REVISIONE	DATA DI APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev.1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

SOMMARIO PARTE GENERALE

1 DEFINIZIONI

- ***Attività sensibili***: le attività di BitControl nel cui ambito sussiste il rischio di commissione di Reati;
- ***BitControl o Società***: BitControl S.r.l.
- ***Business Partners***: qualsiasi terza parte che agisce per conto di BitControl (ivi inclusi, fornitori, intermediari, agenti, consulenti, ecc.).
- ***CCNL***: Metalmeccanico Industria, Contratto Collettivo Nazionale di Lavoro applicato da BitControl nei contratti di lavoro;
- ***D. Lgs. 231/2001 o Decreto***: Il Decreto Legislativo 8 giugno 2001, n°231 "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" e successive modifiche e integrazioni.
- ***Delega Interna***: attribuzione interna di poteri connessi alla funzione, che per il loro esercizio non necessitano di procura notarile, riflessi nel sistema di comunicazioni organizzative.
- ***Dipendenti***: i soggetti aventi un rapporto di lavoro subordinato con BitControl S.r.l.
- ***Modello***: il presente Modello di Organizzazione, Gestione e Controllo.
- ***Organismo di Vigilanza***: l'organismo previsto dal presente Modello.
- ***Presidente***: il Presidente del Consiglio di Amministrazione di BitControl S.r.l.
- ***Reati/Reati presupposto***: la fattispecie di reati ai quali si applica la disciplina prevista.

Soggetti Apicali: persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonchè persone che esercitano, anche di fatto, la gestione o il controllo della società.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale – Approvvigionamento
RGAD	Responsabili Gestione Archivi e Documenti
REC	Responsabile Esterno Contabilità
SOC	Soci
RSGQ	Responsabile Sistema di Gestione Qualità
RTEC	Responsabile Tecnico
RFAM	Responsabile Facility Management
RPROG	Responsabile Progettazione
RSCM	Responsabile singola commessa
RATTR	Responsabile Attrezzature e Mezzi

PROG Programmatori

RSUG Responsabile Specialista Ufficio Gare

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL 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 BITCONTROL S.R.L.;
- CODICE DISCIPLINARE DI BITCONTROL S.R.L.
- MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO DI BITCONTROL S.R.L..
- LEGGE 28 GIUGNO 2024, N. 90: RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE E INASPRIMENTO DELLE FATTISPECIE DI REATO INFORMATICO;
- D.LGS. 4 SETTEMBRE 2024, N. 138: RECEPIMENTO DELLA DIRETTIVA (UE) 2022/2555 (NIS2);
- D.LGS. N. 87/2024: REVISIONE DEL SISTEMA SANZIONATORIO TRIBUTARIO;
- D.LGS. 31 DICEMBRE 2024, N. 209: MODIFICHE RILEVANTI AI FINI DEL D.LGS. 231/2001.

LEGGE 23 SETTEMBRE 2025, N. 132: DISCIPLINA NAZIONALE IN MATERIA DI INTELLIGENZA ARTIFICIALE;

- D.LGS. 30 DICEMBRE 2025, N. 211: RECEPIMENTO DELLA DIRETTIVA (UE) 2024/1226;
- D.L. 8 AGOSTO 2025, N. 116, CONVERTITO CON MODIFICAZIONI DALLA LEGGE 3 OTTOBRE 2025, N. 147: INASPRIMENTO SANZIONI PER VIOLAZIONI DEGLI OBBLIGHI DI TRACCIABILITÀ DEI RIFIUTI

DECRETO-LEGGE 31 OTTOBRE 2025, N. 159, CONVERTITO CON MODIFICAZIONI DALLA LEGGE 29 DICEMBRE 2025, N. 198: MODIFICHE ALLA DISCIPLINA IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO RILEVANTI AI FINI DELL'ART. 25-SEPTIES D.LGS. 231/2001.

D.LGS. 21 APRILE 2026, N. 81: ATTUAZIONE DELLA DIRETTIVA (UE) 2024/1203;

D.LGS. 16 APRILE 2026, N. 83: MODIFICHE AL TESTO UNICO SULL'IMMIGRAZIONE;

LEGGE 11 MARZO 2026, N. 34: OBBLIGHI DEL DATORE DI LAVORO IN MATERIA DI LAVORO AGILE;

LEGGE 9 GIUGNO 2025, N. 80 (CONVERSIONE D.L. 11 APRILE 2025, N. 48);

REGOLAMENTO (UE) 2024/1689 (AI ACT): QUADRO NORMATIVO ARMONIZZATO EUROPEO PER L'USO DELL'INTELLIGENZA ARTIFICIALE;

DELIBERA ANAC N. 148 DEL 1° APRILE 2026: OBBLIGO DI DICHIARAZIONE DELL'USO DI SISTEMI DI IA NELLA PREDISPOSIZIONE DI OFFERTE E DOCUMENTI DESTINATI ALLE STAZIONI APPALTANTI; AGGIORNAMENTO BANDO-TIPO N. 1/2023.

- DELIBERA ANAC N. 153 DEL 15 APRILE 2026: BANDO-TIPO N. 2/2026;
- POLICY AZIENDALE SULL'UTILIZZO DEI SISTEMI DI INTELLIGENZA ARTIFICIALE ("POLICY IA").

4 IL BUSINESS ACTIVITY DI BITCONTROL

La BitControl S.r.l. è una società che opera, in Italia e all'estero, offrendo servizi per la realizzazione di sistemi di controllo automatico di impianti tecnologici per il trattamento e sollevamento di acque sia reflue che potabili e per la produzione di energia idroelettrica. BitControl opera, altresì, nel più ampio mercato globale dei servizi avanzati per l'industria 4.0, svolgendo, per tali servizi, un'attività di ricerca industriale ed innovazione.

5 IL DECRETO LEGISLATIVO 231/2001 E LA RESPONSABILITA' AMMINISTRATIVA DEGLI ENTI

In attuazione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300, in data 8 giugno 2001 è stato emanato il Decreto Legislativo n. 231 (di seguito denominato il "Decreto" o anche "D.Lgs. n. 231/2001"), con il quale il Legislatore ha adeguato la normativa interna alle convenzioni internazionali in materia di responsabilità delle persone giuridiche.

In particolare, si tratta della Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, della Convenzione firmata a Bruxelles il 26 maggio 1997 sulla lotta alla corruzione nella quale siano coinvolti funzionari della Comunità Europea o degli Stati membri e della Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

Il Decreto, recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica*", ha introdotto nell'ordinamento giuridico italiano un regime di responsabilità amministrativa a carico degli Enti (ovvero delle persone giuridiche quali Società, associazioni, consorzi, ecc., di seguito denominati "Enti") per reati tassativamente elencati e commessi 1 nel loro interesse o vantaggio: **(i)** da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli Enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli Enti medesimi, ovvero **(ii)** da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati. Il catalogo degli "illeciti presupposto" si è dilatato in tempi recenti con l'introduzione, nell'ambito degli illeciti presupposto, anche di alcune fattispecie di illecito amministrativo.

La responsabilità dell'Ente si aggiunge a quella della persona fisica, che ha commesso materialmente l'illecito, ed è autonoma rispetto ad essa, sussistendo anche quando l'autore del reato non è stato identificato o non è imputabile oppure nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

La previsione della responsabilità amministrativa di cui al Decreto coinvolge, nella repressione degli illeciti ivi espressamente previsti, gli Enti che abbiano tratto vantaggio dalla commissione del reato o nel cui interesse siano stati compiuti i reati - o gli illeciti amministrativi - presupposto di cui al

Decreto medesimo. A carico dell'Ente sono irrogabili sanzioni pecuniarie e interdittive, nonché la confisca, la pubblicazione della sentenza di condanna ed il commissariamento.
Le misure interdittive, che possono comportare per l'Ente conseguenze più gravose rispetto alle sanzioni pecuniarie, consistono nella sospensione o revoca di licenze e concessioni, nel divieto di contrarre con la Pubblica Amministrazione, nell'interdizione dall'esercizio dell'attività, nell'esclusione o revoca di finanziamenti e contributi, nel divieto di pubblicizzare beni e servizi.
La suddetta responsabilità si configura anche in relazione a reati commessi all'estero, purché per la loro repressione non proceda lo Stato del luogo in cui siano stati commessi e l'Ente abbia nel territorio dello Stato italiano la sede principale.

6 LE FATTISPECIE DI REATO

Al momento dell'entrata in vigore, il Decreto 231 disciplinava la responsabilità amministrativa degli enti in relazione ai soli reati contro la Pubblica Amministrazione previsti agli artt. 24 e 25.
Successivi interventi legislativi hanno progressivamente ampliato il catalogo dei reati presupposto della responsabilità amministrativa dell'ente.
Le fattispecie di reato oggi suscettibili di configurare la responsabilità amministrativa della Società, se commessi nel suo interesse o a suo vantaggio dai soggetti sopra menzionati, sono espressamente richiamate dagli artt. 24, 24-bis, 24-ter, 25, 25-bis, 25-bis 1, 25-ter, 25-quater, 25-quater 1, 25-quinquies, 25-sexies e 25- septies, 25-octies, 25-octies 1, 25-octies 2, 25-novies, 25-decies, 25-undecies, 25-duodecies, 25-terdecies, 25-quaterdecies, 25-quinquiesdecies, 25-sexiesdecies, 25-septiesdecies e 25-duodevicies del D.Lgs. 231/01, nonché dalla L. 146/2006 e dal D.Lgs. 58/1998 (TUF).
Inoltre, si precisa che il D.L. n. 20 del 10 Marzo 2023 ha introdotto alcune disposizioni urgenti in materia di flussi di ingresso legale dei lavoratori stranieri e di prevenzione e contrasto all'immigrazione irregolare.
Nello specifico: modifica Art. 12, commi 1 e 3 del D.Lgs n. 286/1998 – Disposizioni contro le immigrazioni clandestine; inserimento Art. 12-bis D.Lgs n. 286/1998 – Morte o lesioni come conseguenza di delitti in materia di immigrazione clandestina; modifiche Art. 22 del D.Lgs n. 286/1998 – Impiego di cittadini di paesi terzi il cui soggiorno è irregolare che hanno interessato le fattispecie di reato dell'Art. 25-duodecies "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare".
Mentre, il D.Lgs. n. 19 del 02.03.23 è intervenuto in merito alla "Attuazione della Direttiva (UE) 2019/2021 del Parlamento Europeo e del Consiglio, del 27 Novembre 2019 che modifica la Direttiva (UE) 2017/1132 per quanto riguarda le trasformazioni, le fusioni e le scissioni transfrontaliere".
In particolare, il citato provvedimento normativo ha apportato modifiche al testo dell'Art. 25-ter al comma 1; ha introdotto nell'art. 25-ter, il nuovo comma s-ter relativo al delitto di false o omesse

dichiarazioni per il rilascio del certificato preliminare; ha inserito, nell'art. 25-ter, il nuovo reato "False o omesse dichiarazioni per il rilascio del certificato preliminare.

Successivamente, sono intervenute altre disposizioni legislative che hanno ampliato ulteriormente il catalogo dei reati presupposto della responsabilità amministrativa dell'ente e precisamente:

1) Il D.L. n. 13/2022 ha introdotto modifiche, di segno ampliativo, alla rubrica e al testo degli artt. 240-bis, 316-bis ("Malversazione di erogazioni pubbliche") e 316-ter ("Indebita percezione di erogazioni pubbliche") del codice penale, al fine di rafforzare il contrasto alle frodi in materia di erogazioni pubbliche, alla luce delle notizie di operazioni illecite che hanno riguardato le agevolazioni fiscali note come "superbonus".

2) Il D.L. 10 agosto 2023 n. 105 coordinato con la Legge di conversione n. 137 del 9 ottobre 2023 (c.d. "Decreto Giustizia) ha apportato delle modifiche relativamente alle Disposizioni urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia personale della magistratura e della pubblica amministrazione, apportando:

a) Modifica testo 24 D.Lgs 231/01 e inserimento al suo interno delle fattispecie dei reati di Turbata libertà degli incanti (Art.353 c.p.) e di Turbata libertà del procedimento di scelta del contraente (Art.353-bis c.p.);

b) Modifica rubrica e testo 25-octies.1 e inserimento al suo interno dalla fattispecie del reato di Trasferimento fraudolento di valori (Art.512-bis c.p.);

c) Modifica 452-bis c.p. (Inquinamento ambientale) e Art 452-quater c.p. (Disastro ambientale), Inserimento Art.255 D.Lgs152/2006 (Abbandono rifiuti) che vanno ad interessare i Reati ambientali Art. 25-undecies D.Lgs 231/01.

d) Delitti in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. 184/2021 e modificata dalla L. n. 137/2023]. In particolare:
- 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];

3) la Legge n. 93 del 14 luglio 2023 ha apportato delle modifiche relativamente alle Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica, mediante:

a) Modifica 171-ter Abusiva duplicazione di opere dell'ingegno destinate al circuito televisivo, cinematografico, etc. e Art.174-ter Legge sulla protezione del diritto d'autore della Legge 633/41 del 22/04/1941 che hanno interessato il reato di Delitti in materia di violazione del diritto d'autore Art. 25-novies D.Lgs 231/01;

4) Legge n.206 del 27 dicembre 2023 "Disposizioni organiche per la valorizzazione, la promozione e la tutela del made in Italy" con modifiche all'Art. 517 c.p. (Vendita di prodotti alimentari con segni mendaci) che ha interessato sia l'Art.25-bis.1 (Delitti contro l'industria ed il commercio) del D.Lgs231/01 sia la fattispecie della Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013) facente parte del Modello 231;

5) Legge n.6 del 22 Gennaio 2024 "Disposizioni sanzionatorie in materia di distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici e modifiche agli articoli 518-duodecies, 635 e 639 del codice penale" che con le modifiche del testo del comma uno dell'Art.518-duodecies (Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici) ha interessato la fattispecie dei reati previsti dall'Art. 25-septesdecies (Delitti contro il patrimonio culturale) D.Lgs 231/01;

6) D.L. n.19 del 2 marzo 2024 coordinato con la Legge di conversione 29 aprile 2024, n. 56 "Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza" che con le modifiche apportate all'Art. 512-bis c.p. (Trasferimento fraudolento di valori) ha interessato la fattispecie dei reati previsti dall'Art. 25-octies.1 (Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori) D.Lgs 231/01;

7) D.Lgs n.87 del 14 giugno 2024 "Revisione del sistema sanzionatorio tributario, ai sensi dell'articolo 20 della legge 9 agosto 2023, n. 111" che con le modifiche apportate all'Art. 10-quater del D.Lgs n.74 del 10 marzo 2000 (Indebita compensazione) ha interessato la fattispecie dei reati previsti dall'Art. 25-quinquiesdecies (Reati tributari);

8) Legge n.90 del 28 giugno 2024 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" che ha introdotto, abrogato e modificato articoli del codice penale facenti parte dell'Art. 24 del D.Lgs 231/01 (Indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche e frode informatica in danno dello stato o di un ente pubblico e frode nelle pubbliche forniture) e dell'Art. 24-bis del D.Lgs. 231/01 (Delitti informatici e trattamento illecito di dati);

Per quest' ultima fattispecie di reato è stato interamente modificato anche il testo con l'inserimento del comma 1-bis e la modifica dei commi esistenti;

