzare sistemi di Intelligenza Artificiale per:

1. generare documentazione falsa o alterata;
2. falsificare firme, immagini, video o registrazioni;
3. diffondere informazioni non veritiere;
4. aggirare controlli aziendali;
5. elaborare dati in violazione della normativa privacy;
6. divulgare informazioni riservate;
7. compromettere la sicurezza informatica;
8. discriminare persone o categorie di soggetti;
9. porre in essere attività illecite o contrarie ai principi del presente Codice.

È altresì vietato utilizzare piattaforme di Intelligenza Artificiale non autorizzate dalla Società per il trattamento di dati aziendali, informazioni riservate o dati personali.

ART. 76 – VERIFICA DEGLI OUTPUT

Chi utilizza sistemi di Intelligenza Artificiale è tenuto a verificare:

1. accuratezza;
2. completezza;
3. attendibilità;
4. aggiornamento;
5. coerenza;
6. conformità normativa.

Gli elaborati prodotti mediante sistemi di IA non possono essere utilizzati automaticamente senza un'adeguata verifica umana.

ART. 77 – TRASPARENZA NELL'UTILIZZO DELL'IA

Quando richiesto dalla legge, da obblighi contrattuali o dalle procedure aziendali, l'utilizzo di strumenti di Intelligenza Artificiale deve essere dichiarato in modo trasparente.

La Società promuove un utilizzo consapevole dell'IA, evitando qualsiasi impiego suscettibile di generare opacità, inganno o perdita di fiducia nei confronti di clienti, Pubbliche Amministrazioni, partner commerciali e altri stakeholder.

ART. 78 – FORMAZIONE E AGGIORNAMENTO

La Società promuove programmi di formazione periodica finalizzati ad accrescere la cultura digitale dei propri collaboratori e ad assicurare un utilizzo corretto, sicuro, responsabile ed etico delle tecnologie informatiche e dei sistemi di Intelligenza Artificiale.

I Destinatari sono tenuti a partecipare alle iniziative formative organizzate dalla Società e ad applicare le regole contenute nella Policy IA e nelle procedure interne.

CAPITOLO VIII

TUTELA DELL'AMBIENTE, SOSTENIBILITÀ E RESPONSABILITÀ SOCIALE

ART. 79 – PRINCIPI GENERALI

IDRAGEST riconosce la tutela dell'ambiente, l'uso sostenibile delle risorse naturali e la responsabilità sociale quali elementi fondamentali del proprio modello di sviluppo.

La Società orienta le proprie attività secondo i principi dello sviluppo sostenibile, perseguendo un equilibrio tra crescita economica, tutela ambientale e creazione di valore per la collettività.

Ogni Destinatario è chiamato a contribuire, nell'ambito delle proprie competenze, alla diffusione di comportamenti responsabili e sostenibili.

ART. 80 – TUTELA DELL'AMBIENTE

La Società svolge le proprie attività nel pieno rispetto della normativa ambientale nazionale ed europea.

IDRAGEST promuove una gestione responsabile delle proprie attività attraverso:

- la prevenzione dell'inquinamento;
- la riduzione degli impatti ambientali;
- il miglioramento continuo delle prestazioni ambientali;
- l'utilizzo razionale delle risorse naturali;
- la riduzione degli sprechi;
- la corretta gestione dei rifiuti;
- la tutela del territorio e degli ecosistemi.

Ogni Destinatario è tenuto ad adottare comportamenti coerenti con tali principi.

ART. 81 – USO EFFICIENTE DELLE RISORSE

La Società promuove l'utilizzo efficiente delle risorse energetiche, idriche e materiali.

In particolare, favorisce:

- il contenimento dei consumi energetici;
- la riduzione del consumo di carta;
- la digitalizzazione dei processi;
- il riutilizzo delle risorse ove possibile;
- la raccolta differenziata;
- l'utilizzo di tecnologie a basso impatto ambientale.

Ogni lavoratore è chiamato ad utilizzare responsabilmente le risorse aziendali evitando sprechi e utilizzi impropri.

ART. 82 – INNOVAZIONE PER LA SOSTENIBILITÀ

L'innovazione tecnologica rappresenta uno strumento essenziale per migliorare la sostenibilità delle attività aziendali.

IDRAGEST promuove lo sviluppo e l'utilizzo di tecnologie innovative finalizzate a:

- migliorare l'efficienza delle reti idriche;
- ridurre le perdite idriche;
- ottimizzare l'utilizzo delle infrastrutture;
- favorire la digitalizzazione dei processi;
- migliorare il monitoraggio delle reti;
- incrementare la resilienza delle infrastrutture;
- supportare la transizione ecologica.

La Società incoraggia l'impiego di soluzioni tecnologiche che consentano di coniugare innovazione, qualità del servizio e tutela dell'ambiente.

ART. 83 – RESPONSABILITÀ SOCIALE D'IMPRESA

IDRAGEST considera la responsabilità sociale parte integrante della propria strategia aziendale.

La Società promuove comportamenti improntati a:

- correttezza;
- inclusione;
- rispetto dei diritti umani;

- valorizzazione delle persone;
- tutela della salute e sicurezza;
- legalità;
- integrità;
- sviluppo sostenibile.

La Società favorisce relazioni costruttive con clienti, istituzioni, fornitori, comunità locali e tutti gli stakeholder, contribuendo allo sviluppo del territorio in cui opera.

ART. 84 – DIRITTI UMANI

IDRAGEST riconosce e promuove il rispetto dei diritti umani universalmente riconosciuti.

La Società si impegna a contrastare qualsiasi forma di:

- discriminazione;
- sfruttamento;
- lavoro forzato;
- lavoro minorile;
- tratta di esseri umani;
- violenza;
- molestie;
- abuso.

La Società richiede analogo impegno ai propri partner commerciali, fornitori, consulenti e collaboratori.

ART. 85 – SALUTE E SICUREZZA NEI LUOGHI DI LAVORO

La tutela della salute e della sicurezza rappresenta un valore prioritario.
La Società adotta tutte le misure necessarie per prevenire gli infortuni e le malattie professionali, promuovendo una cultura della prevenzione e della responsabilità condivisa.

Ogni Destinatario è tenuto a:

- rispettare le disposizioni aziendali;
- utilizzare correttamente le attrezzature;
- impiegare i dispositivi di protezione individuale;
- segnalare tempestivamente situazioni di rischio;

- collaborare con il Datore di Lavoro, i dirigenti, i preposti, il RSPP, il Medico Competente e gli altri soggetti del sistema di prevenzione.

ART. 86 – RAPPORTI CON LA COLLETTIVITÀ

La Società promuove rapporti improntati alla trasparenza, al dialogo e alla collaborazione con le comunità locali, le istituzioni, il mondo accademico, gli enti di ricerca e gli altri soggetti che operano nei territori interessati dalle proprie attività.

Le iniziative di carattere sociale, culturale o ambientale devono essere coerenti con i valori della Società e preventivamente autorizzate dagli organi competenti.

ART. 87 – SOSTENIBILITÀ NELLA CATENA DI FORNITURA

IDRAGEST promuove comportamenti sostenibili lungo l'intera filiera.

Nella selezione dei fornitori e dei partner commerciali, la Società valuta, ove pertinente:

- il rispetto della normativa ambientale;
- la tutela dei diritti dei lavoratori;
- la conformità in materia di salute e sicurezza;
- il rispetto dei principi anticorruzione;
- l'adozione di comportamenti eticamente responsabili.

La Società può prevedere verifiche e richiedere ai propri partner l'adozione di misure coerenti con i principi del presente Codice.

ART. 88 – IMPEGNO AL MIGLIORAMENTO CONTINUO

IDRAGEST promuove il miglioramento continuo delle proprie prestazioni in materia di sostenibilità, responsabilità sociale e tutela ambientale.

A tal fine, la Società:

- monitora periodicamente i propri processi;
- promuove iniziative di sensibilizzazione;
- favorisce l'innovazione sostenibile;
- valorizza le proposte di miglioramento provenienti dal personale;
- aggiorna le proprie procedure in funzione dell'evoluzione normativa e tecnologica.

Tutti i Destinatari sono chiamati a contribuire al raggiungimento degli obiettivi di sostenibilità attraverso comportamenti responsabili e coerenti con i valori aziendali.

CAPITOLO IX

TRASPARENZA AMMINISTRATIVA, GESTIONE ECONOMICO-FINANZIARIA E PREVENZIONE DEI REATI SOCIETARI, TRIBUTARI E DI RICICLAGGIO

ART. 89 – PRINCIPI GENERALI

IDRAGEST impronta la gestione amministrativa, economica e finanziaria ai principi di legalità, trasparenza, correttezza, veridicità, completezza, prudenza, tracciabilità e responsabilità.

Ogni operazione economica, patrimoniale e finanziaria deve essere ispirata ai criteri di sana gestione imprenditoriale, nel rispetto della normativa vigente, dei principi contabili applicabili, del Modello di Organizzazione, Gestione e Controllo e delle procedure aziendali.

La Società rifiuta qualsiasi comportamento diretto ad alterare la corretta rappresentazione della situazione economica, patrimoniale e finanziaria aziendale.

ART. 90 – VERIDICITÀ DELLE REGISTRAZIONI CONTABILI

Ogni operazione aziendale deve essere registrata in modo:

- veritiero;
- completo;
- accurato;
- tempestivo;
- documentato;
- verificabile.

Ogni registrazione deve trovare adeguato riscontro nella documentazione di supporto, conservata secondo le procedure aziendali.

È vietata qualsiasi registrazione contabile falsa, incompleta, artificiosa o idonea ad occultare la reale natura delle operazioni.

ART. 91 – BILANCIO E COMUNICAZIONI SOCIALI

La redazione del bilancio d'esercizio e di ogni altra comunicazione societaria deve rappresentare in modo veritiero e corretto la situazione patrimoniale, economica e finanziaria della Società.

Gli amministratori, i dirigenti, i dipendenti e tutti i soggetti coinvolti nella predisposizione della documentazione contabile devono operare con la massima diligenza, assicurando:

- completezza delle informazioni;
- attendibilità dei dati;
- correttezza delle valutazioni;
- trasparenza delle operazioni;
- rispetto dei principi contabili applicabili.

È vietato alterare o omettere informazioni rilevanti al fine di rappresentare una situazione economica diversa da quella reale.

ART. 92 – TRACCIABILITÀ DEI FLUSSI FINANZIARI

Ogni movimentazione finanziaria deve essere:

- autorizzata;
- documentata;
- registrata;
- tracciabile;
- riconducibile ad una specifica operazione economica.

La Società utilizza esclusivamente strumenti di pagamento idonei a garantire la piena tracciabilità delle operazioni.

Sono vietati pagamenti o incassi non documentati, non giustificati o effettuati con modalità tali da impedirne la ricostruzione.

ART. 93 – GESTIONE DELLE RISORSE FINANZIARIE

Le risorse economiche della Società devono essere utilizzate esclusivamente per finalità aziendali legittime.

Ogni impiego di denaro, beni o altre risorse deve essere ispirato ai principi di:

- economicità;
- efficienza;
- trasparenza;
- responsabilità;

- corretta amministrazione.

È vietata qualsiasi forma di utilizzo improprio delle risorse aziendali o di costituzione di fondi occulti o extracontabili.

ART. 94 – PREVENZIONE DEI REATI TRIBUTARI

IDRAGEST assicura il puntuale adempimento degli obblighi tributari e fiscali previsti dalla normativa vigente.

La Società impronta i rapporti con l'Amministrazione finanziaria ai principi di collaborazione, correttezza, trasparenza e buona fede.

È fatto divieto di:

- utilizzare fatture per operazioni inesistenti;
- emettere documentazione fiscale falsa;
- occultare o distruggere documentazione contabile;
- indicare elementi passivi fittizi;
- omettere dati rilevanti ai fini fiscali;
- porre in essere operazioni simulate finalizzate all'evasione fiscale.

Ogni operazione avente rilevanza tributaria deve essere adeguatamente documentata e verificabile.

ART. 95 – PREVENZIONE DEI REATI SOCIETARI

La Società adotta ogni misura idonea a prevenire la commissione dei reati societari previsti dal D.Lgs. 231/2001.

In particolare, è vietato:

- esporre fatti materiali non rispondenti al vero;
- omettere informazioni rilevanti;
- ostacolare l'attività degli organi di controllo;
- alterare documentazione societaria;
- compromettere il corretto funzionamento degli organi sociali;
- porre in essere operazioni simulate o fraudolente.

I rapporti con gli organi di controllo devono essere improntati alla massima collaborazione e trasparenza.

ART. 96 – PREVENZIONE DEL RICICLAGGIO, AUTORICICLAGGIO E FINANZIAMENTO DEL TERRORISMO

IDRAGEST contrasta qualsiasi forma di riciclaggio, autoriciclaggio e finanziamento del terrorismo.

I Destinatari devono prestare particolare attenzione alle operazioni che, per caratteristiche, entità o modalità di esecuzione, possano presentare profili di anomalia.

È fatto divieto di:

- sostituire o trasferire denaro, beni o altre utilità provenienti da attività illecite;
- ostacolare l'identificazione della provenienza illecita di beni o disponibilità finanziarie;
- impiegare risorse di provenienza illecita nell'attività economica;
- utilizzare la Società quale strumento di riciclaggio.

Ogni situazione sospetta deve essere tempestivamente segnalata secondo le procedure aziendali.

ART. 97 – CONSERVAZIONE DELLA DOCUMENTAZIONE

La documentazione amministrativa, contabile, fiscale e societaria deve essere conservata in modo da garantirne:

- autenticità;
- integrità;
- leggibilità;
- reperibilità;
- tracciabilità;
- disponibilità.

È vietata qualsiasi distruzione, alterazione, sottrazione o occultamento della documentazione al di fuori dei casi consentiti dalla legge e dalle procedure aziendali.

ART. 98 – RAPPORTI CON GLI ORGANI DI CONTROLLO

La Società garantisce la massima collaborazione nei confronti:

- dell'Organismo di Vigilanza;
- del Revisore legale;
- del Collegio Sindacale, ove nominato;

- delle Autorità amministrative;
- dell'Autorità Giudiziaria;
- dell'Amministrazione finanziaria;
- degli altri organismi di controllo competenti.

Ogni richiesta di informazioni o documentazione deve essere evasa con tempestività, correttezza, completezza e trasparenza.

ART. 99 – RESPONSABILITÀ INDIVIDUALE

Ogni Destinatario è personalmente responsabile della correttezza delle attività amministrative, contabili e finanziarie di propria competenza.

Chiunque venga a conoscenza di irregolarità, anomalie o comportamenti potenzialmente illeciti è tenuto a segnalarli mediante i canali previsti dalla Procedura Whistleblowing e a collaborare con gli organi di controllo nell'accertamento dei fatti.

CAPITOLO X

SEGNALAZIONI, WHISTLEBLOWING, VIGILANZA E SISTEMA DISCIPLINARE

ART. 100 – CULTURA DELLA SEGNALAZIONE E DELLA PREVENZIONE

IDRAGEST promuove una cultura aziendale fondata sulla legalità, sulla responsabilità individuale e sulla prevenzione dei rischi.

Ogni Destinatario è chiamato a contribuire attivamente al corretto funzionamento del sistema di controllo interno, segnalando tempestivamente comportamenti contrari alla legge, al presente Codice Etico, al Modello di Organizzazione, Gestione e Controllo, alle procedure aziendali o ai principi di correttezza e integrità.

Le segnalazioni costituiscono uno strumento di tutela della Società, delle persone che vi operano e degli stakeholder e rappresentano un elemento essenziale del sistema di prevenzione dei rischi.

ART. 101 – OBBLIGO DI SEGNALAZIONE

I Destinatari che vengano a conoscenza, nell'ambito della propria attività lavorativa, di fatti, comportamenti o situazioni che possano costituire violazione della normativa vigente o dei documenti del sistema di compliance aziendale sono

tenuti a segnalarli tempestivamente attraverso i canali previsti dalla Procedura Whistleblowing.

Possono costituire oggetto di segnalazione, a titolo esemplificativo:

- violazioni del presente Codice Etico;
- violazioni del Modello 231;
- violazioni della Politica Anticorruzione;
- utilizzi non autorizzati o illeciti dei sistemi di Intelligenza Artificiale;
- frodi;
- episodi corruttivi;
- conflitti di interesse non dichiarati;
- falsificazioni documentali;
- irregolarità contabili o fiscali;
- violazioni in materia di salute e sicurezza;
- violazioni della normativa ambientale;
- violazioni della normativa sulla protezione dei dati personali;
- violazioni della sicurezza informatica;
- ogni altra condotta suscettibile di arrecare pregiudizio alla Società o di integrare un illecito.

ART. 102 – PROCEDURA WHISTLEBLOWING

Le segnalazioni sono gestite secondo quanto previsto dalla Procedura Whistleblowing adottata dalla Società, nel rispetto del D.Lgs. 10 marzo 2023, n. 24.

La Procedura disciplina, tra l'altro:

- i canali interni di segnalazione;
- i soggetti legittimati a segnalare;
- le modalità di ricezione e gestione delle segnalazioni;
- le misure di tutela della riservatezza;
- i tempi di gestione;
- le modalità di conservazione della documentazione;
- le competenze dell'Organismo di Vigilanza e degli altri soggetti eventualmente coinvolti.

Le disposizioni della Procedura Whistleblowing costituiscono parte integrante del sistema di compliance della Società.

ART. 103 – TUTELA DEL SEGNALANTE

La Società garantisce la tutela della riservatezza dell'identità del segnalante e di ogni altra informazione la cui divulgazione possa consentirne l'identificazione, nei limiti e secondo le modalità previste dalla normativa vigente.

È vietata qualsiasi forma di ritorsione, discriminazione, penalizzazione o trattamento sfavorevole conseguente all'effettuazione di una segnalazione presentata in buona fede.

Le misure di protezione previste dalla normativa si applicano anche ai facilitatori e agli altri soggetti eventualmente tutelati dal D.Lgs. 24/2023.

ART. 104 – SEGNALAZIONI IN MALA FEDE

La Società tutela esclusivamente le segnalazioni effettuate in buona fede e fondate su elementi di fatto ragionevolmente attendibili.

Restano ferme le responsabilità, anche disciplinari, civili e penali, nei confronti di chi effettui con dolo o colpa grave segnalazioni false, manifestamente infondate, calunniose o diffamatorie ovvero utilizzi il sistema di segnalazione per finalità diverse da quelle previste dalla legge.

ART. 105 – ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza, nell'ambito delle competenze attribuite dal D.Lgs. 231/2001 e dal Modello di Organizzazione, Gestione e Controllo, vigila sull'efficace attuazione del presente Codice Etico.

In particolare, l'Organismo:

- promuove la diffusione della cultura della compliance;
- riceve i flussi informativi previsti dal Modello;
- monitora l'efficacia del Codice Etico;
- propone eventuali aggiornamenti;
- verifica le segnalazioni di propria competenza;
- riferisce periodicamente agli organi societari.

L'Organismo opera con autonomia, indipendenza, professionalità e continuità di azione.

ART. 106 – DOVERE DI COLLABORAZIONE

Tutti i Destinatari sono tenuti a collaborare lealmente con l'Organismo di Vigilanza, con la Funzione di Conformità, con gli organi di controllo e con le funzioni aziendali competenti.

In particolare, essi devono:

- fornire informazioni complete e veritiere;
- mettere tempestivamente a disposizione la documentazione richiesta;
- agevolare le attività di verifica;
- non ostacolare le attività di controllo;
- rispettare gli obblighi di riservatezza.

La mancata collaborazione costituisce violazione del presente Codice Etico.

ART. 107 – SISTEMA DISCIPLINARE

Il rispetto del presente Codice Etico costituisce parte integrante delle obbligazioni contrattuali dei Destinatari.

Le violazioni del Codice sono valutate in relazione:

- alla gravità della condotta;
- all'intenzionalità;
- al grado di colpa;
- alla posizione ricoperta dal soggetto;
- al danno arrecato o al rischio determinato;
- all'eventuale reiterazione.

Le sanzioni sono applicate nel rispetto della normativa vigente, del Contratto Collettivo Nazionale di Lavoro applicabile, del Codice Disciplinare aziendale e del Modello di Organizzazione, Gestione e Controllo.

ART. 108 – MISURE NEI CONFRONTI DEI SOGGETTI TERZI

La violazione del presente Codice Etico da parte di consulenti, fornitori, partner commerciali, collaboratori, professionisti o altri soggetti esterni può comportare, in relazione alla gravità della violazione:

- la richiesta di cessazione del comportamento illecito;
- la sospensione del rapporto contrattuale;
- la risoluzione del contratto ai sensi delle clausole contrattuali applicabili;
- l'esclusione da future collaborazioni;
- la richiesta di risarcimento degli eventuali danni subiti dalla Società.

ART. 109 – MONITORAGGIO E AGGIORNAMENTO DEL CODICE ETICO

L'efficacia del presente Codice Etico è oggetto di monitoraggio periodico.

L'Organismo di Vigilanza può formulare osservazioni e proposte di aggiornamento sulla base:

- dell'evoluzione normativa;
- delle modifiche organizzative della Società;
- dell'esperienza applicativa;
- delle risultanze delle attività di vigilanza;
- delle segnalazioni ricevute;
- dell'evoluzione dei rischi aziendali.

Le modifiche al presente Codice Etico sono approvate dal Consiglio di Amministrazione.

CAPITOLO XI

DISPOSIZIONI FINALI

ART. 110 – ADOZIONE ED ENTRATA IN VIGORE

Il presente Codice Etico è adottato dall'Organo Amministrativo della Società quale parte integrante del sistema di governance e del Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D.Lgs. 8 giugno 2001, n. 231.

Il Codice entra in vigore dalla data della sua approvazione e si applica a tutti i Destinatari indicati nel presente documento.

ART. 111 – DIFFUSIONE DEL CODICE ETICO

La Società assicura la più ampia diffusione del presente Codice Etico.

A tal fine provvede, secondo le modalità ritenute più idonee, a:

- pubblicarlo negli strumenti informatici aziendali e, ove previsto, sul sito istituzionale;
- renderlo disponibile a tutti i Destinatari;
- consegnarlo ai neoassunti e ai nuovi collaboratori;
- richiederne la presa visione e l'impegno al rispetto;
- richiamarne i principi nei rapporti contrattuali con clienti, fornitori, consulenti, partner e collaboratori.

La Società promuove altresì la conoscenza del Codice nei confronti degli stakeholder esterni, favorendone la consultazione.

ART. 112 – FORMAZIONE E SENSIBILIZZAZIONE

La Società promuove iniziative periodiche di informazione, formazione e sensibilizzazione finalizzate ad assicurare la conoscenza e la corretta applicazione del presente Codice Etico.

I programmi formativi sono modulati in funzione del ruolo, delle responsabilità e del livello di rischio connesso alle attività svolte dai Destinatari.

Particolare attenzione è riservata alla formazione in materia di:

- Modello 231;
- prevenzione della corruzione;
- protezione dei dati personali;
- sicurezza informatica;
- utilizzo responsabile dell'Intelligenza Artificiale;
- salute e sicurezza sul lavoro;
- prevenzione dei reati presupposto.

La partecipazione alle attività formative costituisce parte integrante degli obblighi professionali dei Destinatari.