9) La Legge Leggi n.112 dell'8 Agosto 2024: Indebita destinazione di denaro o cose mobili, ora "peculato per distrazione";

109 Legge n.114 del 9 Agosto 2024: Modifica rubrica e testo degli artt. sul peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione, etc.); abuso di ufficio; circostanze attenuanti; causa di non punibilità; traffico di influenze illecite;

10) obblighi normativi imposti dalla Direttiva NIS2;

- Legge n. 90 del 2024 nuovi obblighi in materia di sicurezza informatica e gestione delle infrastrutture critiche per le aziende;

11) Decreto Legislativo n.141 del 26 Settembre 2024: disciplina doganale e del sistema sanzionatorio riguardante le imposte indirette;

12) L. n. 166 del 14 novembre 2024: Legge di conversione d.l. salva-infrazioni;

13) L. n. 187 del 9 dicembre 2024: disposizioni urgenti in materia di ingresso in Italia di lavoratori stranieri, di tutela e assistenza alle vittime di caporalato, di gestione dei flussi migratori e di protezione internazionale, nonché dei relativi procedimenti giurisdizionali;

14) Decreto-Legge 11 aprile 2025, n. 48, Disposizioni urgenti in materia di sicurezza pubblica, di tutela del personale in servizio, nonchè di vittime dell'usura e di ordinamento penitenziario;

15) L. n.82 del 6 giugno 2025, ha apportato "Modifiche al codice penale, al codice di procedura penale e altre disposizioni per l'integrazione e l'armonizzazione della disciplina in materia di reati contro gli animali". Inserimento nei reati presupposto D.Lgs 231/01 dell'Art.25-undevicies "Delitti contro gli animali" con relativa modifica testo e introduzione: Art.544- bis c.p. (Uccisione di animali), Art.544-ter c.p. (Maltrattamento di animali), Art. 544-quater c.p. (Spettacoli o manifestazioni vietati), Art.544- quinquies c.p. (Divieto di combattimenti tra animali), introduzione Art. 544-septies (Circostanze aggravanti) e sostituzione e introduzione Art. 638 c.p. (Uccisione o danneggiamento di animali altrui). Modifiche testo Art. 727-bis c.p. (Uccisione, distruzione, cattura, prelievo, detenzione e commercio di esemplari di specie animali o vegetali selvatiche protette) e Art. 733-bis c.p. (Distruzione o deterioramento di habitat all'interno di un sito protetto) facenti parte dell'Art. 25-undecies del D. Lgs 231/01 (Reati ambientali).

16) D.Lgs. n. 81 del 12 giugno 2025 recante "Disposizioni integrative e correttive in materia di adempimenti tributari, concordato preventivo biennale, giustizia tributaria e sanzioni tributarie" Modifiche testo Art. 88 (Circostanze aggravanti del contrabbando) del D. Lgs n.141 del 26 settembre 2024 facente parte dell'Art. 25-sexiesdecies del D.Lgs 231/01 (Contrabbando);

17) L. n.80 del 9 giugno 2025 che ha convertito il D.L. n. 48 dell'11 aprile 2025 contenente "Disposizioni urgenti in materia di sicurezza pubblica, di tutela del personale in servizio, nonchè di vittime dell'usura e di ordinamento penitenziario";

Introduzione testo Art.270-quinquies.3 c.p. (Detenzione di materiale con finalità di terrorismo), ed introduzione e modifica Art.435 c.p. (Fabbricazione o detenzione di materie esplodenti) facenti parte dell'Art. 25-quater del D. Lgs 231/01 (Delitti con finalità di terrorismo o di eversione dell'ordine democratico);

Tale provvedimento ha comportato anche modifiche all'Art. 640 c.p. (Truffa) facente parte dell'Art. 24 del D. Lgs 231/01 (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).

18) Decreto Legge n.116 dell'8 agosto 2025: ha introdotto " Disposizioni urgenti per il contrasto alle attività illecite in materia di rifiuti, per la bonifica dell'area denominata Terra dei fuochi, nonche' in materia di assistenza alla popolazione colpita da eventi calamitosi ";

Modifica nei reati presupposto D.Lgs231/01 dell'Art. 25- undecies "Reati ambientali" con un generale aumento delle quote relative alle sanzioni pecuniarie per tutti i reati.
Modifiche e nuove introduzioni di reati del Codice Penale in materia di bonifiche e contrasto all'inquinamento e al disastro ambientale;
Modificati Art. 452-sexies (Traffico e abbandono di materiale ad alta radioattività), Art. 452-quaterdecies (Attività organizzate per il traffico illecito di rifiuti).
Inseriti Art. 452-septies (Impedimento del controllo) e Art. 452-terdecies (Omessa bonifica);
Modifiche e nuove introduzioni di reati contemplati dal D.Lgs n.152/2006 (Norme in materia ambientale);
Modificati Art.255 (Abbandono di rifiuti non pericolosi), Art.256 (Attività di gestione di rifiuti non autorizzata), Art.258 (Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari), Art.259 (Spedizione illegale di rifiuti).
Inseriti Art.212 comma 19-ter (Albo nazionale gestori ambientali), Art.255-bis (Abbandono di rifiuti non pericolosi in casi particolari), Art.255-ter (Abbandono di rifiuti pericolosi), Art.256-bis (Combustione illecita di rifiuti), Art.259-bis (Aggravante dell'attività di impresa), Art.259-ter (Delitti colposi in materia di rifiuti.
19) Legge n.132 del 23.09.25: Disposizioni e deleghe al Governo in materia di intelligenza artificiale", "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" che ha modificato gli articoli di Codice Civile, della L.633/1941 e del D.Lgs n.58/1998 (TUF), Art. 2637 c.c. (Aggiotaggio) facente parte dell'Art. 25-ter D. Lgs.231/01, Art. 171 L.633/1941 comma 1, lett. a-bis (Messa a disposizione del pubblico di un'opera dell'ingegno protetta o parte di essa) facente parte dell'Art. 25- novies D. Lgs.231/01, Art.185-TUF (Manipolazione del mercato) facente parte dell'Art. 25-sexies D. Lgs.231/01;
20) Legge n.147 del 3 ottobre 2025: "Conversione in legge, con modificazioni, del decreto-legge 8 agosto 2025, n. 116, recante 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". Ha apportato modifica dell'Art. 25-undecies D.Lgs. 231/01 (Reati ambientali);dell'art. 452-quaterdecies c.p. (Attività organizzate per il traffico illecito di rifiuti), e Conversione Art. 452-sexies c.p., (Traffico e abbandono di materiale ad alta radioattività), Art. 452-septies c.p. (Impedimento del controllo) e 452-terdecies c.p. (Omessa bonifica); Modifica di articoli del D.Lgs n.152/2006 (Norme in materia ambientale): Art. 212 (Albo nazionale gestori ambientali), Art. 255 (Abbandono di rifiuti non pericolosi), Art. 256 (Attività di gestione di rifiuti non autorizzata), Art. 258 (Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari) e conversione dell'Art. 255-bis (Abbandono di rifiuti non pericolosi in casi particolari), Art. 255-ter (Abbandono di rifiuti pericolosi), Art. 256- bis (Combustione illecita di rifiuti), Art. 259 (Spedizione illegale di rifiuti), Art. 259-bis (Aggravante dell'attività d'impresa), Art. 259-ter (Delitti colposi in materia di rifiuti).

Estensione per le operazioni sotto copertura, già contemplate dai reati transnazionali, anche ai reati ambientali con la modifica dell'Art.9 comma 1 lettera a) Legge n.146 del 16 marzo 2006.

21) D.Lgs. n. 211 del 30 dicembre 2025 che ha disposto "Attuazione della direttiva 2024/1226/UE del Parlamento europeo e del Consiglio, del 24 aprile 2024, relativa alla definizione dei reati e delle sanzioni per la violazione delle misure restrittive dell'Unione e che modifica la direttiva (UE) 2018/1673";

Inoltre, ha introdotto il nuovo Art. 25-octies.2 del D.Lgs. 231/2001 "Reati in materia di violazione di misure restrittive dell'Unione europea" che inserisce nel catalogo dei reati presupposto le fattispecie previste dal codice penale nel nuovo capo I-bis (del Libro II – Titolo I) i seguenti articoli di Codice Penale:

Art. 275-bis (Violazione delle misure restrittive dell'Unione europea)

Art. 275-ter (Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione europea) Art. 275-quater (Violazione delle condizioni dell'autorizzazione allo svolgimento di attività)

Art. 275-quinques (Violazione colposa di misure restrittive dell'Unione europea)

Art. 275-sexies (Circostanze aggravanti)

Art. 275-septies (Circostanze attenuanti)

Art. 275-octies (Confisca obbligatoria)

Art. 275-novies (Pubblicazione della sentenza di condanna)

Art. 275-decies (Giurisdizione)

Inoltre, ha apportato modifiche all'Art.12 D.Lgs n.286 /1998 "Disposizioni contro le immigrazioni clandestine" con l'aggiunta del comma 1-bis; Modifiche agli Artt. 10 e 13 del D.Lgs 231/01 in merito alla sanzione amministrativa pecuniaria ed alle sanzioni interdittive; Modifica Art. 1 del D.Lgs n. 24/2023 mediante l'introduzione del comma 1-bis ad opera dell'Art. 7 del D.Lgs n. 211/2025, con estensione dell'ambito di applicazione oggettivo della tutela alle persone che segnalano violazioni delle misure restrittive dell'Unione europea.

22) Decreto Legge n. 23 del 24 febbraio 2026 coordinato con Legge di conversione n. 54 del 24 aprile 2026"Disposizioni urgenti in materia di sicurezza pubblica, di attività di indagine dell'autorità giudiziaria in presenza di cause di giustificazione, di funzionalità delle forze di polizia e del Ministero dell'interno, nonché di immigrazione e protezione internazionale " che ha modificato il testo dell'Art. 518-quater (Ricettazione di beni culturali) facente parte dell'Art. 25-septiesdecies del D. Lgs. 231/01 "Delitti contro il patrimonio culturale" e dell'Art. 648 c.p. (Ricettazione) facente parte dell'Art. 25-octies del D. Lgs. 231/01 "Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio"

23) Legge n. 34 dell'11 marzo 2026 "Legge annuale sulle piccole e medie imprese ":Le modifiche hanno interessato l'articolo 3 del D. Lgs. 81/2008 in cui si chiarisce che, anche nel lavoro agile, il datore di lavoro è tenuto a garantire tutti gli obblighi di sicurezza compatibili con tale modalità e l'articolo 55 del D. Lgs. 81/2008 che rafforzando il quadro sanzionatorio ha interessato il perimetro

dei reati presupposto Art. 25-septies del D. Lgs. 231/01 "Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro", con tutte le implicazioni in termini di responsabilità amministrativa dell'ente.

24) Decreto Legislativo n. 83 del 16 aprile 2026 "Attuazione della direttiva (UE) 2024/1233 del Parlamento europeo e del Consiglio, del 24 aprile 2024, relativa a una procedura unica di domanda per il rilascio di un permesso unico che consente ai cittadini di Paesi terzi di soggiornare e lavorare nel territorio di uno Stato membro e a un insieme comune di diritti per i lavoratori di Paesi terzi che soggiornano regolarmente in uno Stato membro"

Modifica Art.22 D. Lgs. n.286/98 (Lavoro subordinato a tempo determinato e indeterminato) facente parte dell'Art.25-duodecies D.Lgs. 231/01 "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare"

25) Decreto Legislativo n. 81 del 21 aprile 2026 "Attuazione della direttiva (UE) 2024/1203 del Parlamento europeo e del Consiglio dell'11 aprile 2024 sulla tutela penale dell'ambiente che sostituisce le direttive 2008/99/CE e 2009/123/CE"**,** che interviene sui Reati ambientali modificando l'Art.25-undecies D.Lgs. n.231/01 e le principali fattispecie del codice penale e del D.Lgs. n.152/2006 (TUA). Sono stati modificati gli Artt. 452-bis c.p. (Inquinamento ambientale) e 256 TUA (Attività di gestione di rifiuti non autorizzata), introdotti gli Artt. 452-bis.1 c.p. (Commercio di prodotti inquinanti), Art. 452-ter c.p. (Morte o lesioni come conseguenza del delitto di inquinamento ambientale e di commercio di prodotti inquinanti), 452-quinquiesdecies c.p. (Nozione di abusività) e 452-sexiesdecies c.p. (Circostanze aggravanti) e abrogato l'Art. 733-bis c.p. (Distruzione o deterioramento di habitat all'interno di un sito protetto).

26) Legge n. 75 del 21 aprile 2026 "Disposizioni sanzionatorie a tutela dei prodotti alimentari italiani". Modifica al testo dell'Art. 25-bis.1 del D. Lgs. 231/2001 "Delitti contro l'industria e il commercio" Abrogazione dell'Art. 516 c.p. e modifica alla rubrica ed al testo dell'Art. 517-quater c.p. (Contraffazione dei segni di indicazione geografica e di denominazione protetta dei prodotti agroalimentari) che hanno interessato sia l'Art. 25-bis.1 del D. Lgs 231/01che l'Art.12 della Legge n.9/2013 (Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato);Introduzione degli articoli 517-sexies c.p. (Frode alimentare), 517-septies c.p. (Commercio di alimenti con segni mendaci) e Art. 517- octies c.p. (Pena accessoria e circostanze aggravanti) che hanno interessato unicamente l'Art. 25-bis.1 del D.Lgs. 231/01;Modifica al testo dell'Art. 9 della Legge n. 146/2006 (Operazioni sotto copertura) che hanno interessato i Reati transnazionali (Legge n.146/2006), l'Art. 25-quater del D. Lgs 231/01 (Delitti con finalità di terrorismo o di eversione dell'ordine democratico), l'Art.25- undecies del D. Lgs 231/01 (Reati ambientali) e l'Art.25-duodevicies del D. Lgs 231/01 (Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici).

27) Decreto Legislativo n. 128 del 25 giugno 2026 "Attuazione della delega di cui all'articolo 19-bis della legge 5 marzo 2024, n. 21, per la riforma organica e il riordino del sistema sanzionatorio e di

tutte le procedure sanzionatorie recati dal testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58" Il provvedimento ha interessato la disciplina degli Abusi di mercato. In particolare, sono stati modificati gli Artt. 187-ter.1 (Sanzioni relative alle violazioni delle disposizioni del Regolamento (UE) n. 596/2014) e 187-quinquies (Responsabilità dell'ente) del D.Lgs. 24 febbraio 1998, n. 58 (TUF), disposizioni richiamate dall'Art. 25-sexies del D.Lgs. n. 231/2001, nell'ambito della riforma organica del sistema sanzionatorio e delle procedure applicabili in materia di abusi di mercato.

28) Decreto Legislativo n. 115 del 12 giugno 2026 "Attuazione della direttiva (UE) 2024/1712 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che modifica la direttiva 2011/36/UE concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime" Il provvedimento ha interessato i "Delitti contro la personalità individuale" con la modifica del testo dell'Art. 25-quinquies del D.Lgs. n. 231/2001 e delle fattispecie di reato ad esso collegate. In particolare, sono stati modificati gli Artt. 600 c.p. (Riduzione o mantenimento in schiavitù), 601 c.p. (Tratta di persone) e 602-ter c.p. (Circostanze aggravanti), nonché introdotto il nuovo Art. 601.1 c.p. (Approfittamento della vittima di riduzione in schiavitù o di tratta).