ART. 113 – COORDINAMENTO CON IL SISTEMA DI COMPLIANCE

Il presente Codice Etico costituisce il documento di riferimento dei principi e dei valori cui si ispira il sistema di compliance della Società.

Esso opera in coordinamento con:

- il Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D.Lgs. 231/2001;
- il Codice Disciplinare;
- la Procedura Whistleblowing;
- la Politica Anticorruzione;
- la Politica sull'utilizzo dell'Intelligenza Artificiale;
- le procedure aziendali;
- i regolamenti interni;
- le istruzioni operative;
- le ulteriori policy adottate dalla Società.

In caso di contrasto tra le disposizioni del presente Codice e quelle contenute nella normativa vigente, prevalgono le disposizioni di legge.

Le procedure aziendali disciplinano gli aspetti operativi necessari all'attuazione dei principi contenuti nel presente Codice.

ART. 114 – INTERPRETAZIONE DEL CODICE ETICO

Ogni dubbio interpretativo concernente l'applicazione del presente Codice deve essere sottoposto ai competenti responsabili aziendali.

Per le materie rientranti nell'ambito di applicazione del Modello di Organizzazione, Gestione e Controllo, possono essere richiesti chiarimenti all'Organismo di Vigilanza, ferme restando le competenze degli organi societari e delle funzioni aziendali interessate.

L'interpretazione del Codice deve essere sempre coerente con i principi di legalità, correttezza, trasparenza, responsabilità e buona fede.

ART. 115 – REVISIONE E AGGIORNAMENTO

Il presente Codice Etico è soggetto a revisione periodica al fine di garantirne il costante allineamento:

- all'evoluzione della normativa nazionale ed europea;
- alle Linee Guida di Confindustria;
- alle modifiche del Modello di Organizzazione, Gestione e Controllo;
- all'evoluzione dell'organizzazione aziendale;
- ai risultati delle attività di vigilanza e audit;
- alle migliori prassi di corporate governance e compliance;
- all'evoluzione tecnologica e digitale;
- ai rischi emergenti.

L'Organismo di Vigilanza può formulare osservazioni e proposte di aggiornamento nell'ambito delle proprie attività di vigilanza.

Le modifiche del presente Codice sono approvate dall'Organo Amministrativo della Società.

ART. 116 – IMPEGNO DEI DESTINATARI

Ogni Destinatario è tenuto a:

- conoscere il presente Codice Etico;
- conformare la propria condotta ai principi in esso contenuti;
- collaborare alla sua effettiva attuazione;
- partecipare alle attività formative previste dalla Società;

- segnalare eventuali violazioni secondo le procedure aziendali.

Il rispetto del presente Codice costituisce elemento essenziale del rapporto fiduciario tra la Società e i propri Destinatari.

DISPOSIZIONE FINALE

Il presente Codice Etico rappresenta l'espressione dei valori, dei principi e degli standard di comportamento cui IDRAGEST ispira la propria attività.

La Società considera la legalità, l'integrità, la trasparenza, la responsabilità, la sostenibilità, l'innovazione e il rispetto della persona elementi imprescindibili per la creazione di valore durevole e per il mantenimento della fiducia dei propri clienti, lavoratori, partner commerciali, istituzioni e di tutti gli stakeholder.

L'osservanza del presente Codice costituisce un impegno condiviso e permanente, volto a rafforzare la cultura della compliance, la prevenzione dei rischi e la reputazione della Società.

APPENDICE DI DETTAGLIO AI FINI DEL D.LGS. 231/2001

Il Codice Etico costituisce un elemento del Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/01.

Il Decreto Legislativo 8 giugno 2001, n. 231, prevede che la Società possa essere ritenuta responsabile per i reati commessi nel suo interesse o vantaggio. Il Decreto stabilisce all'art. 6 che la Società non risponde del reato commesso qualora dimostri (tra l'altro) di aver adottato ed efficacemente attuato Modelli di organizzazione, gestione e controllo idonei a prevenire i reati della specie di quello verificatosi.

Con la locuzione "Modello di organizzazione e gestione" richiamata dall'art. 6, comma 1, lett. a), del Decreto, si intende fare riferimento ad un complesso di regole, al Codice Etico, agli strumenti e condotte costruiti sull'evento reato, funzionale a dotare la Società di un efficace sistema organizzativo e di controllo. Scopo del Modello Organizzativo, e quindi anche del Codice Etico, è quello di essere ragionevolmente idoneo ad individuare e prevenire le condotte penalmente rilevanti poste in essere nell'interesse o a vantaggio della Società, da soggetti "apicali" o sottoposti alla loro direzione e/o vigilanza.

Le norme del Codice Etico costituiscono parte essenziale delle obbligazioni contrattuali del personale ai sensi e per gli effetti degli articoli 2104 e 2105 del codice civile.

Qualsiasi comportamento posto in essere dai Dipendenti, dai Collaboratori e da tutti i Destinatari che intrattengono rapporti con la Società in contrasto con le regole previste nel seguente Codice Etico, lede il rapporto di fiducia instaurato con l'azienda e può determinare, come previsto da specifiche clausole contrattuali, azioni disciplinari e di risarcimento del danno, fermo restando, per i lavoratori dipendenti, il rispetto delle procedure previste dai contratti collettivi di lavoro e dal Sistema disciplinare adottato dalla Società.

La IDRAGEST S.r.l. è consapevole del fatto che l'integrità e i valori etici sono elementi essenziali dell'ambiente di controllo della propria organizzazione e che essi incidono significativamente sulla progettazione, sull'amministrazione e sull'operatività quotidiana del proprio business.

Invero, affinché non vi siano incertezze o fraintendimenti su ciò che IDRAGEST S.r.l. richiede a tutti i Destinatari dello stesso, il presente Codice Etico e il modo in cui esso è inserito nella struttura di controllo dell'organizzazione saranno oggetto di frequenti azioni di formazione e comunicazione, al fine di consentire che il medesimo diventi patrimonio comune e condiviso a tutti i livelli.



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

ALLEGATO - 2 -

CLAUSOLA CONTRATTUALE

Ai fini di garantire l'osservanza e divulgazione del Modello Organizzativo di cui al D.Lgs. 231/2001, IDRAGEST intende inserire tra le condizioni generali di contratto le seguenti dichiarazioni.

1) CLAUSOLA PER CONTROPARTE DOTATA DI UN PROPRIO CODICE ETICO

"Le parti si danno reciprocamente atto di aver preso visione dei codici di condotta e modelli organizzativi di cui al D.Lgs. 231/2001. Ciascuna delle parti si impegna a tenere, nell'esecuzione delle prestazioni oggetto del presente contratto, comportamenti in linea con i propri codici di condotta e modelli organizzativi, nonchè a farvi attenere i propri dipendenti, consulenti, collaboratori, fornitori, soci, partner d'affari e chiunque partecipi all'esecuzione del contratto stesso.

Le parti riconoscono che l'osservanza delle disposizioni tutte del Codice Etico e dei principi e delle norme di comportamento contenuti nel proprio Modello organizzativo, nonchè la prevenzione, sotto ogni forma, delle criticità e dei rischi evidenziati dal medesimo modello organizzativo è considerata parte essenziale, nell'interesse di entrambe le parti, anche ai sensi e per gli effetti dell'articolo 1456 c.c., delle obbligazioni assunte con il presente contratto."

2) CLAUSOLA PER CONTROPARTE NON DOTATA DI UN PROPRIO CODICE ETICO

"La parte X dichiara di conoscere e di aver preso atto delle previsioni di cui al Decreto Legislativo 8 giugno 2001 n. 231 (il "Decreto") e si impegna ad improntare il proprio comportamento, finalizzato all'attuazione del presente contratto, a principi di trasparenza e correttezza e all'osservanza del Decreto, dichiarando, altresì, di non essere sino ad ora mai incorsi nella commissione di uno dei reati nello stesso contemplati.

La parte X dichiara altresì di aver preso atto che IDRAGEST S.r.l. ha adottato il Modello di organizzazione, gestione e controllo di cui al citato Decreto (il "Modello"), nonchè un proprio Codice Etico contenente i principi di etica aziendale (il "Codice Etico", consultabile all'indirizzo Internet www.idragest.it) e di impegnarsi ad aderire per sè e, ai sensi dell'art. 1381 c.c., per i propri consulenti, collaboratori, dipendenti, fornitori e partner d'affari ai principi etico-comportamentali che IDRAGEST ha enunciato nel proprio Codice Etico, di cui dichiara di aver preso visione.

L'inosservanza da parte di X delle disposizioni e/o dei principi sanciti dal Decreto e/o dal Codice Etico comporterà un inadempimento grave degli obblighi di cui al presente contratto e legittimerà IDRAGEST a risolvere lo stesso, ai sensi e per gli effetti di cui all'art. 1456 c.c., fermo restando il risarcimento dei danni eventualmente causati a IDRAGEST".



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

ALLEGATO - 3 -

ELENCO REATI SANZIONATI DAL DECRETO

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, D.Lgs. n. 231/2001) [articolo modificato dalla L. 161/2017, dal D.Lgs. n. 75/2020 e dalla L. n. 137/2023]

- Malversazione di erogazioni pubbliche (art. 316-bis c.p.) [articolo modificato dal D.L. n. 13/2022]
- Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.) [articolo modificato dalla L. n. 3/2019 e dal D.L. n. 13/2022]
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art.640, comma 2, n.1, c.p.) [articolo modificato dal D.Lgs. n. 75/2020 e dalla Legge n. 90/2024]
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.) [articolo modificato dal D.L. n. 13/2022]
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)
- Frode nelle pubbliche forniture (art. 356 c.p.) [articolo introdotto dal D.Lgs. n. 75/2020]
- Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n.898) [articolo introdotto dal D.Lgs. n. 75/2020]
- Turbata libertà degli incanti (art. 353 c.p.) [articolo introdotto dalla L. n. 137/2023]
- Turbata libertà del procedimento di scelta del contraente (art. 353-bis) [articolo introdotto dalla L. n. 137/2023]

2. Delitti informatici e trattamento illecito di dati (Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019]

- Documenti informatici (art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) [articolo modificato dalla Legge n. 90/2024]
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.) [articolo modificato dalla Legge n. 238/2021 e modificato dalla Legge n. 90/2024]

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) [articolo modificato dalla Legge n. 238/2021 e dalla Legge n. 90/2024]
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) [articolo modificato dalla Legge n. 238/2021 e dalla Legge n. 90/2024]
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.) [articolo modificato dalla Legge n. 90/2024]
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.) [articolo modificato dalla Legge n. 90/2024]
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) [articolo modificato dalla Legge n. 90/2024]
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1 c.p.) [articolo introdotto dalla Legge n. 90/2024]
- Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies c.p.) [articolo modificato dalla Legge n. 90/2024]
- Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)
- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)
- Estorsione (art. 629, comma 3, c.p.) [articolo aggiunto dalla Legge n. 90/2024]

3. Delitti di criminalità organizzata (Art. 24-ter, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009 e modificato dalla L. 69/2015]

- Associazione di tipo mafioso anche straniere (art. 416-bis c.p.) [articolo modificato dalla L. n. 69/2015]
- Associazione per delinquere (art. 416 c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.) [così sostituito dall´art. 1, comma 1, L. 17 aprile 2014, n. 62, a decorrere dal 18 aprile 2014, ai sensi di quanto disposto dall´art. 2, comma 1 della medesima L. 62/2014)
- Sequestro di persona a scopo di estorsione (art. 630 c.p.)
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990, n. 309) [comma 7-bis aggiunto dal D.Lgs. n. 202/2016]
- Tutti i delitti se commessi avvalendosi delle condizioni previste dall´art. 416-bis c.p. per agevolare l´attività delle associazioni previste dallo stesso articolo (L. 203/91)
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste

dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110 (art. 407, co. 2, lett. a), numero 5), c.p.p.)

4. Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità e corruzione (Art. 25, D.Lgs. n. 231/2001) [modificato dalla L. n. 190/2012, dalla L. 3/2019, dal D.Lgs. n. 75/2020, dalla L. 112/2024 e dalla L. 114/2024]

- Concussione (art. 317 c.p.) [articolo modificato dalla L. n. 69/2015]
- Corruzione per l'esercizio della funzione (art. 318 c.p.) [modificato dalla L. n. 190/2012, L. n. 69/2015 e L. n. 3/2019]
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.) [articolo modificato dalla L. n. 69/2015]
- Circostanze aggravanti (art. 319-bis c.p.)
- Corruzione in atti giudiziari (art. 319-ter c.p.) [articolo modificato dalla L. n. 69/2015]
- Induzione indebita a dare o promettere utilità (art. 319-quater c.p.) [articolo aggiunto dalla L. n. 190/2012 e modificato dalla L. n. 69/2015]
- 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.)
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione, abuso d'ufficio, di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.) [articolo modificato dalla L. n. 190/2012, dalla L n. 3/2019 e dal D.L. n. 92/2024]
- Traffico di influenze illecite (art. 346-bis c.p.) [modificato dalla L. 3/2019 e dalla L. 114/2024]
- Peculato (limitatamente al primo comma) (art. 314 c.p.) [introdotto dal D.Lgs. n. 75/2020]
- Peculato mediante profitto dell'errore altrui (art. 316 c.p.) [introdotto dal D.Lgs. n. 75/2020]
- Indebita destinazione di denaro o cose mobili (art. 314-bis c.p.) [articolo introdotto dalla L. n. 112/2024]

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

- Alterazione di monete (art. 454 c.p.)

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.)
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.)
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.)
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

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

- Illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.)
- Turbata libertà dell'industria o del commercio (art. 513 c.p.)
- Frodi contro le industrie nazionali (art. 514 c.p.)
- Frode nell'esercizio del commercio (art. 515 c.p.)
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.) [articolo modificato dalla L. n. 206/2023]
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)
- Contraffazione dei segni di indicazione geografica e di denominazione protetta dei prodotti agroalimentari (art. 517-quater c.p.) [articolo modificato dalla L. n. 75/2026]
- Pena accessoria e circostanze aggravanti (art. 517-octies, comma 4) [articolo aggiunto dalla L. n. 206/2023]

7. Reati societari (Art. 25-ter, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. 69/2015, dal D.Lgs. n.38/2017 e dal D.Lgs. n. 19/2023]

- False comunicazioni sociali (art. 2621 c.c.) [articolo modificato dalla L. n. 69/2015]
- Fatti di lieve entità (art. 2621-bis c.c.)
- False comunicazioni sociali delle società quotate (art. 2622 c.c.) [articolo modificato dalla L n. 69/2015]

- Impedito controllo (art. 2625, comma 2, c.c.)
- Indebita restituzione di conferimenti (art. 2626 c.c.)
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.) [aggiunto dalla legge n. 262/2005]
- Formazione fittizia del capitale (art. 2632 c.c.)
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
- Corruzione tra privati (art. 2635 c.c.) [aggiunto dalla legge n. 190/2012; modificato dal D.Lgs. n. 38/2017 e dalla L. n. 3/2019]
- Istigazione alla corruzione tra privati (art. 2635-bis c.c.) [aggiunto dal D.Lgs. n. 38/2017 e modificato dalla L. n. 3/2019]
- Illecita influenza sull'assemblea (art. 2636 c.c.)
- Aggiotaggio (art. 2637 c.c.) [articolo modificato dalla Legge n. 132/2025]
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.) [articolo modificato dal D.Lgs. n. 224/2023]
- False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023) [aggiunto dal D.Lgs. n. 19/2023]

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

- Associazioni sovversive (art. 270 c.p.)
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.)
- Assistenza agli associati (art. 270 ter c.p.)
- Arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.)
- Organizzazione di trasferimento per finalità di terrorismo (art. 270-quater.1) [introdotto dal D.L. n. 7/2015, convertito, con modificazioni, dalla L. n. 43/2015]
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies c.p.)
- Finanziamento di condotte con finalità di terrorismo (L. n. 153/2016, art. 270 quinquies.1 c.p.)
- Sottrazione di beni o denaro sottoposti a sequestro (art. 270 quinquies.2 c.p.)
- Detenzione di materiale con finalità di terrorismo (art. 270-quinquies.3 c.p.) [Articolo inserito dal D.L. n. 48/2025, convertito, con modificazioni, dalla L. n. 80/2025]
- Condotte con finalità di terrorismo (art. 270 sexies c.p.)
- Attentato per finalità terroristiche o di eversione (art. 280 c.p.)

- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis c.p.)
- Atti di terrorismo nucleare (art. 280 ter c.p.)
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.)
- Sequestro a scopo di coazione (art. 289-ter c.p.) [introdotto dal D.Lgs. 21/2018]
- Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo (art. 302 c.p.)
- Cospirazione politica mediante accordo (art. 304 c.p.)
- Cospirazione politica mediante associazione (art. 305 c.p.)
- Banda armata: formazione e partecipazione (art. 306 c.p.)
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.)
- Impossessamento, dirottamento e distruzione di un aereo (L. n. 342/1976, art. 1)
- Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2)
- Sanzioni (L. n. 422/1989, art. 3)
- Pentimento operoso (D.Lgs. n. 625/1979, art. 5)
- Convenzione di New York del 9 dicembre 1999 (art. 2)

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

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

10. Delitti contro la personalità individuale (Art. 25-quinquies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003; modificato dalla L. n. 199/2016 e dal D.Lgs. n. 115/2026]

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.) [articolo modificato dal D.Lgs. n. 115/2026]
- Prostituzione minorile (art. 600-bis c.p.)
- Pornografia minorile (art. 600-ter c.p.)
- Detenzione o accesso a materiale pornografico (art. 600-quater) [articolo modificato dalla Legge n. 238/2021]
- Pornografia virtuale (art. 600-quater.1 c.p.) [aggiunto dall'art. 10, L. 6 febbraio 2006 n. 38]
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.)
- Tratta di persone (art. 601 c.p.) [modificato dal D.Lgs. n. 21/2018 e dal D.Lgs. n. 115/2026]
- Acquisto e alienazione di schiavi (art. 602 c.p.)
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)
- Adescamento di minorenni (art. 609-undecies c.p.) [articolo modificato dalla Legge n. 238/2021]
- Approfittamento della vittima di riduzione in schiavitù o di tratta (Art. 601.1 c.p.) [articolo aggiunto dal D.Lgs. n. 115/2026]

11. Reati di abuso di mercato (Art. 25-sexies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005]

- Manipolazione del mercato (art. 185 D.Lgs. n. 58/1998) [articolo modificato dal D.Lgs. 107/2018, dalla Legge n. 238/2021 e dalla Legge n. 132/2025]
- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 D.Lgs. n. 58/1998) [articolo modificato dalla Legge n. 238/2021]

12. Altre fattispecie in materia di abusi di mercato (Art. 187-quinquies TUF) [articolo modificato dal D.Lgs. n. 107/2018]

- Divieto di manipolazione del mercato (art. 15 Reg. UE n. 596/2014)
- Divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art. 14 Reg. UE n. 596/2014)

13. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Art. 25-septies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007; modificato L. n. 3/2018]

- Lesioni personali colpose (art. 590 c.p.)
- Omicidio colposo (art. 589 c.p.)

14. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonchè autoriciclaggio (Art. 25-octies, D.Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014 e dal D.Lgs. n. 195/2021]

- Ricettazione (art. 648 c.p.) [articolo modificato dal D.Lgs. 195/2021]
- Riciclaggio (art. 648-bis c.p.) [articolo modificato dal D.Lgs. 195/2021]
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.) [articolo modificato dal D.Lgs. 195/2021]
- Autoriciclaggio (art. 648-ter.1 c.p.) [articolo modificato dal D.Lgs. 195/2021]

15. Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori (Art. 25-octies.1, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. 184/2021 e modificato dalla L. n. 137/2023]

- 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 aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.)
- Trasferimento fraudolento di valori (art. 512-bis) [articolo introdotto dalla L. n. 137/2023 e modificato dal D.L. 19/2024]

16. Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1 comma 2, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. 184/2021]

- Altre fattispecie

17. Reati in materia di violazione di misure restrittive dell'Unione europea (Art. 25-octies.2, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. 211/2025]

- Violazione delle misure restrittive dell'Unione europea (art. 275-bis c.p.) [articolo introdotto dal D.Lgs. n. 211/2025]
- Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione europea (art. 275-terc.p.) [articolo introdotto dal D.Lgs. n. 211/2025]
- Violazione delle condizioni dell'autorizzazione allo svolgimento di attività (art. 275-quater c.p.) [articolo introdotto dal D.Lgs. n. 211/2025]
- Morte o lesioni come conseguenza di delitti in materia di immigrazione clandestina (art. 12, comma 1-bis, D.Lgs. 286/1998) [comma introdotto dal D.Lgs. n. 211/2025]

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

- Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, legge n.633/1941 comma 1 lett. a-bis) [articolo modificato dalla Legge n. 132/2025]
- Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, legge n.633/1941 comma 3)
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis legge n.633/1941 comma 1) [articolo modificato dalla L. 166/2024]

- Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis legge n.633/1941 comma 2) [articolo modificato dalla L. 166/2024]
- Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941) [articolo modificato dalla L. 166/2024]
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941) [articolo modificato dalla L. 166/2024]
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

19. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 116/2009]

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

20. Reati ambientali (Art. 25-undecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 121/2011; modificato dalla L. n. 68/2015; modificato dal D.Lgs. n. 21/2018, dalla L. n. 137/202 e dal D.Lgs. 81/2026]

- Inquinamento ambientale (art. 452-bis c.p.) [articolo modificato dalla L. n. 137/2023 e dal D.Lgs. 81/2026]
- Disastro ambientale (art. 452-quater c.p.) [articolo modificato dalla L. n. 137/2023]
- Delitti colposi contro l´ambiente (art. 452-quinquies c.p.)
- Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.) [articolo modificato dalla Legge n. 137/2023 e dal Decreto Legge n. 116/2025]

- Circostanze aggravanti (art. 452-octies c.p.)
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.) [articolo modificato dalla Legge n. 82/2025]
- Distruzione o deterioramento di habitat all´interno di un sito protetto (art. 733-bis c.p.) [articolo modificato dalla Legge n. 82/2025]
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n.150/1992, art. 1, art. 2, art. 3-bis e art. 6)
- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D. Lgs n.152/2006, art. 137)
- Attività di gestione di rifiuti non autorizzata (D. Lgs n.152/2006, art. 256) [articolo modificato dal Decreto Legge n. 116/2025 e modificato dalla Legge n. 147/2025]
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D. Lgs n. 152/2006, art. 257)
- Spedizione illegale di rifiuti (D. Lgs n.152/2006, art. 259) [articolo modificato dal Decreto Legge n. 116/2025 e dalla Legge n. 147/2025]
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D. Lgs n.152/2006, art. 258) [articolo modificato dal Decreto Legge n. 116/2025 e dalla Legge n. 147/2025]
- Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.) [articolo introdotto dal Decreto Legislativo n. 21/2018, modificato dal Decreto Legge n. 116/2025 e dalla Legge n. 147/2025]
- False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (D. Lgs n.152/2006, art. 260-bis)
- Sanzioni (D.Lgs. n. 152/2006, art. 279)
- Inquinamento doloso provocato da navi (D. Lgs. n.202/2007, art. 8)
- Inquinamento colposo provocato da navi (D. Lgs. n.202/2007, art. 9)
- Cessazione e riduzione dell´impiego delle sostanze lesive (L. n. 549/1993 art. 3)
- Abbandono di rifiuti in casi particolari (D.Lgs. n.152/2006, art. 255-bis [articolo introdotto dal Decreto Legge n. 116/2025 e modificato dalla Legge n. 147/2025]
- Abbandono di rifiuti pericolosi (D.Lgs. n.152/2006, art. 255-ter) [articolo introdotto dal Decreto Legge n. 116/2025]
- Combustione illecita di rifiuti (D.Lgs. n.152/2006, art. 256-bis) [articolo introdotto dal Decreto Legge n. 116/2025]
- Aggravante dell'attività d'impresa (D.Lgs. n.152/2006, art. 259-bis) [articolo introdotto dal Decreto Legge n. 116/2025 e modificato dalla Legge n. 147/2025]