Un elenco completo dei reati suscettibili di configurare la responsabilità amministrativa della Società è riportato nell'allegato 2 del presente Modello "Reati sanzionati dal Decreto", predisposto ed aggiornato dai componenti degli Organismi di Vigilanza e pubblicato sul sito web www.bitcontrol.it

7 I REATI COMMESSI ALL'ESTERO

In forza dell'art. 4 del Decreto 231, l'ente che abbia la propria sede principale nel territorio dello Stato può essere chiamato a rispondere innanzi al giudice penale italiano anche per l'illecito amministrativo dipendente da reati commessi all'estero nei casi e alle condizioni previsti dagli articoli da 7 a 10 del codice penale e a condizione che nei suoi confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

Pertanto, la Società è perseguibile quando:

1. in Italia ha la sede principale, cioè la sede effettiva ove si svolgono le attività amministrative e di direzione, eventualmente anche diversa da quella in cui si trova l'azienda o la sede legale (enti dotati di personalità giuridica), ovvero il luogo in cui viene svolta l'attività in modo continuativo (enti privi di personalità giuridica);

2. nei confronti dell'ente non stia procedendo lo Stato dove è stato commesso il fatto;

3. la richiesta del Ministro della giustizia è riferita anche all'ente medesimo.

Tali regole riguardano i reati commessi interamente all'estero da soggetti apicali o sottoposti. Per le condotte criminose che siano avvenute anche solo in parte in Italia, si applica il principio di territorialità ex art. 6 del codice penale, in forza del quale "*il reato si considera commesso nel territorio*

dello Stato quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione".

8 CONDIZIONE ESIMENTE DELLA RESPONSABILITA' AMMINISTRATIVA

Elemento costitutivo della responsabilità dell'ente è rappresentato dalla necessità che la condotta illecita ipotizzata sia stata posta in essere "*nell'interesse o a vantaggio della società*" e non "*nell'interesse esclusivo proprio o di terzi*".

Secondo la Relazione Ministeriale di accompagnamento al Decreto, la nozione di "interesse" ha fondamento soggettivo, indicando il fine in vista del quale il soggetto ha commesso il reato, mentre il "vantaggio" fa riferimento all'oggettiva acquisizione di un profitto da parte dell'ente.

Dunque, poiché la responsabilità della persona giuridica viene ricollegata ad un difetto di organizzazione, consistente nel non avere posto in essere un piano di organizzazione, gestione e controllo idoneo a prevenire la commissione dei Reati, il Decreto prevede infatti, agli articoli 6 e 7, una forma di esonero dalla responsabilità per l'ente quando questo dimostri:

- di aver adottato ed efficacemente attuato un "Modello di Organizzazione, Gestione e Controllo" idoneo a prevenire la realizzazione dei Reati;
- di aver istituito un Organismo di Vigilanza all'interno della società, dotato di completa autonomia di iniziativa e controllo, nonchè con specifici obblighi di vigilanza sul funzionamento, sull'osservanza del Modello e sul suo aggiornamento;
- che le persone che hanno commesso il Reato abbiano agito eludendo fraudolentemente il Modello;
- che non vi siano state omissioni o insufficiente vigilanza da parte dell'Organismo di Vigilanza all'uopo preposto.

In particolare, per evitare la responsabilità, la società deve dimostrare l'assenza di colpa organizzativa, cioè che il Reato è stato commesso nonostante essa avesse adottato tutte le misure idonee alla prevenzione dei reati ed alla riduzione del rischio di loro commissione.

Resta inteso che il Modello per avere efficacia esimente deve rispondere alle seguenti esigenze:

1. individuare le aree di rischio di commissione dei Reati attraverso un adeguato processo di valutazione dei rischi;

2. predisporre specifici protocolli al fine di programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

3. individuare modalità di gestione delle risorse finanziarie idonee a prevenire la commissione dei Reati;

4. prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza;

5. configurare un sistema disciplinare sanzionatorio per la violazione delle norme del codice etico, nonché delle procedure previste dal Modello stesso;

6. verifiche periodiche sulla concreta attuazione e osservanza del Modello 231;

7. l'eventuale modifica del Modello 231 quando siano emerse significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività;

9 IL MODELLO ADOTTATO DA BITCONTROL S.R.L.

9.1. Le finalità del Modello nell'ambito del sistema di controllo interno

BITCONTROL S.R.L. (di seguito anche "BITCONTROL" o la "Società") aspira a mantenere e sviluppare il rapporto di fiducia con i suoi stakeholders, cioè con quelle categorie di individui, gruppi o istituzioni i cui interessi sono influenzati dagli effetti diretti e indiretti dell'attività di BITCONTROL. È politica di BITCONTROL diffondere a tutti i livelli una cultura orientata al rispetto delle norme e al controllo interno, come definito nel Codice Etico. L'adozione ed il continuo aggiornamento del presente Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/01 (il "Modello") risponde all'esigenza di indirizzare l'operato della Società in tal senso, per quanto più specificatamente attinente i "processi sensibili" connessi con i reati- presupposto ex D.Lgs. 231/01. Infatti, nonostante gli strumenti aziendali adottati dalla BITCONTROL, quali il Codice Etico e il Codice Disciplinare, risultino di per sé idonei anche a prevenire i reati contemplati dal Decreto, la Società, ha ritenuto opportuno adottare uno specifico "Modello di organizzazione, gestione e controllo ai sensi del Decreto Legislativo 8 giugno 2001, n. 231" (di seguito anche "Modello"), nella convinzione che ciò costituisca, oltre che un valido strumento di sensibilizzazione di tutti coloro che operano per conto della Società affinché tengano comportamenti corretti e lineari, anche un più efficace mezzo di prevenzione contro il rischio di commissione dei reati e degli illeciti amministrativi previsti dalla normativa di riferimento.

IN PARTICOLARE, ATTRAVERSO L'ADOZIONE ED IL COSTANTE AGGIORNAMENTO DEL MODELLO, LA SOCIETÀ SI PROPONE DI PERSEGUIRE LE SEGUENTI PRINCIPALI FINALITÀ:

• determinare, in tutti coloro che operano per conto della Società nell'ambito di "attività sensibili" (ossia di quelle nel cui ambito, per loro natura, possono essere commessi i reati di cui al Decreto), la consapevolezza di poter incorrere, in caso di violazione delle disposizioni impartite in materia, in conseguenze disciplinari e/o contrattuali, oltre che in sanzioni penali e amministrative irrogabili nei loro stessi confronti;

• ribadire che tali forme di comportamento illecito sono fortemente condannate, in quanto le stesse (anche nel caso in cui la Società fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etici ai quali la Società intende attenersi nell'esercizio dell'attività aziendale;

• consentire alla Società, grazie ad un'azione di monitoraggio sulle aree di attività a rischio, di intervenire tempestivamente, al fine di prevenire o contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello.

Dunque, il Modello opera mediante regole generali e protocolli speciali riferiti ai processi sensibili, con particolare riguardo alla tracciabilità documentale, alla segregazione delle funzioni, ai livelli autorizzativi, ai flussi informativi verso l'Organismo di Vigilanza, alla conservazione delle evidenze e alla formalizzazione dei controlli preventivi e successivi.

Tali protocolli trovano concreta attuazione nelle Parti Speciali, le quali disciplinano, per ciascuna area sensibile, i comportamenti vietati, i soggetti responsabili, la documentazione da produrre e conservare, nonché gli eventi che devono essere tempestivamente segnalati all'Organismo di Vigilanza.

A seguito dell'introduzione della Policy IA e della Parte Speciale dedicata alla gestione e utilizzo delle piattaforme di Intelligenza Artificiale si evidenzia che costituiscono presidi trasversali del Modello e si applicano a tutti i processi aziendali nei quali l'IA sia utilizzata per finalità documentali, tecniche, amministrative, contabili, difensive, commerciali o di gara.

È consentito esclusivamente l'utilizzo di strumenti di IA autorizzati; è vietato l'uso di account personali o piattaforme non approvate per finalità aziendali rilevanti ai fini del Modello.

Ogni output generato con l'ausilio dell'IA deve essere sottoposto a supervisione, controllo e validazione umana documentata prima di essere utilizzato, sottoscritto, trasmesso all'esterno, depositato o incorporato in atti, offerte, bilanci, documentazione tecnica, atti giudiziari o comunicazioni ufficiali.

È vietato inserire nei sistemi di IA dati personali non anonimizzati, dati appartenenti a categorie particolari, credenziali, codice sorgente, segreti commerciali, configurazioni di rete o di impianto, documenti contabili o fiscali riservati, atti giudiziari riservati, condizioni transattive, documentazione di gara non pubblica o altre informazioni riservate, salvo quanto espressamente consentito dalle procedure aziendali e previa adozione delle misure di sicurezza prescritte.

L'utilizzo dell'IA deve essere tracciato mediante conservazione delle evidenze essenziali, inclusi utente, strumento utilizzato, finalità, prompt e output rilevanti, controlli svolti, validazione umana ed eventuali anomalie o incidenti

9.2. I Destinatari del Modello

Il Modello e le disposizioni normative ivi richiamate devono essere rispettate dagli esponenti aziendali, da tutto il personale, compresi gli eventuali dipendenti della Società, tutti i dipendenti che operano in regime di distacco, dai collaboratori interni ed esterni che operano in nome e per

conto della Società ed, in particolare, da parte di coloro che si trovino a svolgere tutte le attività sensibili.

La formazione del personale e l'informazione interna sul contenuto del Modello vengono costantemente assicurate con le modalità meglio di seguito precisate.

Al fine di garantire l'efficace ed effettiva prevenzione dei reati, il Modello è destinato anche ai soggetti esterni (intendendosi per tali i fornitori, gli agenti, i consulenti, i professionisti, i lavoratori autonomi o parasubordinati, i partner commerciali o altri soggetti) che, in forza di rapporti contrattuali, prestino la loro collaborazione alla Società per la realizzazione delle sue attività. Nei confronti dei medesimi il rispetto del Modello è garantito mediante l'apposizione di una clausola contrattuale che impegni il contraente ad attenersi ai principi del Modello della Società, del Codice Etico, del Codice Disciplinare ed a segnalare all'Organismo di Vigilanza ed al Responsabile Aziendale eventuali notizie della commissione di illeciti o della violazione del Modello prevedendosi che la violazione degli impegni o, comunque, eventuali condotte illecite poste in essere in occasione o comunque in relazione all'esecuzione degli incarichi costituiranno a tutti gli effetti grave inadempimento ai sensi dell'art. 1455 cod. civ. ai fini della risoluzione del contratto.

9.3 Gli Obiettivi del Modello

L'adozione del Modello ha come obiettivo quello di migliorare il proprio sistema di controllo interno, limitando in maniera significativa il rischio di commissione dei reati previsti dalla normativa in oggetto nel rispetto delle disposizioni di cui al D.Lgs. 231/2001 ed è teso a favorire:

• l'individuazione delle attività svolte dalle singole funzioni aziendali che per la loro particolare tipologia, possono comportare un rischio reato ai sensi del D.Lgs. 231/2001;

• l'analisi dei rischi potenziali con riguardo alle possibili modalità attuative dei reati rispetto al contesto operativo interno ed esterno in cui opera la Società;

• la valutazione del sistema dei controlli preventivi ed il suo adeguamento per garantire che il rischio di commissione dei reati sia ridotto ad un "livello accettabile";

• la definizione di un sistema di regole che fissi le linee di comportamento generali (Codice Etico) e specifiche (modelli, sistemi di gestione, linee guida, policy, procedure organizzative e parti speciali) volte a disciplinare le attività aziendali delle aree "sensibili";

• la definizione di un sistema di poteri autorizzativi e di firma che garantisca una puntuale e trasparente rappresentazione del processo aziendale di formazione e di attuazione delle decisioni;

• la definizione di un sistema di controllo in grado di segnalare tempestivamente l'esistenza e l'insorgere di situazioni di criticità generale e/o particolare;

• la definizione di un sistema di comunicazione e formazione per il personale che consenta la conoscibilità del Codice Etico, dei poteri autorizzativi, delle linee di dipendenza gerarchica, delle

procedure, dei flussi di informazione e di tutto quanto contribuisce a dare trasparenza all'attività aziendale;

• l'attribuzione ad un Organismo di Vigilanza di specifiche competenze in ordine al controllo dell'effettivo funzionamento, dell'adeguatezza e dell'aggiornamento del Modello;

• la definizione di un sistema sanzionatorio relativo alla violazione delle disposizioni del Codice Etico e delle procedure previste o esplicitamente richiamate dal Modello.

9.4. La struttura del Modello

Il presente Modello è costituito da una "Parte Generale", da singole "Parti Speciali" e dagli Allegati di seguito citati.

Le Parti Speciali sono state predisposte per alcune categorie di reato previste ai sensi del D.Lgs. 231/2001, laddove siano stati individuati profili di rischio-reato potenziali applicabili a BITCONTROL, a seguito dell'identificazione dei processi societari "sensibili".

Attualmente le Parti Speciali sono:

• PMOG 01: "Gestione rapporti con la P.A.";

• PMOG 02: "Predisposizione del Bilancio e Prevenzione dei reati tributari";

• PMOG 03: "Gestione rapporti P.A. e ispezioni Pubblica Amministrazione";

• PMOG 04: "Gestione dei contenziosi e degli accordi transattivi e dichiarazioni all'Autorità Giudiziaria";

• PMOG 05: "Scelta partner commerciali e omaggi"

• PMOG 06: "Gestione gare ed esecuzioni appalti"

• PMOG 07: "Ruoli e responsabilità per la comunicazione all'estero";

• PMOG 08: "Gestione per la prevenzione dei reati informatici";

• PMOG 09: "Selezione e Gestione personale";

• PMOG 10: "Adempimenti in materia di salute e sicurezza sui luoghi di lavoro";

• PMOG 11: "Gestione ed utilizzo opere dell'ingegno";

• PMOG 12: "Richiesta finanziamenti, autorizzazioni, permessi e licenze ad Enti ed Istituzioni Pubbliche"

• PMOG 13 "Gestione attività di prevenzione dei reati ambientali"

• PMOG 14 "Gestione attività di prevenzione dei delitti di criminalità organizzata".

• PMOG 15 "Gestione e prevenzione reati corruzione"

• PMOG 16 "Procedura per la gestione e l'utilizzo dei sistemi di Intelligenza Artificiale"

Costituiscono parte integrante del Modello adottato da BITCONTROL i seguenti documenti riportati in allegato:

- Il Codice Etico – Allegato 1;

- La clausola contrattuale – Allegato 2;
- L' elenco dei reati sanzionati dal D.Lgs. 231/01 - Allegato 3;
- La Composizione dell'Organismo di Vigilanza - Allegato 4;
- Compensi, cause di (in)eleggibilità, decadenza e sospensione dei componenti dell'Organismo di Vigilanza - Allegato 5;
- Procedura Whistleblowing – Allegato 6.