- Impedimento del controllo (art. 452-septies c.p.) [articolo introdotto dal Decreto Legge n. 116/2025]
- Omessa bonifica (art. 452-terdecies c.p.) [articolo introdotto dal Decreto Legge n. 116/2025]
- Commercio di prodotti inquinanti (Art. 452-bis.1) [articolo aggiunto dal D.Lgs. n. 81/2026]
- Produzione e commercio di sostanze ozono lesive (art. 4 D.Lgs. n. 81/2026) [articolo aggiunto dal D.Lgs. n. 81/20
- Produzione e commercio di gas a effetto serra (art. 5 D.Lgs. n. 81/2026) [articolo aggiunto dal D.Lgs. n. 81/2026]

21. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 109/2012, modificato dalla Legge 17 ottobre 2017 n. 161 e dal D.L. n. 20/2023]

- Disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3 bis, 3 ter e comma 5, D.Lgs. n. 286/1998) [articolo modificato dal D.Lgs. n. 211/2025]
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12 bis, D.Lgs. n. 286/1998) [articolo modificato dalla Legge n. 187/2024]

22. Razzismo e xenofobia (Art. 25-terdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla Legge 20 novembre 2017 n. 167, modificato dal D.Lgs. n. 21/2018]

- Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (art. 604-bis c.p.) [aggiunto dal D.Lgs. n. 21/2018]

23. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 39/2019]

- Frodi in competizioni sportive (art. 1, L. n. 401/1989)
- Esercizio abusivo di attività di giuoco o di scommessa (art. 4, L. n. 401/1989)

24. Reati Tributari (Art. 25-quinquesdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 157/2019 e dal D.Lgs. n. 75/2020]

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000)
- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000)
- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000)
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)

- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]
- Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]
- Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000) [articolo introdotto dal D.Lgs. n. 75/2020 e modificato dal D.Lgs. n. 87/2024]

25. Contrabbando (Art. 25-sexiesdecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 75/2020 e modificato dal D.Lgs. 141/2024]

- Contrabbando per omessa dichiarazione (art. 78 D.Lgs. n. 141/2024)
- Contrabbando per dichiarazione infedele (art. 79 D.Lgs. n. 141/2024)
- Contrabbando nel movimento delle merci marittimo, aereo e nei laghi di confine (art. 80 D.Lgs. n. 141/2024)
- Contrabbando per indebito uso di merci importate con riduzione totale o parziale dei diritti (art. 81 D.Lgs. n. 141/2024)
- Contrabbando nell'esportazione di merci ammesse a restituzione di diritti (art. 82 D.Lgs. n. 141/2024)
- Contrabbando nell'esportazione temporanea e nei regimi di uso particolare e di perfezionamento (art. 83 D.Lgs. n. 141/2024)
- Contrabbando di tabacchi lavorati (art. 84 D.Lgs. n. 141/2024)
- Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati (art. 85 D.Lgs. n. 141/2024)
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati (art. 86 D.Lgs. n. 141/2024)
- Equiparazione del delitto tentato a quello consumato (art. 87 D.Lgs. n. 141/2024)
- Circostanze aggravanti del contrabbando (art. 88 D.Lgs. n. 141/2024) [articolo modificato dal D.Lgs. 81/2025]
- Sottrazione all'accertamento o al pagamento dell'accisa sui prodotti energetici (art. 40 D.Lgs. n. 504/1995)
- Sottrazione all'accertamento o al pagamento dell'accisa sui tabacchi lavorati (art. 40-bis D.Lgs. n. 504/1995)
- Fabbricazione clandestina di alcole e di bevande alcoliche (art. 41 D.Lgs. n. 504/1995)
- Associazione a scopo di fabbricazione clandestina di alcole e di bevande alcoliche (art. 42 D.Lgs. n. 504/1995)
- Sottrazione all'accertamento ed al pagamento dell'accisa sull'alcole e sulle bevande alcoliche (art. 43 D.Lgs. n. 504/1995)
- Circostanze aggravanti (art. 45 D.Lgs. n. 504/1995)
- Alterazione di congegni, impronte e contrassegni (art. 46 D.Lgs. n. 504/1995)

26. Delitti contro il patrimonio culturale (Art. 25-septiesdecies, D.Lgs. n. 231/2001) [Articolo aggiunto dalla L. n. 22/2022 e modificato dalla L. n. 6/2024]

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

27. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25-duodevicies, D.Lgs. n. 231/2001) [Articolo aggiunto dalla L. n. 22/2022]

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

28. Delitti contro gli animali (Art. 25-undevicies, D.Lgs. n. 231/2001) [Articolo aggiunto dalla L. n. 82/2025]

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

29. Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013) [Costituiscono presupposto per gli enti che operano nell´ambito della filiera degli oli vergini di oliva]

- Commercio di sostanze alimentari contraffatte o adulterate (art. 442 c.p.)
- Adulterazione e contraffazione di sostanze alimentari (art. 440 c.p.)
- Commercio di sostanze alimentari nocive (art. 444 c.p.)
- Contraffazione, alterazione o uso di segni distintivi di opere dell´ingegno o di prodotti industriali (art. 473 c.p.)
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)
- Frode nell´esercizio del commercio (art. 515 c.p.)

- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.) [articolo modificato dalla L. n. 206/2023]
- Contraffazione dei segni di indicazione geografica e di denominazione protetta dei prodotti agroalimentari (art. 517-quater c.p.) [articolo modificato dalla L. n. 75/2026]

30. Reati transnazionali (L. n. 146/2006) [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]

- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al D. Lgs. 25 luglio 1998, n. 286)
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309)
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al D.P.R. 23 gennaio 1973, n. 43)
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)
- Favoreggiamento personale (art. 378 c.p.)
- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniere (art. 416-bis c.p.)

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

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



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

ALLEGATO - 4 -

COMPOSIZIONE ORGANISMO DI VIGILANZA

Il compito di vigilare continuativamente sull'efficace attuazione, sul funzionamento, sull'osservanza del Modello e di proporne l'aggiornamento al fine di migliorarne l'efficacia nella prevenzione dei reati e degli illeciti, in conformità all'art. 6 del D. Lgs. 231/2001, è affidato all'Organismo di Vigilanza, organismo esterno ad IDRAGEST, dotato di autonomi poteri di iniziativa e di controllo.

In considerazione dell'assetto di governance adottato da IDRAGEST, della sua dimensione e della complessità organizzativa della sua struttura, le funzioni di Organismo di Vigilanza sono attribuite ad un organismo monocratico, esterno ad IDRAGEST S.r.l., in grado di garantire autonomia, indipendenza, professionalità e onorabilità nell'esercizio dei compiti allo stesso demandati.

L'Organismo di Vigilanza si occupa esclusivamente, ai sensi del D. Lgs. 231/2001, della vigilanza sull'attuazione e sull'osservanza del Modello da parte dei soggetti allo stesso sottoposti e formula proposte di sua modifica, per migliorarne l'efficacia di prevenzione dei reati compresi nel catalogo contenuto nel D. Lgs. 231/2001.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

ALLEGATO -5-

COSTITUZIONE, COMPENSI, CAUSE DI (IN) ELEGGIBILITÀ, DECADENZA E SOSPENSIONE DEI COMPONENTI DELL'ORGANISMO DI VIGILANZA

Il Consiglio di Amministrazione di IDRAGEST si riserva di stabilire per l'intera durata della carica il compenso annuo spettante al componente monocratico dell'Organismo di Vigilanza.

Al componente monocratico dell'Organismo di Vigilanza compete, inoltre, il rimborso delle spese vive e documentate sostenute nell'espletamento dell'incarico.

INELEGGIBILITÀ

Il componente monocratico dell'Organismo di Vigilanza deve essere in possesso dei requisiti di onorabilità di cui all'art. 109 del D.Lgs. 1 settembre 1993, n. 385: in particolare, non può essere nominato componente dell'Organismo di Vigilanza colui che si trovi nelle condizioni previste dall'art. 2399 c.c..

Non può, inoltre, essere nominato alla carica di componente monocratico dell'Organismo di Vigilanza colui il quale è stato condannato con sentenza divenuta definitiva, anche se emessa ex artt. 444 e ss. c.p.p. e anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:

1) alla reclusione per un tempo non inferiore ad un anno per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267;

2) alla pena detentiva per un tempo non inferiore ad un anno per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;

3) alla reclusione per un tempo non inferiore ad un anno per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, per un delitto in materia tributaria;

4) per un qualunque delitto non colposo alla pena della reclusione per un tempo non inferiore a due anni;

5) per uno dei reati previsti dal titolo XI del libro V del codice civile così come riformulato del D.Lgs. 61/02;

6) per un reato che importi e abbia importato la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;

7) per uno o più reati tra quelli tassativamente previsti dal Decreto anche se con condanne a pene inferiori a quelle indicate ai punti precedenti;

8) coloro che hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate le sanzioni previste dall'art. 9 del Decreto;

9) coloro nei cui confronti sia stata applicata in via definitiva una delle misure di prevenzione previste dall'art. 10, comma 3, della legge 31 maggio 1965, n. 575, come sostituito dall'articolo 3 della legge 19 marzo 1990, n. 55 e successive modificazioni;

10) coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187 quater Decreto Legislativo n. 58/1998.

Il Consiglio di Amministrazione di IDRAGEST può revocare il componente monocratico dell'Organismo di Vigilanza nei casi in cui si verifichino: **i)** rilevanti inadempimenti rispetto al mandato conferito, in ordine ai compiti indicati nel regolamento; **ii)** per ipotesi di violazione degli obblighi di riservatezza; **iii)** quando si manifestino cause di ineleggibilità di cui sopra, anteriori alla nomina a componente dell'OdV; **iv)** quando intervengano le cause di decadenza di seguito specificate.

DECADENZA

Il componente monocratico dell'Organismo di Vigilanza decade dalla carica nel momento in cui venga a trovarsi, successivamente alla sua nomina:

• in una delle situazioni contemplate nell'art. 2399 c.c.;

• condannato con sentenza definitiva (intendendosi per sentenza di condanna anche quella pronunciata ex art. 444 c.p.p.) per uno dei reati indicati ai numeri 1, 2, 3, 4, 5, 6 e 7 delle condizioni di ineleggibilità innanzi indicate;

• nella situazione in cui, dopo la nomina, si accerti aver rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate le sanzioni previste dall'art. 9 del Decreto in relazione a illeciti amministrativi commessi durante la loro carica.

SOSPENSIONE

Costituiscono cause di sospensione dalla funzione di componente monocratico dell'Organismo di Vigilanza:

• la condanna con sentenza non definitiva per uno dei reati dei numeri da 1 a 7 delle condizioni di ineleggibilità innanzi indicate;

• l'applicazione su richiesta delle parti di una delle pene di cui ai numeri da 1 a 7 delle condizioni di ineleggibilità innanzi indicate;

• l'applicazione di una misura cautelare personale;

• l'applicazione provvisoria di una delle misure di prevenzione previste dall'art. 10, comma 3, della legge 31 maggio 1965, n. 575, come sostituito dall'articolo 3 della legge 19 marzo 1990, n. 55 e successive modificazioni.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

ALLEGATO – 6

PROCEDURA WHISTLEBLOWING

per le segnalazioni di illeciti e irregolarità

Sommario

1. PREMESSA 2

2. FINALITÀ E PRINCIPI DELLA PROCEDURA 3

3 CAMPO DI APPLICAZIONE 4

5. RIFERIMENTI NORMATIVI 5

SEGNALAZIONE 5

PERSONA COINVOLTA 5

FACILITATORE 5

5 ORGANISMO DI VIGILANZA (ODV) 6

6 SOGGETTI LEGITTIMATI AD EFFETTUARE LE SEGNALAZIONI 6

7 OGGETTO DELLE SEGNALAZIONI 7

8 CANALI DI SEGNALAZIONE 8

9 CONTENUTO DELLE SEGNALAZIONI 8

9.1 Segnalazioni anonime 9

10. GESTIONE DELLE SEGNALAZIONI 9

10.1 RICEZIONE DELLA SEGNALAZIONE 9
10.2 VERIFICA PRELIMINARE DI AMMISSIBILITÀ 9
10.3 APERTURA DELL'ISTRUTTORIA 10
10.4 DEFINIZIONE DELL'ISTRUTTORIA 10
10.5 ESITI DEL PROCEDIMENTO 10
10.6 RISCONTRO AL SEGNALANTE 11

11. ATTIVITÀ DELL'ORGANISMO DI VIGILANZA 11

12 MISURE DI PROTEZIONE DEL SEGNALANTE 12

12.1 Principi generali 12

12.2 RISERVATEZZA DELL'IDENTITÀ 12
12.3 DIVIETO DI RITORSIONE 12
12.4 SOGGETTI PROTETTI 13

13. TRATTAMENTO DEI DATI PERSONALI 13

14. CONSERVAZIONE DELLA DOCUMENTAZIONE 14

15. COORDINAMENTO CON IL SISTEMA DISCIPLINARE 14

16. MONITORAGGIO E AGGIORNAMENTO DELLA PROCEDURA 14

ALLEGATI: Modulo per la segnalazione di condotte illecite o violazioni del Modello di cui al D.lgs. 231/01

1. PREMESSA

La presente Procedura disciplina il sistema interno di gestione delle segnalazioni di violazioni (whistleblowing) adottato da **IDRAGEST S.r.l.** in attuazione del Decreto Legislativo 10 marzo 2023, n. 24, recante attuazione della Direttiva (UE) 2019/1937 riguardante la protezione delle persone che

segnalano violazioni del diritto dell'Unione, nonché dell'art. 6 del Decreto Legislativo 8 giugno 2001, n. 231.

La Procedura costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo adottato dalla Società e rappresenta uno degli strumenti fondamentali del sistema di controllo interno e di compliance aziendale.

Attraverso il sistema di whistleblowing, la Società promuove una cultura improntata alla legalità, alla trasparenza, all'integrità e alla responsabilità, favorendo l'emersione tempestiva di comportamenti illeciti, irregolarità o violazioni suscettibili di arrecare pregiudizio alla Società, ai suoi stakeholder o all'interesse pubblico.

La Società garantisce che ogni segnalazione sia gestita nel rispetto dei principi di riservatezza, imparzialità, tempestività, proporzionalità, buona fede e tutela del segnalante, assicurando la protezione da qualsiasi forma di ritorsione o discriminazione prevista dalla normativa vigente.

La presente Procedura è coordinata con:

- il Modello di Organizzazione, Gestione e Controllo adottato dalla Società;
- il Codice Etico;
- le Parti Speciali del Modello (PMOG);
- il Sistema Disciplinare;
- il Regolamento dell'Organismo di Vigilanza;
- le procedure aziendali rilevanti ai fini della prevenzione dei reati;
- le policy aziendali in materia di anticorruzione, sicurezza delle informazioni, protezione dei dati personali e utilizzo dell'intelligenza artificiale.

2. FINALITÀ E PRINCIPI DELLA PROCEDURA

La presente Procedura ha lo scopo di disciplinare le modalità di ricezione, gestione, istruttoria e definizione delle segnalazioni riguardanti violazioni di disposizioni normative, del Modello 231, del Codice Etico o delle procedure aziendali.

In particolare, essa è finalizzata a:

1. favorire l'emersione tempestiva di comportamenti illeciti o irregolari;
2. prevenire la commissione dei reati rilevanti ai sensi del D.Lgs. 231/2001;
3. garantire la tutela del segnalante contro qualsiasi forma di ritorsione;
4. assicurare la riservatezza dell'identità delle persone coinvolte;
5. consentire all'Organismo di Vigilanza di svolgere efficacemente le proprie funzioni di vigilanza;
6. rafforzare il sistema di controllo interno e di gestione dei rischi;
7. promuovere una cultura aziendale improntata all'etica, alla legalità e alla trasparenza;
8. assicurare il miglioramento continuo del sistema di compliance aziendale.

L'applicazione della presente Procedura si ispira ai seguenti principi:

- legalità;
- buona fede;
- imparzialità;
- indipendenza;
- riservatezza;
- proporzionalità;
- tempestività;
- tracciabilità;
- tutela della persona;
- protezione dei dati personali;
- divieto di discriminazione e di ritorsione.

3 CAMPO DI APPLICAZIONE

La presente Procedura si applica alle segnalazioni aventi ad oggetto informazioni su violazioni di cui il segnalante sia venuto a conoscenza nell'ambito del proprio contesto lavorativo.

Possono costituire oggetto di segnalazione, a titolo esemplificativo e non esaustivo:

1. condotte rilevanti ai sensi del D.Lgs. 231/2001;
2. violazioni del Modello di Organizzazione, Gestione e Controllo;
3. violazioni del Codice Etico;
4. violazioni delle Parti Speciali del Modello;
5. violazioni delle procedure aziendali;
6. fatti di corruzione, concussione o induzione indebita;
7. frodi;
8. reati tributari;
9. reati societari;
10. riciclaggio, autoriciclaggio e finanziamento del terrorismo;
11. reati ambientali;
12. violazioni in materia di salute e sicurezza sul lavoro;
13. reati informatici e violazioni della sicurezza delle informazioni;
14. utilizzi impropri dell'intelligenza artificiale in violazione delle policy aziendali;
15. conflitti di interesse non dichiarati;
16. falsificazioni documentali;
17. violazioni della normativa sulla protezione dei dati personali;
18. violazioni della normativa europea richiamata dal D.Lgs. 24/2023;
19. comportamenti diretti ad occultare o impedire l'accertamento delle violazioni;
20. tentativi di elusione dei controlli previsti dal Modello.

Non rientrano nell'ambito della presente Procedura:

- contestazioni aventi ad oggetto esclusivamente interessi personali del segnalante;
- rivendicazioni inerenti al rapporto individuale di lavoro;
- reclami di natura commerciale;
- contestazioni disciplinate da specifiche procedure aziendali o normative speciali.

5. RIFERIMENTI NORMATIVI

La presente Procedura è adottata in conformità alla normativa vigente in materia di responsabilità amministrativa degli enti, tutela del segnalante e protezione dei dati personali.

Costituiscono, in particolare, riferimenti normativi:

1. **Direttiva (UE) 2019/1937** del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione;
2. **Decreto Legislativo 10 marzo 2023, n. 24**, recante attuazione della Direttiva (UE) 2019/1937;
3. **Decreto Legislativo 8 giugno 2001, n. 231** e successive modificazioni;
4. **Regolamento (UE) 2016/679 (GDPR)**;
5. **Decreto Legislativo 30 giugno 2003, n. 196**, come modificato dal D.Lgs. 101/2018;
6. **Linee Guida ANAC** adottate ai sensi del D.Lgs. 24/2023;
7. **Linee Guida Confindustria** per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001;
8. ogni ulteriore disposizione normativa nazionale o dell'Unione Europea applicabile alla materia.

La presente Procedura deve essere interpretata e applicata in modo coordinato con il Modello di Organizzazione, Gestione e Controllo, il Codice Etico, il Sistema Disciplinare e gli altri documenti che compongono il sistema di compliance aziendale.

4. DEFINIZIONI

Ai fini della presente Procedura si intende per:

SEGNALAZIONE

La comunicazione, scritta o orale, avente ad oggetto informazioni su violazioni di cui il segnalante sia venuto a conoscenza nell'ambito del proprio contesto lavorativo.

SEGNALANTE (WHISTLEBLOWER)

La persona fisica che effettua una segnalazione o una divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo.

PERSONA COINVOLTA

La persona fisica o giuridica indicata nella segnalazione quale soggetto cui la violazione è attribuita ovvero comunque implicata nei fatti segnalati.

FACILITATORE

La persona fisica che assiste il segnalante nel processo di segnalazione operando nel medesimo contesto lavorativo e la cui assistenza deve rimanere riservata.

5 ORGANISMO DI VIGILANZA (ODV)

L'Organismo di Vigilanza nominato ai sensi dell'art. 6 del D.Lgs. 231/2001, incaricato della gestione del canale interno di segnalazione e dello svolgimento delle attività previste dalla presente Procedura.
MODELLO: Il Modello di Organizzazione, Gestione e Controllo adottato dalla Società ai sensi del D.Lgs. 231/2001.
CODICE ETICO: Il documento che definisce i principi etici ed i valori ai quali devono attenersi tutti i Destinatari.
PARTI SPECIALI: Le Procedure Speciali del Modello (PMOG) che disciplinano i processi sensibili e i protocolli di prevenzione dei reati presupposto.
CANALE INTERNO: Il sistema predisposto dalla Società per consentire la presentazione e la gestione riservata delle segnalazioni.
C**ANALE ESTERNO**: Il canale di segnalazione istituito presso ANAC nei casi previsti dal D.Lgs. 24/2023.
DIVULGAZIONE PUBBLICA: La diffusione al pubblico di informazioni sulle violazioni nei casi tassativamente previsti dall'art. 15 del D.Lgs. 24/2023.
RITORSIONE: Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, conseguente alla segnalazione e idoneo a provocare un danno ingiusto al segnalante.
RISCONTRO: La comunicazione fornita al segnalante riguardante le attività svolte o che si intendono svolgere in relazione alla segnalazione.
FOLLOW-UP: L'insieme delle attività istruttorie svolte dall'Organismo di Vigilanza al fine di verificare la fondatezza della segnalazione e adottare i conseguenti provvedimenti.

6 SOGGETTI LEGITTIMATI AD EFFETTUARE LE SEGNALAZIONI

Possono effettuare segnalazioni attraverso il canale interno tutti i soggetti che abbiano acquisito informazioni sulle violazioni nell'ambito del proprio contesto lavorativo con la Società.
In particolare, possono presentare segnalazioni:

1. componenti del Consiglio di Amministrazione;
2. componenti del Collegio Sindacale, ove nominato;
3. componenti dell'Organismo di Vigilanza;
4. dirigenti;
5. dipendenti;
6. lavoratori subordinati a tempo determinato o indeterminato;
7. lavoratori in somministrazione;
8. collaboratori;

9. consulenti;
10. professionisti incaricati dalla Società;
11. agenti;
12. intermediari;
13. fornitori;
14. appaltatori;
15. subappaltatori;
16. lavoratori autonomi;
17. tirocinanti, retribuiti o non retribuiti;
18. volontari;
19. candidati durante la fase di selezione;
20. ex dipendenti e soggetti il cui rapporto con la Società sia cessato, qualora le informazioni siano state acquisite durante il rapporto;
21. soci e azionisti.