9.5. Attuazione, implementazione e aggiornamento del Modello

È cura del Consiglio di Amministrazione provvedere all'efficace attuazione del Modello, mediante valutazione e approvazione delle azioni necessarie per implementarlo o modificarlo. Per l'individuazione di tali azioni, l'Organo amministrativo si avvale dell'Organismo di Vigilanza.
L'efficace e concreta attuazione del Modello è garantita:
• dall'Organismo di Vigilanza, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti sulle attività svolte dalle BITCONTROL nelle aree sensibili;
• dai responsabili preposti all'espletamento delle attività a rischio.
Il Consiglio di Amministrazione deve inoltre garantire, attraverso l'intervento dell'Organismo di Vigilanza, l'aggiornamento delle aree sensibili e del Modello, in relazione alle esigenze di adeguamento che si rendessero necessarie nel futuro, in relazione alla previsione di nuovi reati presupposto e/o alle diverse attività di impresa poste in essere dalla BITCONTROL.
Le modalità operative seguite per l'implementazione e il successivo aggiornamento del Modello sono state le seguenti:

- Mappatura, mediante incontri con il personale interessato, delle aree "sensibili" a rischio 231, identificazione dei profili di rischio potenziale, rilevazione del sistema di controllo interno esistente e Gap Analysis. I risultati di tale attività sono stati formalizzati in un report, che illustrano:

▪ le aree di rischio (anche dette "attività sensibili") rilevate, intendendosi per tali le attività il cui svolgimento potrebbe dare direttamente adito alla commissione di una delle fattispecie di reato contemplate dal Decreto 231;
▪ le attività "strumentali", ovvero le aree in cui, in linea di principio, potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione dei reati in oggetto;
▪ il profilo di rischio potenziale (modalità o occasione di possibile commissione del reato);
▪ i meccanismi di controllo implementati dalla Società, valutandone l'adeguatezza ossia la loro attitudine a prevenire o individuare comportamenti illeciti;

all'upo si precisa che i protocolli aziendali si fondano, in via generale, sui seguenti principi: segregazione delle funzioni; autorizzazione preventiva e documentata; tracciabilità delle attività e delle decisioni; verificabilità ex post; conservazione ordinata delle evidenze; divieto di operazioni

non supportate da adeguata documentazione; obbligo di escalation e segnalazione in caso di anomalia.

Nei processi supportati da strumenti digitali o di IA, tali principi si estendono alla classificazione preventiva dei dati, all'autorizzazione all'uso dello strumento, al logging, alla validazione umana degli output, alla gestione degli incidenti e alla conservazione dei registri e delle evidenze di audit.

- eventuali suggerimenti per integrare o rafforzare i meccanismi di controllo.

- Formalizzazione / aggiornamento del Codice Etico.
- Verifica ed eventuale istituzione e revisione, ove opportuno, del sistema di deleghe e procure.
- Identificazione ed eventuale integrazione del corpo procedurale aziendale con riferimento alle aree a rischio reato e/o strumentali citate.
- Adeguamento del sistema sanzionatorio previgente al fine di renderlo applicabile ed efficace anche con riferimento alle violazioni del Modello.
- Introduzione di specifiche "clausole contrattuali 231" da inserire nelle condizioni generali di contratto, al fine di tutelare BITCONTROL e responsabilizzare il terzo.

10 PROCESSI SENSIBILI DI BITCONTROL

L'art. 6, comma 2, del D. Lgs. n. 231/2001 prevede che il Modello debba "*individuare le attività nel cui ambito possono essere commessi reati*".

Pertanto, è stata eseguita una mappatura dei rischi - così come disposta dal D.Lgs. 231/2001 - partendo dall'analisi delle fattispecie di illeciti presupposto per le quali si applica il Decreto e, con riferimento a ciascuna categoria dei medesimi, sono state identificate le aree aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati da parte della Società.

Quindi, per ciascuna di tali aree sono state individuate le singole attività sensibili e qualificati i principi di controllo e di comportamento cui devono attenersi tutti coloro che vi operano.

Il risk assessment è probabilmente la parte fondamentale del sistema di monitoraggio e controllo del rischio reato all'interno di una organizzazione e da tale esercizio ne derivano conseguenze fondamentali, quali:

– la predisposizione di misure di controllo e protocolli idonei ed adeguati,

– la predisposizione di flussi di comunicazione e reporting;

– la pianificazione di controlli da parte dell'organizzazione dell'OdV.

Il Modello trova poi piena attuazione nella realtà della Società attraverso il collegamento di ciascuna attività "sensibile" con i soggetti e le strutture aziendali coinvolte e con la gestione dinamica dei processi e della relativa normativa di riferimento.

Sarà compito dell'Organismo di Vigilanza svolgere nel continuo la necessaria attività di monitoraggio del livello di adeguatezza del presente Modello, al fine di garantirne una costante funzionalità e conformità alle prescrizioni del Decreto.

Sulla base delle disposizioni di legge attualmente in vigore le aree sensibili identificate dal Modello riguardano in via generale:

• Area Sensibile concernente i reati contro la Pubblica Amministrazione e il reato di corruzione tra privati;

• Area Sensibile concernente i reati societari;

• Area Sensibile concernente i reati tributari;

• Area Sensibile concernente i reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;

• Area Sensibile concernente i reati in tema di salute e sicurezza sul lavoro;

• Area Sensibile concernente i reati informatici e di indebito utilizzo di strumenti di pagamento diversi dai contanti;

• Area Sensibile concernente i reati ambientali;

• Area Sensibile concernente la gestione delle gare e l'esecuzione degli appalti ed il reato di "frode nelle pubbliche forniture";

• Area Sensibile concernente le frodi in materia di erogazione pubblica;

Per ciascuna Area Sensibile, i processi definiti nelle procedure speciali hanno il preciso scopo di garantire ed assicurare il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Per quanto concerne, invece, le seguenti fattispecie di reato, si è ritenuto che non sia ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio di BITCONTROL. Esse sono:

• gli illeciti contro la personalità individuale (art. 25-quinquies). Si è ritenuto esaustivo il richiamo ai principi contenuti sia nel presente Modello sia nel Codice Etico, che prevedono il rispetto dei valori di tutela della personalità individuale, correttezza, moralità, dignità ed uguaglianza nonchè il rispetto delle leggi;

• il reato di "impiego di cittadini di paesi terzi il cui soggiorno è irregolare" (art. 25-duodecies) del Decreto 231. Peraltro, le procedure interne per la selezione ed assunzione del personale contengono presidi di controllo idonei a prevenire tale rischio;

• i reati di "razzismo e xenofobia" (art. 25-terdecies). Non si ritengono applicabili tali tipi di reato nell'interesse o a vantaggio di BITCONTROL. Nondimeno, la Società intende rimarcare la propria attenzione ai principi di tolleranza, rispetto e equità di trattamento nell'ambito aziendale; come sancito dal proprio Codice Etico, BITCONTROL è contraria ad ogni forma di discriminazione, di razzismo, di xenofobia, di intolleranza e di violenza;

• i reati di "frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale", rilevante per le aziende agricole;

• il reato di "contrabbando" (art. 25-sexiesdecies). Non si ritiene applicabile tale fattispecie di reato né per le attività di importazione, in quanto BITCONTROL non è iscritta all'albo degli importatori e

pertanto non gestisce direttamente gli adempimenti doganali, né alle attività di esportazione, gestite tramite contratti di fornitura stipulati con corrieri e a carico dei clienti.

Infine, considerato l'ambito di attività di BITCONTROL e a seguito delle analisi condotte, è stata ragionevolmente esclusa la possibilità di realizzazione delle condotte criminose di falso nummario di cui all'art. 25-bis del Decreto 231, di terrorismo ed eversione dell'ordine democratico ex art. 25-quater del richiamato Decreto 231, di mutilazione degli organi genitali femminili ex art. 25-quater 1, di frode in competizioni sportive ed esercizio abusivo di attività di giuoco o di scommessa ex art. 25-quaterdecies,dei residui 5 reati ex art. 24-ter, 25-duodevicies (riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici), nonché dei reati transnazionali (L. n. 146/2006)

• 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];

Conseguentemente, sulla base dell'analisi di cui sopra, le aree rilevanti individuate, per le quali sono state identificate idonee regole interne (parti speciali del presente Modello, politiche e procedure) ad integrazione del Codice Etico, sono le seguenti:

AREE RILEVANTI	REGOLAMENTAZIONE
Gestione dei rapporti con la Pubblica Amministrazione	Parte speciale 01 Parte Speciale 02 Parte Speciale 03 Parte Speciale 06 Parte Speciale 12 Parte Speciale 14 Parte Speciale 15
Gestione della salute e sicurezza nei luoghi di lavoro	Parte Speciale 10
Gestione delle tematiche ambientali	Parte Speciale 10 Parte speciale 13
Gestione e concessione di omaggi e liberalità	Parte Speciale 01 Parte Speciale 05
Gestione dei finanziamenti (pubblici e non)	Parte Speciale 02 Parte Speciale 12

	Parte Speciale 14
Approvvigionamento di beni e servizi	Parte Speciale 06
Gestione della tesoreria	Parte Speciale 02
Gestione della contabilità, del bilancio e degli adempimenti fiscali (inclusa l'archiviazione dei documenti contabili)	Parte Speciale 02
Gestione delle operazioni societarie ordinarie e straordinarie	Parte Speciale 02 Parte Speciale 03
Gestione dei rapporti e degli adempimenti verso Soci e Organismi di Controllo	Parte Speciale 02 Parte Speciale 03 Parte Speciale 04 Parte Speciale 06
Gestione delle risorse umane	Parte Speciale 09 Parte Speciale 14
Gestione dei rimborsi spese e delle spese di rappresentanza	Parte Speciale 05 Parte Speciale 09
Gestione dei sistemi informativi e delle risorse informatiche aziendali	Parte Speciale 07 Parte Speciale 08 Parte speciale 16

Gestione del contenzioso, dei rapporti con le Autorità Giudiziarie e dei rapporti con i soggetti indagati	Parte Speciale 04
Gestione, mantenimento ed utilizzo delle certificazioni e gestione dei rapporti con enti certificatori	Parte Speciale 10
Definizione e gestione delle politiche fiscali	Parte Speciale 02
Gestione degli asset aziendali	Parte Speciale 05 Parte Speciale 9 Parte Speciale 12

Tra le aree sensibili rilevanti ai fini del Modello rientrano altresì i processi trasversali di utilizzo dei sistemi di Intelligenza Artificiale, di gestione dei flussi informativi e documentali, di screening delle controparti e dei beneficiari effettivi, di tracciabilità delle autorizzazioni e di conservazione delle evidenze di controllo.

La Società affida la propria tenuta contabile anche a professionisti esterni e, per tale ragione, la stessa ha conferito mandato con apposito contratto o lettera di incarico professionale contenente specifiche clausole relative alla necessaria osservanza dei principi di cui al Modello e al Codice Etico. In tale ambito, sarà necessario garantire che l'attività di registrazione dei dati contabili sia svolta in aderenza agli obblighi di legge ed ai principi contabili nazionali e sia finalizzata ad assicurare la correttezza e l'affidabilità delle registrazioni contabili e dei *report* gestionali, nonché il tempestivo adempimento di tutti gli obblighi previsti dalle vigenti disposizioni di legge.

11 POLICY AZIENDALE SULL'UTILIZZO DI INTELLIGENZA ARTIFICIALE

BITCONTROL S.r.l. adotta una specifica **Policy aziendale sull'utilizzo dei sistemi di Intelligenza Artificiale ("Policy IA"), approvata dall'Organo Amministrativo, quale documento parte integrante del presente Modello.

La Policy IA definisce principi, ruoli e misure operative per garantire un impiego dei sistemi di IA conforme al quadro normativo vigente — Regolamento (UE) 2024/1689 (AI Act), D.Lgs. n. 138/2024 (NIS2), GDPR, Legge 23 settembre 2025, n. 132 — nonché alle disposizioni del presente Modello, al Codice Etico e agli obblighi contrattuali nei rapporti con clienti, fornitori e Pubblica Amministrazione.

La Policy IA persegue obiettivi di legalità, tutela dei diritti fondamentali, protezione del patrimonio informativo aziendale e sicurezza informatica, stabilendo in particolare:

- l'elenco degli strumenti di IA autorizzati all'utilizzo e il divieto assoluto di utilizzo di strumenti non approvati o di account personali per finalità aziendali;
- l'obbligo di supervisione umana effettiva e documentata su ogni output generato da sistemi di IA prima del suo utilizzo in documenti ufficiali, offerte, comunicazioni esterne, atti giudiziari, scritture contabili o dichiarazioni destinate alla Pubblica Amministrazione;
- i divieti di inserimento nei sistemi di IA di dati personali non anonimizzati, categorie particolari di dati, credenziali, segreti industriali, documentazione riservata, atti giudiziari e condizioni di accordi transattivi;
- gli obblighi di tracciabilità e conservazione delle evidenze (utente, strumento, finalità, prompt, output, validazione umana), con conservazione per almeno cinque anni nell'archivio digitale aziendale;
- gli obblighi di dichiarazione dell'uso dell'IA nelle gare pubbliche e nei rapporti con la Pubblica Amministrazione, in conformità alla Delibera ANAC n. 148 del 1° aprile 2026 e all'art. 13 della Legge n. 132/2025;
- i flussi informativi verso l'Organismo di Vigilanza in caso di utilizzo rilevante, anomalie negli output, incidenti informatici o violazioni della Policy;
- le responsabilità del Responsabile dell'Intelligenza Artificiale (RIA), del Responsabile Sicurezza Informatica e del DPO nei processi che coinvolgono sistemi di IA;
- il sistema disciplinare applicabile in caso di violazione delle prescrizioni della Policy, in coordinamento con il Codice Disciplinare aziendale.

La Policy IA si applica in modo trasversale a tutti i processi aziendali nei quali l'IA sia utilizzata — ivi inclusi tesoreria, predisposizione del bilancio, rapporti con la PA, gare, contenziosi, comunicazioni esterne, gestione del personale, salute e sicurezza, proprietà intellettuale e prevenzione dei reati ambientali — e costituisce presidio integrativo di tutte le Parti Speciali del Modello. Le relative misure di dettaglio sono disciplinate nella Parte Speciale PMOG 16 e richiamate nelle singole Parti Speciali applicabili ai processi sensibili.

Il rispetto della Policy IA è condizione necessaria ai fini della corretta attuazione del Modello. La sua violazione integra violazione del Modello stesso ed è soggetta alle sanzioni previste dal sistema disciplinare aziendale.

11 L'ORGANISMO DI VIGILANZA

11.1. Identificazione dell'Organismo di Vigilanza. Nomina e revoca

In base alle previsioni del D.Lgs. 231/2001, l'Organismo cui affidare il compito di vigilare sul funzionamento e l'osservanza del Modello, nonchè di curarne l'aggiornamento può essere esterno alla Società (art. 6, comma 1, lett. b del D.Lgs. 231/2001) e deve essere dotato di autonomi poteri di iniziativa e controllo.
L'Organismo di Vigilanza deve possedere caratteristiche di autonomia, indipendenza, professionalità e continuità di azione necessarie per il corretto ed efficiente svolgimento delle funzioni ad esso assegnate. Esso inoltre deve essere dotato di poteri di iniziativa e di controllo sulle attività della Società, senza disporre di poteri gestionali e/o amministrativi.
In virtù delle superiori previsioni, la Società ha affidato l'incarico di Organismo di Vigilanza ad un componente esterno monocratico.
Il componente dell'Organismo è scelto tra soggetti in possesso di un profilo etico e professionale di indiscutibile valore e non deve essere in rapporti di coniugio o parentela con i Consiglieri di Amministrazione.
Non può essere nominato componente dell'Organismo di Vigilanza, e, se nominato decade, l'interdetto, l'inabilitato, il fallito o chi è stato condannato, ancorchè con condanna non definitiva, ad una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità ad esercitare uffici direttivi, ovvero sia stato condannato, anche con sentenza non definitiva o con sentenza di patteggiamento, per aver commesso uno dei reati previsti dal D.Lgs. 231/2001.
Il componente che abbia un rapporto di lavoro subordinato con la Società decade automaticamente dall'incarico, in caso di cessazione di detto rapporto e indipendentemente dalla causa di interruzione dello stesso.

Applicando tali principi alla realtà di BITCONTROL, si è ritenuto opportuno proporre l'affidamento di tale incarico ad un organismo monocratico, il cui componente, che può essere nominato tra soggetti interni o esterni a BITCONTROL deve avere le qualità richieste per effettuare i suoi compiti assicurando professionalità e competenza.
Il componente dell'Organismo di Vigilanza resta in carica un anno, al termine del quale l'eventuale rinnovo deve essere espressamente deliberato dal CDA.
Il Consiglio di Amministrazione può revocare, con delibera, il componente dell'Organismo in ogni momento, ma solo per giusta causa. Per l'approvazione di una delibera di revoca per giusta causa del componente dell'Organismo di Vigilanza, è richiesto il voto favorevole di una maggioranza pari ai 2/3 dei componenti il Consiglio.

Costituiscono giusta causa di revoca del componente esclusivamente:

• l'accertamento di un grave inadempimento da parte dell'Organismo di Vigilanza nello svolgimento dei propri compiti;

• l'omessa comunicazione al Consiglio di Amministrazione di un conflitto di interessi che impedisca il mantenimento del ruolo di componente dell'Organismo stesso;

• la sentenza di condanna della Società, passata in giudicato, ovvero una sentenza di patteggiamento, ove risulti dagli atti l'omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza;

• la violazione degli obblighi di riservatezza in ordine alle notizie e informazioni acquisite nell'esercizio delle funzioni proprie dell'Organismo di Vigilanza;

• per il componente legato alla Società da un rapporto di lavoro subordinato, l'avvio di un procedimento disciplinare per fatti da cui possa derivare la sanzione del licenziamento.

Il componente può recedere in ogni momento dall'incarico con preavviso scritto di almeno 30 giorni, da comunicarsi ai Consiglieri di Amministrazione con raccomandata A.R. o con PEC. Il Consiglio di Amministrazione provvede a nominare il nuovo componente durante la prima riunione del Consiglio stesso, e comunque entro 60 giorni dalla data di cessazione del componente recesso.

L'Organismo di Vigilanza provvede a disciplinare in autonomia le regole per il proprio funzionamento in un apposito Regolamento di Funzionamento, in particolare definendo le modalità operative per l'espletamento delle funzioni ad esso rimesse.

È, pertanto, rimesso al suddetto organo, il compito di svolgere le funzioni di vigilanza e controllo previste dal Modello.

Tenuto conto della peculiarità delle responsabilità e dei contenuti professionali specifici da esse richiesti, nello svolgimento dei compiti di vigilanza e controllo l'Organismo di Vigilanza di BITCONTROL si può avvalere di altre funzioni interne che, di volta in volta, si rendessero a tal fine necessarie.

In conformità ai principi di cui al D.Lgs. 231/2001, mentre non è consentito affidare in outsourcing la funzione dell'Organismo di Vigilanza, è invece possibile solo affidare all'esterno (a soggetti terzi che posseggano le specifiche competenze necessarie per la migliore esecuzione dell'incarico) compiti di natura tecnica, rimanendo la responsabilità complessiva per la vigilanza sul Modello in capo all'Organismo di Vigilanza stesso.

11.2 Funzioni e poteri dell'Organismo di Vigilanza

L'Organismo di Vigilanza è dotato di autonomi poteri di iniziativa e di controllo.

L'Organismo di Vigilanza, nell'esecuzione della sua attività ordinaria, vigila in generale:

• sull'efficienza, efficacia e adeguatezza del Modello nel prevenire e contrastare la commissione degli illeciti per i quali è applicabile il D.Lgs. n. 231/2001, anche di quelli che in futuro dovessero, comunque, comportare una responsabilità amministrativa della persona giuridica;
• sull'osservanza delle prescrizioni contenute nel Modello da parte dei destinatari, rilevando la coerenza e gli eventuali scostamenti dei comportamenti attuati, attraverso l'analisi dei flussi informativi e le segnalazioni alle quali sono tenuti i responsabili delle varie funzioni aziendali;
• sull'aggiornamento del Modello laddove si riscontrino esigenze di adeguamento, formulando proposte agli Organi Societari competenti, laddove si rendano opportune modifiche e/o integrazioni in conseguenza di significative violazioni delle prescrizioni del Modello stesso, di significativi mutamenti dell'assetto organizzativo e procedurale della Società, nonché delle novità legislative intervenute in materia;
• sull'esistenza ed effettività del sistema aziendale di prevenzione e protezione in materia di salute e sicurezza sui luoghi di lavoro;
• sull'attuazione delle attività formative del personale in ordine alla concreata attuazione ed osservanza del Modello;
• sull'adeguatezza delle procedure e dei canali per la segnalazione interna di condotte illecite rilevanti ai fini del D.Lgs. n. 231/2001 o di violazioni del Modello e sulla loro idoneità a garantire la riservatezza dell'identità del segnalante nelle attività di gestione delle segnalazioni;
• sul rispetto del divieto di porre in essere "atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante" per motivi collegati, direttamente o indirettamente, alla segnalazione;
• sull'avvio e sullo svolgimento del procedimento di irrogazione di un'eventuale sanzione disciplinare, a seguito dell'accertata violazione del Modello;
• sul rispetto dei principi e dei valori contenuti nel "Codice Etico di BITCONTROL".

Nel perseguimento della finalità di vigilare sull'effettiva attuazione del Modello, l'Organismo di Vigilanza valuta l'adeguatezza dei presidi delle singole attività aziendali sensibili e indirizza eventuali ulteriori azioni di rafforzamento dei piani di controllo disposti dalla Società.

L'attività di controllo segue appositi protocolli elaborati e costantemente aggiornati in base alle risultanze dell'analisi dei rischi e degli interventi di controllo.

L'analisi dei rischi è il processo continuo di identificazione, classificazione e valutazione preventiva dei rischi (esterni ed interni) e dei controlli interni, da cui discende l'attività di verifica e di controllo posta in essere dall'Organismo di Vigilanza.

L'Organismo di Vigilanza esercita i propri poteri anche mediante esame dei fascicoli digitali, dei registri, dei log, delle checklist, delle autorizzazioni e delle evidenze di validazione umana previsti dalle Parti Speciali, potendo richiedere report periodici, eseguire controlli a campione e formulare proposte di adeguamento dei protocolli interni.

L'OdV monitora in particolare l'effettiva attuazione dei presìdi in materia di uso dell'IA, cybersecurity, rapporti con la P.A., flussi finanziari, salute e sicurezza, ambiente, personale, proprietà intellettuale e gestione del contenzioso.

11.3 Reporting dell'Organismo di Vigilanza verso il vertice aziendale

L'Organismo di Vigilanza ha la responsabilità nei confronti del Consiglio di Amministrazione di:

• comunicare, all'inizio di ciascun esercizio, il piano delle attività che intende svolgere per adempiere ai compiti assegnatigli;

• comunicare periodicamente lo stato di avanzamento del programma definito ed eventuali cambiamenti apportati al piano, motivandoli;

• comunicare immediatamente eventuali problematiche significative scaturite dalle attività nonché dalle eventuali informazioni e segnalazioni ricevute;

• relazionare, almeno annualmente, in merito all'attuazione del Modello, segnalando la necessità di interventi migliorativi e correttivi del medesimo.

L'Organismo di Vigilanza potrà essere invitato a relazionare periodicamente al Consiglio di Amministrazione in merito alle proprie attività.

Nel caso in cui, dagli accertamenti svolti dall'Organismo di Vigilanza, emergessero elementi tali da far risalire la commissione del reato o il tentativo di commissione del reato ad uno o più amministratori, l'Organismo di Vigilanza dovrà riferire tempestivamente al Consiglio di Amministrazione.

L'Organismo di Vigilanza potrà richiedere di essere convocato dai suddetti organi per riferire in merito al funzionamento del Modello o a situazioni specifiche.

L'Organismo di Vigilanza potrà, inoltre, valutando le singole circostanze:

• comunicare i risultati dei propri accertamenti ai responsabili delle funzioni aziendali qualora dalle attività dagli stessi poste in essere scaturissero aspetti suscettibili di miglioramento. In tale fattispecie sarà necessario che l'Organismo di Vigilanza ottenga dai responsabili delle funzioni aziendali un piano delle azioni, con relativa tempistica, per le attività suscettibili di miglioramento nonchè le specifiche delle modifiche operative necessarie per realizzare l'implementazione;

• segnalare al Consiglio di Amministrazione eventuali comportamenti/azioni non in linea con il Modello ed il Codice Etico al fine di:

- acquisire tutti gli elementi per effettuare eventuali comunicazioni alle strutture preposte per la valutazione e l'applicazione delle sanzioni disciplinari;
- dare indicazioni per la rimozione delle carenze onde evitare il ripetersi dell'accadimento.

Tali circostanze dovranno essere comunicate dall'Organismo di Vigilanza al Consiglio di Amministrazione, nel più breve tempo possibile, richiedendo anche il supporto delle funzioni

aziendali che possono collaborare nell'attività di accertamento e nell'individuazione delle azioni idonee ad impedire il ripetersi di tali circostanze.

11.4 Flussi informativi verso l'Organismo di Vigilanza

11.4.1. Flussi informativi da effettuarsi al verificarsi di particolari eventi o in caso di segnalazioni whistleblowing

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte del personale, di tutte funzioni aziendali, degli Organi Societari, dei soggetti esterni (intendendosi per tali fornitori, gli agenti, i consulenti, i professionisti, i lavoratori autonomi o parasubordinati, i partner commerciali, o altri soggetti) in merito ad eventi che potrebbero ingenerare responsabilità di BITCONTROL ai sensi del Decreto.

Devono essere segnalate senza ritardo le notizie circostanziate, fondate su elementi di fatto precisi e concordanti, concernenti:

• la commissione, o la ragionevole convinzione di commissione, degli illeciti per i quali è applicabile il D.Lgs. n. 231/2001;

• le violazioni delle regole di comportamento o procedurali contenute nel presente Modello e nella normativa interna in esso richiamata;

• l'avvio di procedimenti giudiziari a carico dei destinatari del Modello per reati previsti nel D.Lgs. n. 231/01.

Le segnalazioni possono essere effettuate, anche in forma anonima:

• direttamente all'Organismo di Vigilanza, tramite email all'indirizzo: organismodivigilanza@bitcontrol.it.

I soggetti esterni, ivi compresi i soggetti che svolgono attività in outsourcing per conto della Società, possono inoltrare la segnalazione direttamente all'Organismo di Vigilanza con una delle modalità sopra indicate.

Inoltre, ai sensi delle varie fonti normative che prevedono l'adozione di sistemi interni di segnalazione delle violazioni delle disposizioni che regolamentano specifici settori (T.U.B., T.U.F., normativa antiriciclaggio, ecc.), le segnalazioni possono essere effettuate dal personale, necessariamente informa non anonima, secondo le disposizioni dettate dalla procedura Whistleblowing, procedura alla quale si rimanda e che tutti i Destinatari sono tenuti a conoscere ed applicare ove opportuno.

L'Organismo di Vigilanza valuta le segnalazioni ricevute direttamente e adotta gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna.

L'Organismo di Vigilanza prenderà in considerazione le segnalazioni, ancorché anonime, che presentino elementi fattuali.

Si precisa che le Parti Speciali individuano eventi specifici che devono essere comunicati tempestivamente all'Organismo di Vigilanza, fermo restando l'obbligo generale di segnalazione di ogni violazione del Modello, del Codice Etico, della Policy IA o delle procedure aziendali rilevanti.

Costituiscono, a titolo esemplificativo e non esaustivo, flussi informativi obbligatori verso l'OdV: operazioni sospese o anomale in tesoreria; pagamenti di importo significativo; screening con esito critico su controparti, beneficiari effettivi o Paesi; anomalie in gare, finanziamenti, autorizzazioni o rapporti con la P.A.; procedimenti giudiziari, avvisi di garanzia, pressioni indebite o irregolarità documentali; uso non autorizzato dell'IA; incidenti informatici e data breach; anomalie contabili o fiscali; irregolarità nella gestione del personale; infortuni, quasi infortuni, ispezioni e aggiornamenti del DVR; anomalie ambientali, ispezioni e irregolarità nella documentazione ambientale; violazioni relative a software, licenze, banche dati, scraping o deepfake.

Le evidenze documentali e i registri previsti dalle Parti Speciali devono essere messi a disposizione dell'OdV per le attività di verifica, audit, monitoraggio periodico e proposta di aggiornamento del Modello.

BITCONTROL garantisce i segnalanti, qualunque sia il canale utilizzato, da qualsiasi forma di ritorsione, discriminazione o penalizzazione e assicura in ogni caso la massima riservatezza circa la loro identità, fatti salvi gli obblighi di legge. Ai sensi dell'art.6 del Decreto:

• sono vietati atti di ritorsione o discriminatori, diretti o indiretti nei confronti del segnalante, per motivi collegati, direttamente o indirettamente, alla segnalazione. Sono nulli il licenziamento ritorsivo e le misure organizzative aventi effetti negativi diretti o indiretti sulle condizioni di lavoro, se non sia dimostrato che non abbiano natura ritorsiva e che si fondino su ragioni estranee alla segnalazione;

• l'adozione di misure discriminatorie può essere denunciata all'Ispettorato nazionale del lavoro;

• il sistema disciplinare previsto dal Decreto, in attuazione del quale sono stabilite le relative sanzioni, si applica anche a chi:

1) viola gli obblighi di riservatezza sull'identità del segnalante o i divieti di atti discriminatori o ritorsivi;

2) effettua con dolo o colpa grave segnalazioni di fatti che risultino infondati.

Oltre alle segnalazioni relative alle violazioni sopra descritte, devono obbligatoriamente ed immediatamente essere trasmesse all'Organismo:

• le informazioni concernenti i provvedimenti e/o notizie provenienti da organi di Polizia Giudiziaria, o da qualsiasi altra Autorità, fatti comunque salvi gli obblighi di segreto imposti dalla legge, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti per i quali è applicabile il D.Lgs. n. 231/2001, qualora tali indagini coinvolgano la Società o il suo personale od Organi Societari o comunque la responsabilità della Società stessa;

• l'informativa su fatti, atti, eventi e omissioni con profili di grave criticità rispetto all'osservanza delle norme del Decreto, rilevati dalle funzioni di controllo aziendali nell'ambito delle loro attività e le relative azioni correttive.