La tutela prevista dalla presente Procedura si applica nei limiti e alle condizioni stabilite dal D.Lgs. 24/2023.

7 OGGETTO DELLE SEGNALAZIONI

Possono costituire oggetto di segnalazione tutte le informazioni riguardanti violazioni di cui il segnalante sia venuto a conoscenza nell'ambito della propria attività lavorativa.

In particolare, possono essere segnalati:

1. fatti costituenti reato;
2. tentativi di commissione di reati;
3. violazioni del D.Lgs. 231/2001;
4. violazioni del Modello di Organizzazione, Gestione e Controllo;
5. violazioni del Codice Etico;
6. inosservanza delle Parti Speciali del Modello;
7. violazioni delle procedure aziendali;
8. condotte corruttive;
9. frodi;
10. irregolarità contabili o amministrative;
11. falsificazioni documentali;
12. reati tributari;
13. reati societari;
14. reati ambientali;
15. reati informatici;

16. violazioni in materia di salute e sicurezza sul lavoro;
17. violazioni della normativa sulla protezione dei dati personali;
18. utilizzi impropri di sistemi di intelligenza artificiale in violazione delle policy aziendali;
19. conflitti di interesse non dichiarati;
20. qualsiasi comportamento idoneo ad eludere il sistema dei controlli previsto dal Modello.

Non costituiscono oggetto della presente Procedura le contestazioni, rivendicazioni o richieste aventi ad oggetto esclusivamente interessi personali del segnalante che attengano al proprio rapporto individuale di lavoro, salvo che tali fatti siano collegati ad una delle violazioni disciplinate dal D.Lgs. 24/2023.

8 CANALI DI SEGNALAZIONE

La Società mette a disposizione dei soggetti legittimati uno o più canali interni che garantiscono la riservatezza dell'identità del segnalante, della persona coinvolta e di ogni altro soggetto menzionato nella segnalazione, nonché del contenuto della stessa e della relativa documentazione.

Le segnalazioni possono essere effettuate:

1. mediante la piattaforma informatica eventualmente adottata dalla Società;
2. mediante invio all'indirizzo di posta elettronica dedicato dell'Organismo di Vigilanza;
3. mediante invio di comunicazione cartacea in busta chiusa recante la dicitura **"Riservata – Organismo di Vigilanza – Whistleblowing"**;
4. mediante incontro diretto richiesto all'Organismo di Vigilanza, che dovrà essere fissato entro un termine ragionevole e comunque nel rispetto delle disposizioni del D.Lgs. 24/2023.

Qualora ricorrano le condizioni previste dagli articoli 6 e seguenti del D.Lgs. 24/2023, il segnalante può altresì ricorrere al canale esterno istituito presso l'Autorità Nazionale Anticorruzione (ANAC) ovvero procedere alla divulgazione pubblica nei casi espressamente previsti dalla legge.

L'Organismo di Vigilanza assicura la gestione del canale interno nel rispetto dei principi di autonomia, imparzialità, indipendenza, riservatezza e tempestività.

9 CONTENUTO DELLE SEGNALAZIONI

Le segnalazioni devono essere formulate in modo chiaro, circostanziato e basate su elementi di fatto precisi e verificabili, al fine di consentire all'Organismo di Vigilanza di effettuare le necessarie verifiche.

Il segnalante è invitato, ove possibile, a indicare:

a) le proprie generalità e un recapito per eventuali comunicazioni, fermo restando quanto previsto per le segnalazioni anonime;

b) una descrizione dettagliata dei fatti oggetto della segnalazione;

c) il luogo e il periodo temporale in cui i fatti si sono verificati;

d) le persone coinvolte o comunque a conoscenza dei fatti;

e) l'eventuale funzione aziendale interessata;

f) la documentazione disponibile a supporto della segnalazione;

g) ogni ulteriore elemento utile all'accertamento dei fatti.

Le segnalazioni devono essere effettuate in buona fede e sulla base di un ragionevole convincimento circa la veridicità delle informazioni comunicate.

Non sono ammesse segnalazioni manifestamente infondate, formulate con dolo o colpa grave ovvero aventi carattere esclusivamente diffamatorio, calunnioso o strumentale.

La presentazione di una segnalazione consapevolmente falsa può comportare l'applicazione delle misure disciplinari previste dal Sistema Disciplinare aziendale, fatti salvi gli ulteriori profili di responsabilità civile e penale.

9.1 Segnalazioni anonime

La Società prende in considerazione anche le segnalazioni anonime qualora risultino adeguatamente circostanziate e contengano elementi concreti, precisi e concordanti tali da consentire l'avvio di un'istruttoria.

Le segnalazioni anonime sono trattate secondo le medesime modalità previste per le altre segnalazioni, fermo restando che le tutele specifiche previste dal D.Lgs. 24/2023 trovano applicazione nei limiti stabiliti dalla normativa vigente.

10. GESTIONE DELLE SEGNALAZIONI

L'Organismo di Vigilanza gestisce il procedimento di ricezione, istruttoria e definizione delle segnalazioni secondo criteri di indipendenza, imparzialità, riservatezza, tempestività e tracciabilità.

L'intero procedimento è documentato e conservato secondo le modalità previste dalla presente Procedura.

10.1 Ricezione della segnalazione

All'atto della ricezione, l'Organismo di Vigilanza:

a) registra la segnalazione in un apposito Registro riservato;

b) attribuisce un codice identificativo univoco;

c) verifica la competenza del canale utilizzato;

d) assicura la separazione della documentazione identificativa dal contenuto della segnalazione, ove necessario.

Entro sette giorni dalla ricezione della segnalazione, l'Organismo di Vigilanza rilascia al segnalante un avviso di ricevimento, salvo che ciò possa compromettere la riservatezza della segnalazione ovvero il segnalante abbia espressamente rinunciato a ricevere comunicazioni.

10.2 Verifica preliminare di ammissibilità

Ricevuta la segnalazione, l'Organismo di Vigilanza effettua una verifica preliminare volta ad accertare:

- la riconducibilità della segnalazione all'ambito di applicazione del D.Lgs. 24/2023 e della presente Procedura;
- la presenza di elementi sufficienti per l'avvio dell'istruttoria;
- l'assenza di profili di manifesta infondatezza.

Qualora la segnalazione risulti incompleta, l'Organismo di Vigilanza può richiedere al segnalante, ove possibile, integrazioni o chiarimenti.

Le segnalazioni manifestamente infondate, generiche, prive di elementi minimi o palesemente estranee all'ambito di applicazione della presente Procedura possono essere archiviate con provvedimento motivato.

10.3 Apertura dell'istruttoria

Qualora la segnalazione sia ritenuta ammissibile, l'Organismo di Vigilanza avvia l'istruttoria, definendo il piano delle attività istruttorie da svolgere.

Nel corso dell'istruttoria l'Organismo di Vigilanza può:

- acquisire documentazione aziendale;
- richiedere informazioni alle funzioni competenti;
- effettuare verifiche documentali;
- svolgere audizioni del segnalante, della persona coinvolta e di altri soggetti informati sui fatti;
- richiedere il supporto di consulenti esterni, nel rispetto degli obblighi di riservatezza;
- effettuare accessi presso le strutture aziendali;
- acquisire ogni ulteriore elemento ritenuto utile.

L'istruttoria è svolta nel rispetto del principio del contraddittorio, ove compatibile con la tutela della riservatezza e con le esigenze investigative.

10.4 Definizione dell'istruttoria

Al termine dell'istruttoria l'Organismo di Vigilanza redige una relazione contenente:

- la descrizione sintetica della segnalazione;
- le attività istruttorie svolte;
- gli elementi acquisiti;
- le valutazioni effettuate;
- le conclusioni raggiunte;
- le eventuali proposte di intervento.

La relazione è conservata agli atti dell'Organismo di Vigilanza.

10.5 Esiti del procedimento

All'esito dell'istruttoria l'Organismo di Vigilanza può:

a) archiviare la segnalazione;

b) formulare raccomandazioni alle funzioni competenti;

c) proporre interventi correttivi;

d) proporre l'avvio del procedimento disciplinare;

e) proporre l'aggiornamento del Modello 231 o delle procedure aziendali;

f) trasmettere gli atti agli organi societari competenti qualora emergano fatti di particolare rilevanza;

g) effettuare le comunicazioni alle Autorità competenti nei casi previsti dalla legge.

10.6 Riscontro al segnalante

Entro tre mesi dalla data dell'avviso di ricevimento, ovvero, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione, l'Organismo di Vigilanza fornisce al segnalante un riscontro sul seguito dato o che intende dare alla segnalazione, nei limiti consentiti dalla normativa e compatibilmente con le esigenze di riservatezza.

11. ATTIVITÀ DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza è il soggetto incaricato della gestione del canale interno di segnalazione e opera con piena autonomia, indipendenza, continuità di azione e imparzialità.

Nell'ambito della presente Procedura l'Organismo di Vigilanza:

a) riceve e gestisce le segnalazioni;

b) garantisce la riservatezza dell'identità del segnalante e delle persone coinvolte;

c) verifica l'ammissibilità delle segnalazioni;

d) svolge le attività istruttorie necessarie all'accertamento dei fatti;

e) richiede informazioni e documentazione alle funzioni aziendali;

f) effettua audizioni e acquisisce dichiarazioni;

g) valuta la fondatezza delle segnalazioni;

h) propone eventuali misure correttive e preventive;

i) segnala agli organi societari competenti le violazioni di particolare rilevanza;

j) propone l'aggiornamento del Modello di Organizzazione, Gestione e Controllo e delle procedure aziendali qualora emergano carenze del sistema di controllo interno;

k) verifica l'attuazione delle misure correttive adottate;

l) conserva la documentazione relativa alle segnalazioni;

m) relaziona periodicamente all'Amministratore Unico sull'attività svolta, nel rispetto degli obblighi di riservatezza e limitatamente agli aspetti rilevanti ai fini della vigilanza sul Modello 231.

L'Organismo di Vigilanza esercita le proprie funzioni senza interferenze da parte di altri organi aziendali e dispone di libero accesso alla documentazione e alle informazioni necessarie allo svolgimento delle proprie attività.

12 MISURE DI PROTEZIONE DEL SEGNALANTE

12.1 Principi generali

La Società promuove una cultura improntata alla legalità, alla trasparenza e all'integrità, riconoscendo il valore delle segnalazioni effettuate in buona fede quale fondamentale strumento di prevenzione dei rischi e di tutela dell'interesse aziendale.

La Società garantisce che il segnalante non subisca alcuna conseguenza pregiudizievole per aver effettuato una segnalazione conforme alla normativa vigente.

Le misure di protezione previste dalla presente Procedura si applicano anche quando la segnalazione, pur rivelatasi infondata all'esito dell'istruttoria, sia stata effettuata sulla base di fondati motivi che inducevano il segnalante a ritenere veritiere le informazioni comunicate.

12.2 Riservatezza dell'identità

L'identità del segnalante, del facilitatore, delle persone coinvolte e di ogni altro soggetto menzionato nella segnalazione è tutelata durante tutte le fasi del procedimento.

Le informazioni idonee a rivelare l'identità del segnalante non possono essere divulgate senza il suo consenso espresso, salvo i casi previsti dalla legge.

L'accesso alla documentazione è consentito esclusivamente ai soggetti autorizzati alla gestione della segnalazione.

12.3 Divieto di ritorsione

È vietata qualsiasi forma di ritorsione, diretta o indiretta, conseguente alla presentazione di una segnalazione effettuata in conformità al D.Lgs. 24/2023.