Ogni Funzione Aziendale, in caso di eventi che potrebbero ingenerare gravi responsabilità della Società ai sensi del D.Lgs. n. 231/2001, informa tempestivamente l'Organismo di Vigilanza e predispone specifica relazione che

descriva nel dettaglio l'evento stesso, il rischio, il personale coinvolto, i provvedimenti disciplinari in corso e le soluzioni per limitare il ripetersi dell'evento.

BITCONTROL richiede che le segnalazioni vengano fatte in forma nominativa, impegnandosi a mantenere riservata l'identità del Segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti di BITCONTROL o delle persone accusate erroneamente e/o in mala fede. BITCONTROL si impegna a tutelare il Segnalante in buona fede contro qualsiasi forma di ritorsione, discriminazione o penalizzazione per motivi collegati, direttamente o indirettamente, alla Segnalazione. Atti di tale natura, diretti o indiretti, nei confronti del segnalante, sono vietati e potranno essere sanzionati secondo quanto previsto dal presente Modello.

Eventuali segnalazioni ricevute in forma anonima non saranno prese in considerazione.

Il Segnalante è responsabile della segnalazione fatta, che dovrà avere i requisiti di cui sopra (e quindi essere circostanziata e fondata su elementi di fatto precisi e concordanti). Sono vietate forme di "abuso" del whistleblowing, con segnalazioni manifestamente opportunistiche e/o effettuate con il solo scopo di danneggiare il Segnalato, e ogni altra ipotesi di utilizzo improprio o strumentale del meccanismo di segnalazione. Atti di tale natura nei confronti del soggetto segnalato sono vietati e potranno essere sanzionati secondo quanto previsto dal presente Modello.

L'Organismo di Vigilanza agirà secondo i principi di confidenzialità, tempestività di investigazione e azione, imparzialità e collegialità.

L'Organismo di Vigilanza dovrà valutare le informazioni ricevute e disporre le necessarie verifiche finalizzate ad accertare se, sulla base degli elementi in proprio possesso, è effettivamente avvenuta una violazione del Modello. Nel caso in cui l'Organismo riscontri una violazione del Modello informerà dell'esito dei suoi accertamenti gli Organi Aziendali competenti, che sono tenuti a dare corso al procedimento di contestazione degli addebiti secondo le procedure definite.

Ogni informazione, segnalazione, report ricevuti dall'Organismo di Vigilanza sono conservati in un apposito archivio (informatico o cartaceo). L'accesso all'archivio è consentito al solo componente dell'Organismo. L'accesso da parte di soggetti diversi dal componente dell'Organismo deve essere preventivamente autorizzato da quest'ultimo.

La Società assicura la conservazione ordinata e accessibile della documentazione rilevante ai fini del Modello, inclusi fascicoli digitali, autorizzazioni, verbali, registri, checklist, evidenze di screening, documentazione di validazione e log dei sistemi utilizzati, secondo quanto previsto dalle Parti Speciali applicabili.

Nei processi che comportano utilizzo dell'IA o di sistemi informatici, la conservazione deve consentire la ricostruzione dell'iter decisionale, del soggetto utilizzatore, dei controlli effettuati e della validazione finale umana.

Come specificato dalla procedura "whistleblowing", resta valida la possibilità di effettuare segnalazioni in modo verbale o in forma scritta (es. e-mail) direttamente al proprio superiore gerarchico / referente aziendale, nonchè agli organi / alle Funzioni aziendali preposte a specifiche funzioni di controllo.
Dunque, le segnalazioni sono gestite secondo la Procedura Whistleblowing aziendale, che costituisce parte integrante del Modello. Sono tutelate la riservatezza del segnalante, del segnalato e dei soggetti comunque menzionati nella segnalazione, nonché il divieto di ritorsione. Le segnalazioni anonime, ove sufficientemente circostanziate e supportate da elementi di fatto specifici, possono essere valutate secondo i criteri previsti dalla procedura aziendale applicabile.
Le Parti Speciali richiedono l'utilizzo del canale whistleblowing anche per segnalare tentativi corruttivi, violazioni della Policy IA, pressioni indebite, anomalie documentali, incidenti cyber, violazioni ambientali, irregolarità nella gestione del personale e ogni altra condotta rilevante ai fini del D.Lgs. 231/2001.

11.5. Verifiche periodiche dell'Organismo di Vigilanza

Oltre all'attività di vigilanza che l'Organismo svolge continuamente sull'effettivo funzionamento e sulla corretta osservanza del Modello (e che si traduce nella verifica della coerenza tra i comportamenti concreti dei destinatari ed il Modello stesso) lo stesso periodicamente effettua specifiche verifiche sulla reale capacità del Modello alla prevenzione dei reati (eventualmente, qualora lo ritenga opportuno, coadiuvandosi con soggetti terzi).
Tale attività si può concretizzare in una verifica a campione dei principali atti societari e dei contratti di maggior rilevanza conclusi da BITCONTROL in relazione ai processi sensibili e alla conformità degli stessi alle regole di cui al presente Modello.
Inoltre, viene svolta una review di tutte le informazioni e segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'Organismo di Vigilanza, degli eventi considerati rischiosi e della consapevolezza degli stakeholders rispetto alla problematica della responsabilità penale dell'impresa con eventuali verifiche a campione.
Le verifiche sono condotte dall'Organismo di Vigilanza che si avvale del supporto di altre funzioni interne che, di volta in volta, si rendano a tal fine necessarie.
Le verifiche e il loro esito sono oggetto di report semestrale al Consiglio di Amministrazione.
In particolare, in caso di esito negativo, l'Organismo di Vigilanza esporrà, nel piano relativo all'anno, i miglioramenti da attuare.
Le verifiche sull'adeguatezza del Modello svolte dall'Organismo di Vigilanza sono concentrate sull'efficacia applicativa dello stesso all'interno degli assetti societari.

E' possibile compiere la verifica svolgendo attività di audit, svolta a campione, dei principali atti societari e dei contratti di maggior rilevanza conclusi dall'ente in relazione ai «processi sensibili» e alla conformità degli stessi a quanto prescritto dal Modello.

Con riferimento alle informazioni e segnalazioni ricevute nel corso dell'anno, alle azioni intraprese dall'Organismo di Vigilanza e dagli altri soggetti interessati, sugli eventi considerati rischiosi verrà predisposto un report semestrale indirizzato al Consiglio di Amministrazione, come riportato al precedente punto.

L'Organismo di Vigilanza stila con regolare cadenza un programma di vigilanza attraverso il quale pianifica la propria attività di verifica e controllo.

Il programma contiene un calendario delle attività da svolgere nel corso dell'anno prevedendo, altresì, la possibilità di effettuare verifiche e controlli non programmati.

Nello svolgimento della propria attività, l'Organismo di Vigilanza può avvalersi del supporto di funzioni e strutture interne alla Società e/o in outsourcing con specifiche competenze nei settori aziendali di volta in volta sottoposti a controllo.

All'Organismo di Vigilanza sono riconosciuti, nel corso delle verifiche ed ispezioni, i più ampi poteri al fine di svolgere efficacemente i compiti affidatigli come:

• Verificare e segnalare le necessità di modifica del Modello, quando intervengono mutamenti nell'organizzazione aziendale o nel modello di business che rendano il Modello non più aggiornato o che comportino nuovi potenziali “rischi 231”.

Il Consiglio di Amministrazione ha la responsabilità di disporre l'aggiornamento del Modello e l’adeguamento in relazione al mutamento degli assetti organizzativi, dei processi operativi nonchè alle risultanze dei controlli e di tale aggiornamento conferisce apposito mandato all’Organismo Di Vigilanza.

È inoltre compito dell'Organismo di Vigilanza:

• Verificare se è stata effettuata un’adeguata formazione e informazione del personale sugli aspetti rilevanti ai fini dell'osservanza della legge nello svolgimento dell'attività dell'organizzazione.

La comunicazione al personale e la sua formazione sono due importanti requisiti del Modello ai fini del suo buon funzionamento. Con riferimento alla comunicazione, essa deve riguardare ovviamente il Codice Etico ma anche gli altri strumenti quali i poteri autorizzativi, le linee di dipendenza gerarchica, le procedure, i flussi di informazione e tutto quanto contribuisca a dare trasparenza nell'operare quotidiano. La comunicazione deve essere: capillare, efficace, autorevole (cioè emessa da un livello adeguato) chiara e dettagliata, periodicamente ripetuta. Accanto alla comunicazione, deve essere sviluppato un adeguato programma di formazione rivolto al personale delle aree a rischio, appropriatamente tarato in funzione dei livelli dei destinatari, che illustri le ragioni di opportunità, oltre che giuridiche, che ispirano le regole e la loro portata concreta.

• Verificare se sono state adottate misure materiali, organizzative e protocolli di comportamento atti a garantire lo svolgimento dell'attività nel rispetto della legge ed a scoprire ed eliminare tempestivamente eventuali situazioni irregolari.
• Verificare l'attuazione di un idoneo sistema di controllo sull' attuazione del Modello organizzativo e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.
Infatti, il sistema delineato non può, per operare efficacemente, ridursi ad un'attività una tantum, bensì deve tradursi in un processo continuo e costante (o comunque svolto con una periodicità adeguata), da reiterare con particolare attenzione nei momenti di cambiamento aziendale (ampliamento di attività, acquisizioni, riorganizzazioni, ecc.).

12 LA FORMAZIONE DELLE RISORSE E LA DIFFUSIONE DEL MODELLO

12.1. Formazione ed informazione dei Dipendenti

Ai fini dell'attuazione del presente Modello, è obiettivo di BITCONTROL garantire una corretta conoscenza, sia alle risorse già presenti in azienda sia a quelle da inserire, delle regole di condotta ivi contenute, con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nei processi sensibili.

Il sistema di informazione e formazione è supervisionato ed integrato dall'Organismo di Vigilanza, nella sua prerogativa di promuovere la conoscenza e la diffusione del Modello stesso, in collaborazione con il Responsabile delle Risorse Umane e con i responsabili delle altre funzioni di volta in volta coinvolte nella applicazione del Modello.

LA COMUNICAZIONE INIZIALE

Gli eventuali neo assunti di BITCONTROL ricevono, all'atto dell'assunzione, unitamente alla prevista documentazione, copia del Modello, del Codice Etico, del Codice Disciplinare, dell'Informativa Privacy.

La sottoscrizione di un'apposita dichiarazione attesta la consegna dei documenti, l'integrale conoscenza dei medesimi e l'impegno ad osservare le relative prescrizioni.

Sull'intranet aziendale sono pubblicate e rese disponibili per la consultazione, oltre alle varie comunicazioni interne, il Modello e le normative collegate.

I documenti pubblicati sono costantemente aggiornati in relazione alle modifiche che via via intervengono nell'ambito della normativa di legge e del Modello, i cui periodici aggiornamenti sono comunicati dal vertice aziendale a tutto il personale dipendente e la suddetta pubblicazione, unitamente, alle circolari interne, garantiscono a tutto il personale una informazione completa e tempestiva.

LA FORMAZIONE

Le iniziative formative hanno l'obiettivo di far conoscere il Decreto, il Modello e, in particolare, di sostenere adeguatamente coloro che sono coinvolti nelle attività "sensibili".

Per garantirne l'efficacia esse sono erogate tenendo conto delle molteplici variabili presenti nel contesto di riferimento; in particolare:

• i target (i destinatari degli interventi, il loro livello e ruolo organizzativo);

• i contenuti (gli argomenti attinenti al ruolo delle persone);

• gli strumenti di erogazione (formazione live, digitali);

• i tempi di erogazione e di realizzazione (la preparazione e la durata degli interventi);

• l'impegno richiesto al target (i tempi di fruizione);

• le azioni necessarie per il corretto sostegno dell'intervento (promozione, supporto dei capi).

Le attività prevedono:

• una formazione digitale destinata a tutto il personale;

• specifiche iniziative formative per le persone che lavorano nelle strutture in cui maggiore è il rischio di comportamenti illeciti;

• altri strumenti formativi di approfondimento da impiegare attraverso la piattaforma della formazione.

La piattaforma consente a ciascun partecipante di consultare i contenuti formativi di base sul Decreto, oltre ad eventuali aggiornamenti legislativi, e verificare il proprio livello di apprendimento attraverso un test finale.

La formazione specifica interviene laddove necessario, a completamento della fruizione dei contenuti digitali destinati a tutto il personale e ha l'obiettivo di diffondere la conoscenza dei reati, delle fattispecie configurabili, dei presidi specifici relativi alle aree di competenza degli operatori, e di richiamare alla corretta applicazione del Modello di organizzazione, gestione e controllo. La metodologia didattica è fortemente interattiva e si avvale di case studies.

I contenuti formativi digitali e gli interventi specifici sono aggiornati in relazione all'evoluzione della normativa esterna e del Modello. Se intervengono modifiche rilevanti (ad es. estensione della responsabilità amministrativa dell'ente a nuove tipologie di reati), si procede ad una coerente integrazione dei contenuti medesimi, assicurandone altresì la fruizione.

La fruizione delle varie iniziative di formazione è obbligatoria per tutto il personale cui le iniziative stesse sono dirette ed è monitorata a cura della competente funzione Personale, nonché dei responsabili ai vari livelli che devono farsi garanti, in particolare, della fruizione delle iniziative di formazione "a distanza" da parte dei loro collaboratori.

La funzione Formazione ha cura di raccogliere i dati relativi alla partecipazione ai vari programmi edi archiviarli, rendendoli disponibili alle strutture interessate.

L'Organismo di Vigilanza verifica, lo stato di attuazione delle attività formative e ha facoltà di chiedere controlli periodici sul livello di conoscenza, da parte del personale, del Decreto, del Modello e delle sue implicazioni operative.

Sarà cura dell'Organismo di Vigilanza – d'intesa ed in coordinamento con il Responsabile delle Risorse Umane ed in collaborazione con i Responsabili delle Funzioni/Direzioni di volta in volta coinvolte – prevedere il contenuto dei corsi, la loro diversificazione, le modalità di erogazione, la loro reiterazione, i controlli sull'obbligatorietà della partecipazione e le misure da adottare nei confronti di quanti non frequentino senza giustificato motivo.
Si precisa che la formazione deve essere differenziata in funzione del ruolo, delle deleghe, del livello di rischio e della Parte Speciale applicabile, e deve comprendere anche i contenuti relativi al corretto utilizzo dell'Intelligenza Artificiale, alla tracciabilità documentale, ai flussi verso l'OdV e alle regole specifiche dei processi sensibili di competenza.
Ai nuovi assunti e ai collaboratori coinvolti nei processi sensibili devono essere consegnati, secondo i casi applicabili, il Modello, il Codice Etico, il Codice Disciplinare, la Procedura Whistleblowing, la Policy IA e le Parti Speciali di riferimento, con raccolta della relativa evidenza di ricezione e presa visione.

11.2. Informazione ai collaboratori ed ai partner

I consulenti ed i partner devono essere informati del contenuto del Modello e del Codice Etico e dell'esigenza di BITCONTROL che il loro comportamento sia conforme ai disposti del D.Lgs. 231/2001.
Al fine di formalizzare l'impegno al rispetto dei principi del Modello e del Codice Etico da parte di terzi aventi rapporti contrattuali con la Società, è previsto l'inserimento nel contratto di riferimento di un'apposita clausola nelle condizioni generali di contratto.

13 SISTEMA DISCIPLINARE

13.1. Funzione del sistema disciplinare

La predisposizione di un efficace sistema sanzionatorio costituisce, ai sensi dell'art. 6 secondo comma lettera e) del D.Lgs. 231/2001, un requisito essenziale del Modello ai fini dell'esimente rispetto alla responsabilità della Società. Medesimo requisito è richiamato anche dall'art. 30, terzo comma, del Testo Unico sulla Sicurezza, con specifico riferimento agli aspetti inerenti la sicurezza e la tutela della salute dei lavoratori.
Il Modello di Organizzazione, di gestione e di controllo adottato da BITCONTROL, prevede un adeguato sistema disciplinare applicabile in caso di violazioni del Modello stesso. Per "violazione del Modello" s'intende una condotta non conforme - per negligenza, dolo o colpa - alle regole generali di comportamento previste dal Codice Etico e alle norme procedurali previste o esplicitamente richiamate dal Modello, per quanto applicabili al soggetto coinvolto, in base al ruolo, ai poteri e alle funzioni che ricopre nell'ambito della Società o per conto di essa.
La previsione di un sistema sanzionatorio rende efficiente l'azione dell'Organismo di Vigilanza e ha lo scopo di garantire l'effettiva attuazione del Modello.

L'applicazione del sistema disciplinare e delle relative sanzioni è indipendente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D.Lgs. 231/2001.

Il sistema disciplinare si rivolge a tutti i dipendenti della Società, a tutte le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, a tutte le persone che esercitano, anche di fatto, la gestione e il controllo della Società nonchè alle persone che sono sottoposte alla loro vigilanza ed alla loro direzione, così come disposto dall'art 5 del D.Lgs. 231/2001.

Con riferimento ai lavoratori dipendenti, tale codice disciplinare deve integrare i presupposti di idoneità ai sensi del Decreto 231 con i profili giuslavoristici definiti dalla corrente normativa codicistica, dalla legislazione speciale e dalla contrattazione collettiva nazionale e aziendale e, precisamente ai provvedimenti disciplinari di cui all'art. 8 del CCNL Metalmeccanica Industria.

In considerazione di quanto sopra, il codice disciplinare applicabile ai soggetti che collaborano con la Società a titolo di lavoratori dipendenti - dirigenti e non dirigenti - amministratori, collaboratori, consulenti e terzi che operino per conto o nell'ambito della medesima Società si uniformerà alle linee guida illustrate nei paragrafi seguenti.

Sulla base delle segnalazioni pervenute all'Organismo di Vigilanza, l'attivazione, lo svolgimento e la definizione del procedimento disciplinare nei confronti dei dipendenti sono affidati, nell'ambito delle competenze alla stessa attribuite, alle funzioni Risorse Umane.

Gli interventi sanzionatori nei confronti dei soggetti esterni sono affidati alla funzione che gestisce il contratto o presso cui opera il lavoratore autonomo ovvero il fornitore.

Il tipo e l'entità di ciascuna delle sanzioni stabilite, saranno applicate, ai sensi della normativa richiamata, tenuto conto del grado di imprudenza, imperizia, negligenza, colpa o dell'intenzionalità del comportamento relativo all'azione/omissione, tenuto altresì conto di eventuale recidiva, nonché dell'attività lavorativa svolta dall'interessato e della relativa posizione funzionale, unitamente a tutte le altre particolari circostanze che possono aver caratterizzato il fatto.

Quanto precede verrà adottato indipendentemente dall'avvio e/o svolgimento e definizione dell'eventuale azione penale, in quanto i principi e le regole di condotta imposte dal Modello sono assunte da BITCONTROL in piena autonomia ed indipendentemente dai possibili reati che eventuali condotte possano determinare e che l'autorità giudiziaria ha il compito di accertare.

Pertanto, in applicazione dei suddetti criteri, viene stabilito il seguente sistema sanzionatorio.

La verifica dell'adeguatezza del sistema sanzionatorio, il costante monitoraggio dei procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché degli interventi nei confronti dei soggetti esterni sono affidati all'Organismo di vigilanza, il quale riceve dalla funzione Risorse Umane un'informativa con cadenza almeno annuale sui provvedimenti disciplinari comminati al personale dipendente nel periodo di riferimento.

Costituisce violazione del Modello anche l'inosservanza delle prescrizioni contenute nelle Parti Speciali e nei documenti attuativi richiamati dalle medesime, incluse la Procedura Whistleblowing, il Codice Etico e la Policy IA.

Sono in particolare rilevanti, ai fini disciplinari, l'uso non autorizzato di sistemi di IA, l'omessa validazione umana degli output, l'alterazione o mancata conservazione dei log e delle evidenze, la violazione dei protocolli di autorizzazione, la falsificazione documentale, l'omessa segnalazione all'OdV di eventi rilevanti, la violazione degli obblighi di riservatezza, sicurezza informatica, salute e sicurezza, ambiente, correttezza contabile, fiscale e nei rapporti con la Pubblica Amministrazione.

Si riporta di seguito il sistema sanzionatorio previsto per i dipendenti (aree professionali, quadri direttivi e dirigenti) con contratto di lavoro regolato dal CCNL Metalmeccanica Industria.

13.2 Sanzioni disciplinari

13.2.1 Sanzioni per i lavoratori dipendenti

Le condotte dei lavoratori dipendenti non conformi alle norme comportamentali previste dal Modello costituiscono illeciti disciplinari e, in quanto tali, devono essere sanzionate.

Il lavoratore deve rispettare le disposizioni normative impartite dalla Società, al fine di evitare le sanzioni previste dal vigente Contratto Collettivo Nazionale, divulgate ai sensi e nei modi previsti dall'art. 7 della legge 20 maggio 1970, n. 300 (c.d. "Statuto dei Lavoratori").

La tipologia e l'entità del provvedimento disciplinare saranno individuate tenendo conto della gravità o recidività della mancanza o del grado di colpa e valutando in particolare:

- l'intenzionalità del comportamento o il grado di negligenza, imprudenza o imperizia, anche alla luce della prevedibilità dell'evento;
- il comportamento complessivo del lavoratore, verificando l'esistenza di eventuali altri simili precedenti disciplinari;
- le mansioni assegnate al lavoratore, nonché il relativo livello di responsabilità gerarchica e autonomia;
- l'eventuale condivisione di responsabilità con altri dipendenti che abbiano concorso nel determinare la violazione nonchè la relativa posizione funzionale;
- le particolari circostanze che contornano la violazione o in cui la stessa è maturata;
- la rilevanza degli obblighi violati e la circostanza che le conseguenze della violazione presentino o meno rilevanza esterna all'azienda;
- l'entità del danno derivante alla Società o dall'eventuale applicazione di sanzioni.

I provvedimenti disciplinari vengono applicati non solo in relazione alla gravità delle infrazioni, ma anche in considerazione di eventuali ripetizioni delle stesse; quindi le infrazioni, se ripetute più volte, danno luogo a provvedimenti disciplinari di peso crescente, fino alla eventuale risoluzione del rapporto di lavoro.

Vengono tenuti in considerazione a questo fine i provvedimenti comminati al lavoratore negli ultimi due anni.

I poteri disciplinari per i lavoratori dipendenti – accertamento delle infrazioni, procedimenti disciplinari e applicazione delle sanzioni – verranno esercitati, a norma di legge e di contratto, dal Datore di Lavoro.

Sono previste sanzioni disciplinari nei confronti di chi viola i principi alla base del meccanismo di segnalazione ("c.d. whistleblowing"), volti a tutelare sia il soggetto segnalante, sia il soggetto segnalato. In particolare:

- sanzioni disciplinari nei confronti di chi, essendone responsabile, non mantiene riservata l'identità del segnalante;
- sanzioni disciplinari nei confronti di cui attua o minaccia forme di ritorsione, discriminazione o penalizzazione per motivi collegati, indirettamente o direttamente, alla segnalazione;
- sanzioni disciplinari nei confronti di chi, abusando del maccanismo di whistleblowing, effettua segnalazioni manifestatamente opportunistiche allo scopo di danneggiare il Segnalato, effettuando con dolo o colpa grave segnalazioni che si rivelano infondate, fatta salva l'eventuale accertamento di responsabilità civile (ex art. 2043) o penale (per ipotesi di segnalazione calunniosa o diffamatoria ex codice penale).

***

Si riportano di seguito le correlazioni esistenti tra le mancanze specifiche e le sanzioni disciplinari che saranno applicate in caso di inosservanza, da parte del personale dipendente non dirigente, del Modello adottato dalla Società per prevenire la commissione dei reati previsti dal Decreto 231.

A) RIMPROVERO VERBALE

Nel caso di lieve inosservanza dei principi e delle regole di comportamento previsti dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello, correlandosi detto comportamento ad una "lieve inosservanza delle norme contrattuali o delle direttive ed istruzioni impartite dalla direzione o dai superiori".

B) AMMONIZIONI SCRITTE, MULTE E SOSPENSIONI

Incorre nei provvedimenti di ammonizione scritta, multa o sospensione il lavoratore che:

a) non si presenti al lavoro o abbandoni il proprio posto di lavoro senza giustificato motivo oppure non giustifichi l'assenza entro il giorno successivo a quello dell'inizio dell'assenza stessa salvo il caso di impedimento giustificato;

b) senza giustificato motivo ritardi l'inizio del lavoro o lo sospenda o ne anticipi la cessazione;

c) compia lieve insubordinazione nei confronti dei superiori;

d) esegua negligentemente o con voluta lentezza il lavoro affidatogli;

e) per disattenzione o negligenza guasti il materiale dello stabilimento o il materiale in lavorazione;

f) venga trovato in stato di manifesta ubriachezza, durante l'orario di lavoro;

g) fuori dell'azienda compia, per conto terzi, lavoro di pertinenza dell'azienda stessa;

h) contravvenga al divieto di fumare, laddove questo esista e sia indicato con apposito cartello;

i) esegua entro l'officina dell'azienda lavori di lieve entità per conto proprio o di terzi, fuori dell'orario di lavoro e senza sottrazione di materiale dell'azienda, con uso di attrezzature dell'azienda stessa;

l) in altro modo trasgredisca l'osservanza del presente Contratto o commetta qualsiasi mancanza che porti pregiudizio alla disciplina, alla morale, all'igiene ed alla sicurezza dello stabilimento.

L'ammonizione verrà applicata per le mancanze di minor rilievo; la multa e la sospensione per quelle di maggior rilievo.

L'importo delle multe che non costituiscono risarcimento di danni è devoluto alle esistenti istituzioni assistenziali e previdenziali di carattere aziendale o, in mancanza di queste, alla Cassa mutua malattia.

C) LICENZIAMENTO CON PREAVVISO.

In tale provvedimento incorre il lavoratore che commetta infrazioni alla disciplina ed alla diligenza del lavoro che, pur essendo di maggior rilievo di quelle contemplate nell'articolo 9, non siano così gravi da rendere applicabile la sanzione di cui alla lettera b).

A titolo indicativo rientrano nelle infrazioni di cui sopra:

a) insubordinazione ai superiori;

b) sensibile danneggiamento colposo al materiale dello stabilimento o al materiale di lavorazione;

c) esecuzione senza permesso di lavori nell'azienda per conto proprio o di terzi, di lieve entità senza impiego di materiale dell'azienda;

d) rissa nello stabilimento fuori dei reparti di lavorazione;

e) abbandono del posto di lavoro da parte del personale a cui siano specificatamente affidate mansioni di sorveglianza, custodia, controllo, fuori dei casi previsti al punto e) della seguente lettera b);

f) assenze ingiustificate prolungate oltre 4 giorni consecutivi o assenze ripetute per tre volte in un anno nel giorno seguente alle festività o alle ferie;

g) condanna ad una pena detentiva comminata al lavoratore, con sentenza passata in giudicato, per azione commessa non in connessione con lo svolgimento del rapporto di lavoro, che leda la figura morale del lavoratore;

h) recidiva in qualunque delle mancanze contemplate nell'articolo 9, quando siano stati comminati due provvedimenti di sospensione di cui all'articolo 9, salvo quanto disposto dall'ultimo comma dell'articolo 8.

D) LICENZIAMENTO SENZA PREAVVISO.

In tale provvedimento incorre il lavoratore che provochi all'azienda grave nocumento morale o materiale o che compia, in connessione con lo svolgimento del rapporto di lavoro, azioni che costituiscono delitto a termine di legge.

A titolo indicativo rientrano nelle infrazioni di cui sopra:

a) grave insubordinazione ai superiori;

b) furto nell'azienda;

c) trafugamento di schizzi o di disegni di macchine e di utensili o di altri oggetti, o documenti dell'azienda;

d) danneggiamento volontario al materiale dell'azienda o al materiale di lavorazione;

e) abbandono del posto di lavoro da cui possa derivare pregiudizio alla incolumità delle persone od alla sicurezza degli impianti o comunque compimento di azioni che implichino gli stessi pregiudizi;

f) fumare dove ciò può provocare pregiudizio all'incolumità delle persone od alla sicurezza degli impianti;

g) esecuzione senza permesso di lavori nell'azienda per conto proprio o di terzi, di non lieve entità e/o con l'impiego di materiale dell'azienda;

h) rissa nell'interno dei reparti di lavorazione

13.2.2 Sospensione cautelare non disciplinare

In caso di licenziamento per mancanze di cui al punto D) dell'articolo 10 (senza preavviso), l'azienda potrà disporre la sospensione cautelare non disciplinare del lavoratore con effetto immediato, per un periodo massimo di 6 giorni.

Il datore di lavoro comunicherà per iscritto al lavoratore i fatti rilevanti ai fini del provvedimento e ne esaminerà le eventuali deduzioni contrarie. Ove il licenziamento venga applicato, esso avrà effetto dal momento della disposta sospensione.

13.2.3 Misure nei confronti degli Amministratori

In caso di violazione accertata delle disposizioni del Modello, ivi incluse quelle della documentazione che di esso forma parte, da parte di uno o più amministratori, l'Organismo di Vigilanza è tenuto ad informare tempestivamente l'intero Consiglio di Amministrazione, affinchè provvedano ad assumere o promuovere le iniziative più opportune ed adeguate, in relazione alla gravità della violazione rilevata e conformemente ai poteri previsti dalla vigente normativa e dallo Statuto sociale.

In particolare, in caso di violazione delle disposizioni del Modello ad opera di uno o più Amministratori, il Consiglio di Amministrazione ha facoltà di procedere direttamente, in base all'entità e gravità della violazione commessa, all'irrogazione della misura sanzionatoria del richiamo formale scritto ovvero della revoca anche parziale dei poteri delegati e delle procure conferite nei casi più gravi, tali da ledere la fiducia della Società nei confronti del responsabile.

Infine, in caso di violazioni delle disposizioni del Modello ad opera di uno o più Amministratori, dirette in modo univoco ad agevolare o istigare la commissione di un reato rilevante ai sensi del D.Lgs. 231/2001 ovvero a commetterlo, le misure sanzionatorie (quali a mero titolo di esempio, la sospensione temporanea dalla carica e, nei casi più gravi, la revoca dalla stessa) dovranno essere adottate dall'Assemblea dei Soci, su proposta del Consiglio di Amministrazione.