Costituiscono, a titolo esemplificativo, misure ritorsive:

- licenziamento;
- sospensione;
- demansionamento;
- mancata promozione;
- trasferimento ingiustificato;
- modifica peggiorativa delle mansioni;
- riduzione della retribuzione;
- discriminazione;
- intimidazioni;
- molestie;
- isolamento professionale;
- valutazioni artificiosamente negative;
- mancato rinnovo di contratti per ragioni ritorsive;
- qualsiasi altro comportamento idoneo a determinare un pregiudizio ingiusto.

Ogni comportamento ritorsivo costituisce grave violazione del Modello 231, del Codice Etico e della presente Procedura.

12.4 Soggetti protetti

Le misure di protezione si applicano, nei limiti previsti dal D.Lgs. 24/2023, anche a:

- facilitatori;
- colleghi del segnalante;
- familiari del segnalante;
- persone appartenenti al medesimo contesto lavorativo;
- enti di proprietà del segnalante;
- enti presso i quali il segnalante presta attività lavorativa;
- enti comunque collegati al segnalante.

12.5 Perdita delle tutele

Le misure di protezione non trovano applicazione qualora sia accertato, anche con sentenza di primo grado, che il segnalante abbia agito con dolo o colpa grave, ovvero abbia formulato segnalazioni false, diffamatorie o calunniose.

Restano ferme le responsabilità disciplinari, civili e penali previste dall'ordinamento.

13. TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali effettuato nell'ambito della gestione delle segnalazioni è svolto nel rispetto:

- del Regolamento (UE) 2016/679 (GDPR);
- del D.Lgs. 196/2003;
- del D.Lgs. 24/2023;
- delle disposizioni emanate dall'Autorità Garante per la protezione dei dati personali.

I dati personali sono trattati esclusivamente per finalità connesse alla gestione della segnalazione e sono limitati a quanto necessario per l'istruttoria.

La Società adotta misure tecniche e organizzative idonee a garantire:

- riservatezza;
- integrità;
- disponibilità;
- autenticità;
- tracciabilità degli accessi;
- protezione contro accessi non autorizzati;
- conservazione sicura della documentazione.

L'Organismo di Vigilanza e tutti i soggetti coinvolti nel procedimento sono tenuti al rispetto degli obblighi di riservatezza e di protezione dei dati personali.

14. CONSERVAZIONE DELLA DOCUMENTAZIONE

L'Organismo di Vigilanza assicura la completa tracciabilità dell'intero procedimento di gestione delle segnalazioni.

Tutta la documentazione relativa alle segnalazioni è conservata:

- in formato elettronico su una piattaforma informatica o in un'area digitale riservata, protetta mediante adeguate misure di sicurezza;
- ove necessario, in formato cartaceo presso un archivio riservato accessibile esclusivamente ai soggetti autorizzati.

La documentazione è conservata per il tempo necessario alla gestione della segnalazione e, comunque, **per un periodo non superiore a cinque anni dalla comunicazione dell'esito finale della procedura**, fatti salvi eventuali termini più lunghi previsti dalla legge o necessari per la tutela dei diritti della Società nell'ambito di procedimenti giudiziari o amministrativi.

Al termine del periodo di conservazione la documentazione è eliminata o anonimizzata con modalità idonee a garantirne la definitiva irreversibilità.

15. COORDINAMENTO CON IL SISTEMA DISCIPLINARE

La violazione della presente Procedura costituisce violazione del Modello di Organizzazione, Gestione e Controllo e può determinare l'applicazione delle sanzioni previste dal Sistema Disciplinare aziendale, nel rispetto delle disposizioni di legge e della contrattazione collettiva applicabile.

In particolare, costituiscono violazioni disciplinarmente rilevanti:

a) l'adozione di atti di ritorsione nei confronti del segnalante o degli altri soggetti tutelati;

b) l'ostacolo o il tentativo di ostacolare la presentazione di una segnalazione;

c) la violazione degli obblighi di riservatezza;

d) l'omessa collaborazione con l'Organismo di Vigilanza durante l'istruttoria;

e) la distruzione, alterazione od occultamento della documentazione relativa alle segnalazioni;

f) la presentazione, con dolo o colpa grave, di segnalazioni false, manifestamente infondate, diffamatorie o calunniose;

g) il mancato rispetto delle misure correttive adottate a seguito dell'istruttoria.

L'applicazione delle sanzioni disciplinari non pregiudica l'eventuale esercizio delle azioni civili, penali o amministrative previste dall'ordinamento.

16. MONITORAGGIO E AGGIORNAMENTO DELLA PROCEDURA

La presente Procedura è soggetta a monitoraggio periodico da parte dell'Organismo di Vigilanza, che ne verifica l'effettiva applicazione, l'idoneità e l'efficacia nell'ambito delle attività di vigilanza previste dal Modello 231.

L'Organismo di Vigilanza, ove rilevi criticità applicative, modifiche normative, evoluzioni organizzative o esigenze di miglioramento del sistema di controllo interno, formula all'Amministratore Unico proposte motivate di aggiornamento della Procedura.

Le modifiche alla presente Procedura sono approvate dall'Amministratore Unico, previo esame delle proposte formulate dall'Organismo di Vigilanza, e sono tempestivamente comunicate ai Destinatari mediante gli strumenti informativi adottati dalla Società.

La Società assicura un'adeguata attività di informazione e formazione sul sistema di whistleblowing e sulle modalità di utilizzo dei canali di segnalazione, promuovendo la conoscenza della presente Procedura tra tutti i Destinatari.

ALLEGATO A

MODULO DI SEGNALAZIONE DI VIOLAZIONI (WHISTLEBLOWING)

(D.Lgs. 10 marzo 2023, n. 24 – Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001)

SEZIONE 1 – DATI DEL SEGNALANTE

(La compilazione è facoltativa. Il presente modulo può essere utilizzato anche per segnalazioni anonime.)

Cognome e Nome

Qualifica/Funzione

Società/Funzione Aziendale

Recapito telefonico

Indirizzo e-mail

Altro recapito per comunicazioni

☐ Desidero ricevere comunicazioni sull'esito della segnalazione.

☐ Non desidero ricevere comunicazioni.

SEZIONE 2 – OGGETTO DELLA SEGNALAZIONE

Tipologia della presunta violazione

☐ Violazione del Modello 231

☐ Violazione del Codice Etico

☐ Violazione di una Procedura Aziendale

☐ Corruzione

☐ Frode

☐ Reati tributari

☐ Reati societari

☐ Reati informatici

☐ Reati ambientali

☐ Violazioni in materia di salute e sicurezza

☐ Violazioni in materia di protezione dei dati personali

☐ Utilizzo improprio di sistemi di Intelligenza Artificiale

☐ Conflitto di interessi

☐ Altro

Specificare:

SEZIONE 3 – DESCRIZIONE DEI FATTI

Descrivere i fatti nel modo più dettagliato possibile.

SEZIONE 4 – LUOGO E PERIODO

Luogo in cui si sono verificati i fatti

Periodo

SEZIONE 5 – PERSONE COINVOLTE

Indicare, se conosciuti, i soggetti coinvolti.

Nome Qualifica/Funzione

SEZIONE 6 – EVENTUALI TESTIMONI

Nome Recapito (se noto)

SEZIONE 7 – DOCUMENTAZIONE ALLEGATA

☐ Documenti

☐ E-mail

☐ Fotografie

☐ Registrazioni

☐ File informatici

☐ Altro

Descrizione:

SEZIONE 8 – ALTRE INFORMAZIONI

Indicare qualsiasi ulteriore elemento utile ai fini dell'istruttoria.

SEZIONE 9 – DICHIARAZIONI DEL SEGNALANTE

Il sottoscritto dichiara:

☐ di aver effettuato la presente segnalazione in buona fede;

☐ di ritenere veritiere le informazioni fornite sulla base delle conoscenze acquisite;

☐ di essere consapevole che le segnalazioni effettuate con dolo o colpa grave possono comportare responsabilità disciplinari, civili e penali.

Data _____

Firma (ove apposta)

SPAZIO RISERVATO ALL'ORGANISMO DI VIGILANZA

Protocollo

Codice segnalazione

Data ricezione

Modalità ricezione

Fascicolo n.

Esito verifica preliminare

Data chiusura istruttoria

ALLEGATO B

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

(Articoli 13 e 14 del Regolamento UE 2016/679 - GDPR)

1. Titolare del trattamento

Il Titolare del trattamento è **IDRAGEST S.r.l.**, con sede legale in _____.

Recapiti:

Telefono: _____

PEC: _____

E-mail: _____

---

2. Finalità del trattamento

I dati personali acquisiti attraverso il sistema di whistleblowing sono trattati esclusivamente per:

- ricevere le segnalazioni;
- svolgere le attività istruttorie;
- verificare la fondatezza dei fatti segnalati;
- adottare gli eventuali provvedimenti conseguenti;
- adempiere agli obblighi previsti dal D.Lgs. 24/2023;
- adempiere agli obblighi previsti dal D.Lgs. 231/2001;
- tutelare i diritti della Società e dei soggetti coinvolti.

---

3. Base giuridica del trattamento

Il trattamento è effettuato ai sensi:

- dell'art. 6, par. 1, lett. c) ed e) del GDPR;
- degli articoli 9 e 10 del GDPR, ove applicabili;
- del D.Lgs. 24/2023;
- del D.Lgs. 231/2001.

---

4. Tipologia dei dati trattati

Possono essere trattati:

- dati identificativi;
- dati di contatto;
- dati professionali;
- dati contenuti nella segnalazione;
- eventuali categorie particolari di dati personali e dati relativi a condanne penali o reati, esclusivamente nei limiti consentiti dalla legge.

---

5. Modalità del trattamento

Il trattamento è effettuato mediante strumenti informatici e cartacei nel rispetto dei principi di:

- liceità;
- correttezza;
- trasparenza;
- minimizzazione;
- esattezza;
- limitazione della conservazione;
- integrità;
- riservatezza.

Sono adottate misure tecniche ed organizzative idonee a prevenire accessi non autorizzati, perdita, distruzione o divulgazione indebita dei dati.

---

6. Destinatari dei dati

I dati possono essere conosciuti esclusivamente da:

- Organismo di Vigilanza;
- soggetti specificamente autorizzati dal Titolare;
- consulenti eventualmente incaricati dell'istruttoria;
- Autorità competenti nei casi previsti dalla legge.

L'identità del segnalante è protetta nei limiti stabiliti dal D.Lgs. 24/2023.

---

7. Periodo di conservazione

La documentazione relativa alle segnalazioni è conservata per il tempo necessario alla gestione della procedura e, comunque, **non oltre cinque anni dalla comunicazione dell'esito finale della segnalazione**, fatti salvi i diversi termini previsti dalla legge.

---

8. Natura del conferimento

Il conferimento dei dati è facoltativo.

L'eventuale mancata indicazione di elementi essenziali potrebbe tuttavia impedire lo svolgimento delle attività istruttorie.

Le segnalazioni anonime sono trattate nei limiti previsti dalla Procedura Whistleblowing.

---

9. Diritti dell'interessato

Gli interessati possono esercitare, ove compatibili con la disciplina del D.Lgs. 24/2023, i diritti previsti dagli articoli 15 e seguenti del GDPR.

L'esercizio di tali diritti può subire limitazioni nei casi previsti dalla normativa vigente qualora possa compromettere la tutela della riservatezza del segnalante o il corretto svolgimento delle attività istruttorie.

10. Reclamo all'Autorità Garante

Gli interessati hanno diritto di proporre reclamo al **Garante per la Protezione dei Dati Personali**, secondo le modalità previste dall'art. 77 del Regolamento (UE) 2016/679.

11. Aggiornamento dell'informativa

La presente informativa è soggetta a periodico aggiornamento in funzione dell'evoluzione normativa, organizzativa e delle eventuali modifiche apportate alla Procedura Whistleblowing o al Modello di Organizzazione, Gestione e Controllo della Società.