A titolo esemplificativo e non esaustivo, commette una violazione rilevante ai fini del presente paragrafo l'Amministratore che:

• commetta gravi violazioni delle disposizioni del Modello e/o del Codice Etico, ivi inclusa l'omissione o il ritardo nella comunicazione all'Organismo di Vigilanza di informazioni dovute ai sensi del Modello e relative a situazioni non particolarmente a rischio o comunque ponga in essere tali comunicazioni in modo lacunoso o incompleto;
• ometta di vigilare adeguatamente sul comportamento dei dipendenti posti a proprio diretto riporto, al fine di verificare le loro azioni nell'ambito delle aree a rischio reato e, comunque, nello svolgimento di attività strumentali a processi operativi a rischio reato;
• non provveda a segnalare tempestivamente eventuali situazioni di irregolarità o anomalie inerenti il corretto adempimento delle procedure di cui al Modello di cui abbia notizia, tali da compromettere l'efficacia del Modello della Società o determinare un potenziale od attuale pericolo per la Società di irrogazione delle sanzioni di cui al Decreto 231;
• non individui tempestivamente, anche per negligenza o imperizia, eventuali violazioni delle procedure di cui al Modello e non provveda ad intervenire per il rispetto delle procedure e del Modello;
• attui o minacci forme di ritorsione, discriminazione o penalizzazione nei confronti di un dipendente o collaboratore, anche per motivi collegati, indirettamente o direttamente, ad una segnalazione;
• effettui con dolo o colpa grave segnalazioni di possibili violazioni che si rivelino infondate, fatta salva l'eventuale accertamento di responsabilità civile (ex art. 2043) o penale (per ipotesi di segnalazione calunniosa o diffamatoria ex codice penale);
• ponga in essere comportamenti tali da integrare le fattispecie di reato previste dal Decreto 231;
• ponga in essere qualsiasi situazione di conflitto di interessi – anche potenziale - nei confronti della Società o della Pubblica Amministrazione;
• distribuisca omaggi o regali a funzionari pubblici al di fuori di quanto previsto nel Codice Etico o accordi altri vantaggi di qualsiasi natura (ad es. promesse di assunzione);
• effettui prestazioni in favore dei partner che non trovino adeguata giustificazione nel contesto del rapporto costituito con i partner stessi;
• presenti dichiarazioni non veritiere ad organismi pubblici, nazionali e non, al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
• destini somme ricevute da organismi pubblici, nazionali e non, a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli a cui erano destinati;
• riconosca compensi in favore di collaboratori esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e alle prassi vigenti in ambito locale;
• non osservi rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, o non agisca nel rispetto delle procedure interne aziendali che su tali norme si fondano;

• non assicuri il regolare funzionamento della Società e degli organi sociali o non garantisca o non agevoli ogni forma di controllo sulla gestione sociale previsto dalla legge, nonchè la libera e corretta formazione della volontà assembleare;
• non effettui con tempestività, correttezza e buona fede tutte le comunicazioni previste dalle leggi e dai regolamenti nei confronti delle autorità di vigilanza, o ostacoli l'esercizio delle funzioni di vigilanza da queste intraprese;
• assuma un comportamento non corretto o non veritiero con gli organi di stampa e di informazione.
Inoltre, rientrano tra le gravi inosservanze l'omessa segnalazione all'Organismo di Vigilanza di qualsiasi violazione alle norme previste dal Modello di cui gli amministratori venissero a conoscenza, nonchè il non aver saputo – per negligenza o imperizia - individuare e conseguentemente eliminare violazioni del Modello e, nei casi più gravi, perpetrazione di reati.
Resta salvo in ogni caso il diritto della Società ad agire per il risarcimento del maggior danno subito a causa del comportamento dell'Amministratore.

13.2.4 Misure da attuare nei confronti di collaboratori esterni alla Società

Ogni comportamento posto in essere da soggetti esterni a BITCONTROL che, in contrasto con il presente Modello, sia suscettibile di comportare il rischio di commissione di uno degli illeciti per i quali è applicabile il Decreto, determinerà, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di convenzione, la risoluzione anticipata del rapporto contrattuale, fatta ovviamente salva l'ulteriore riserva di risarcimento qualora da tali comportamenti derivino danni concreti a BITCONTROL, come nel caso di applicazione da parte dell'Autorità Giudiziaria delle sanzioni previste dal Decreto.

13.2.5 Misure nei confronti dell'Organismo di Vigilanza

Nei casi in cui l'Organismo di Vigilanza, per negligenza ovvero imperizia, non abbia saputo individuare, e, conseguentemente, adoperarsi per eliminare, violazioni del Modello e, nei casi più gravi, perpetrazione di reati, il Consiglio d'Amministrazione procederà agli accertamenti necessari e potrà assumere, a norma di legge e di statuto, gli opportuni provvedimenti, ivi inclusa la revoca dell'incarico per giusta causa. Per l'approvazione di una delibera di revoca per giusta causa del componente l'Organismo di Vigilanza, è richiesto il voto favorevole di una maggioranza pari ai 2/3 dei membri del Consiglio.
Resta salvo in ogni caso il diritto della Società ad agire per il risarcimento del maggior danno subito a causa del comportamento dell'Organismo di Vigilanza.

13.3 Accertamento delle violazioni e procedimento disciplinare

13.3.1 Valutazione, indagine e accertamento della violazione

Le responsabilità e le modalità di valutazione, indagine e successivo accertamento della violazione sono definite nell'ambito della procedura "whistleblowing", cui si rimanda.

13.3.2 Irrogazione della sanzione a dipendenti (non dirigenti)

I soggetti interessati potranno essere convocati per chiarire i fatti e le situazioni contestate. In ogni caso l'addebito sarà formalizzato e comunicato al/agli interessati, garantendo ad essi la possibilità di opporsi e fornire la propria versione, con un congruo termine di replica in ordine alla propria difesa.

Resta inteso che saranno sempre rispettate le procedure, le disposizioni e le garanzie previste dall'art.7 dello Statuto dei Lavoratori, nonchè dal CCNL Metalmeccanica Industria applicato al personale dipendente di BITCONTROL.

Al Responsabile delle Risorse Umane spetta in ogni caso l'attuazione del procedimento disciplinare e l'irrogazione della sanzione, proporzionata alla gravità della violazione commessa ed all'eventuale recidiva.

Nell'irrogazione della sanzione disciplinare sarà rispettato il principio della proporzionalità tra infrazione e sanzione e dovrà tenersi conto di eventuali circostanze attenuanti la gravità del comportamento (attività diretta a rimuovere o impedire le conseguenze dannose, entità del danno o delle conseguenze, etc.) e saranno valutate le circostanze specifiche.

L'esito di ogni procedimento disciplinare, derivante da inadempienze del Modello 231, è comunicato all'Organismo di Vigilanza.

Tutta la documentazione prodotta con riferimento alla rilevazione, accertamento e comunicazione di eventi potenzialmente oggetto di sanzione e alla relativa valutazione da parte del Responsabile di Funzione e del datore di lavoro, nonchè la notifica al dipendente della sanzione e l'eventuale contestazione, sono archiviate presso la Direzione Risorse Umane.

Si applicano le medesime regole e procedure sopra menzionate per quanto riguarda i dipendenti non dirigenti, fatti salvi i richiami normativi non applicabili per legge ai dirigenti.

La sanzione sarà determinata e successivamente irrogata, previa contestazione formale dell'addebito all'interessato, dai soggetti dotati di idonea procura, in forma congiunta.

13.3.4 Accertamento della violazione e provvedimenti nei confronti di amministratori

Alla notizia di una rilevante inosservanza, da parte di uno o più Amministratori, delle norme previste dal Modello e/o dal Codice Etico o di comportamenti, durante lo svolgimento di attività a rischio ai sensi del Decreto 231, non conformi a quanto prescritto nel Modello stesso, l'Organismo di Vigilanza dovrà tempestivamente informare dell'accaduto l'intero Consiglio di Amministrazione, per l'adozione di ogni più opportuna iniziativa.

Il Consiglio di Amministrazione procederà agli accertamenti necessari e potrà assumere, a norma di legge e di statuto, gli opportuni provvedimenti quali, ad esempio, la convocazione dell'Assemblea dei soci per la revoca del mandato, e/o l'azione sociale di responsabilità ai sensi dell'art. 2393 c. c..

13 AGGIORNAMENTO DEL MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Il Decreto 231 espressamente prevede la necessità di aggiornare il Modello d'organizzazione, gestione e controllo, al fine di rendere lo stesso costantemente adeguato alle specifiche esigenze dell'ente e della sua concreta operatività. Gli interventi di adeguamento e/o aggiornamento del Modello saranno realizzati essenzialmente in occasione di:

• innovazioni normative;

• violazioni del Modello e/o rilievi emersi nel corso di verifiche sull'efficacia del medesimo (che potranno anche essere desunti da esperienze riguardanti altre Società);

• modifiche della struttura organizzativa dell'ente, anche derivanti da operazioni di finanza straordinaria ovvero da mutamenti nella strategia d'impresa derivanti da nuovi campi di attività intrapresi.

Segnatamente, l'aggiornamento del Modello e, quindi, la sua integrazione e/o modifica, spetta al medesimo Consiglio di Amministrazione cui il legislatore ha demandato l'onere di adozione del Modello medesimo. La semplice "cura" dell'aggiornamento, ossia la mera sollecitazione in tal senso e non già la sua diretta attuazione spetta invece all'Organismo di Vigilanza.

L'aggiornamento del Modello deve essere effettuato anche quando intervengano revisioni delle Parti Speciali, della Policy IA, delle procedure di cybersecurity, della Procedura Whistleblowing o delle altre procedure organizzative che incidano sui processi sensibili, sui controlli, sui flussi informativi o sui reati presupposto rilevanti.

Le risultanze delle verifiche svolte dall'OdV, gli audit interni, le segnalazioni whistleblowing, gli incidenti informatici, le non conformità documentali, gli eventi infortunistici, le criticità ambientali e le anomalie nell'uso dei sistemi di IA costituiscono elementi rilevanti ai fini della revisione della Parte Generale e delle Parti Speciali.

In caso di contrasto apparente tra disposizioni generali e protocolli speciali, prevale la disciplina più specifica contenuta nella Parte Speciale applicabile al processo sensibile interessato, fermo restando il rispetto dei principi generali del Modello, del Codice Etico, della Procedura Whistleblowing e della Policy IA.

14 IL CODICE ETICO DI BITCONTROL

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

Il Codice Etico adottato da BITCONTROL è uno strumento di autoregolamentazione volontaria, parte integrante del modello di gestione della Sostenibilità e contiene la mission, i valori aziendali e i principi che regolano le relazioni con gli stakeholder, a partire dall'identità aziendale. In alcuni

ambiti di particolare rilevanza (es. diritti umani, tutela del lavoro, salvaguardia dell'ambiente, lotta alla corruzione) richiama regole e principi coerenti ai migliori standard internazionali.
Il Modello risponde, invece, a specifiche prescrizioni contenute nel D.Lgs. 231/2001 finalizzate a prevenire la commissione di particolari tipologie di reati.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA del 14.11.2020	ADOZIONE
Rev. 1	CDA del 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA del 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA del 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA del 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA del 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

2 SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

La presente procedura definisce i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento adottati dalla BITCONTROL S.r.l. nell'ambito dei processi di incasso e pagamento, derivanti dalle attività operative, nel rispetto dei vincoli e degli obiettivi previsti.

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.

La presente procedura si intende altresì aggiornata alla disciplina introdotta dal D.Lgs. n. 211/2025, entrato in vigore il 24.01.2026, che recepisce la Direttiva (UE) 2024/1226 e introduce nuovi reati presupposto nel catalogo del D.Lgs. 231/2001 relativi alle violazioni delle misure restrittive dell'Unione Europea, con specifica rilevanza per la gestione dei flussi finanziari, dei pagamenti, delle controparti estere e dei beneficiari effettivi.

La suddetta riforma, ha fissato i ruoli, le responsabilità operative, le attività di controllo e i principi di comportamento adottati dalla BITCONTROL 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).

Invero, 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, in attuazione del D.Lgs. 30 dicembre 2025, n. 211, i controlli di tesoreria comprendono la verifica delle misure restrittive dell'Unione europea applicabili alla controparte, al beneficiario effettivo, agli intermediari, al Paese di destinazione o provenienza dei fondi e all'oggetto dell'operazione, con obbligo di sospensione ed escalation in presenza di corrispondenze, anomalie o dubbi.

Invero, i presidi qui previsti sono finalizzati, in particolare, alla prevenzione dei reati rilevanti nei processi finanziari e di tesoreria, tra cui i delitti informatici e la frode informatica, i delitti in materia

di strumenti di pagamento diversi dai contanti, la ricettazione, il riciclaggio, l'impiego di denaro, beni o utilità di provenienza illecita, l'autoriciclaggio, il trasferimento fraudolento di valori, i reati tributari e le violazioni delle misure restrittive dell'Unione europea.

3 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
RIA	Responsabile IA
RCA	Responsabile interno conformità aziendale

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E AI RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

4 RIFERIMENTI NORMATIVI DEL MODELLO

- DECRETO LEGISLATIVO 231/2001 E S.S. MM.II (DI SEGUITO ANCHE D.LGS 231/01);
- CODICE ETICO DI BITCONTROL S.R.L.;
- CODICE DISCIPLINARE DI BITCONTROL S.R.L.
- MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO DI BITCONTROL S.R.L..
- D.LGS. 21 NOVEMBRE 2007, N. 231 E SUCCESSIVE MODIFICAZIONI, PER QUANTO APPLICABILE;
- D.LGS. 8 NOVEMBRE 2021, N. 184;
- ART. 25-OCTIES E ART. 25-OCTIES.1 DEL D.LGS. 231/2001;
- D.LGS. 30 DICEMBRE 2025, N. 211;
- NORMATIVA VIGENTE IN MATERIA DI LIMITAZIONE ALL'USO DEL CONTANTE, TRACCIABILITÀ DEI PAGAMENTI, MISURE RESTRITTIVE DELL'UNIONE EUROPEA E PROTEZIONE DEI DATI PERSONALI;
- POLICY IA, PROCEDURA WHISTLEBLOWING E PROCEDURE DI SICUREZZA DELLE INFORMAZIONI DI BITCONTROL S.R.L.

5 CAMPO DI APPLICAZIONE E DESTINATARI DELLA PROCEDURA

La presente procedura si applica a tutti i *Destinatari* che hanno il potere di ricevere denaro o effettuare pagamenti in nome e per conto della Società, nonché di gestire i profili connessi agli 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 BITCONTROL S.r.l. che potrebbero concorrere alla realizzazione delle fattispecie delittuose qui declamate.

6 RESPONSABILE DELLA PROCEDURA

Il principale responsabile della seguente procedura 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*.

Le figure aziendali coinvolte nei processi di tesoreria operano in coordinamento con i presidi organizzativi adottati o aggiornati nel 2026, inclusi Modello 231, Codice Etico, Codice di Condotta, Procedura Whistleblowing, Policy IA, regolamenti sul lavoro agile e procedure di sicurezza delle informazioni.

L'elenco del personale autorizzato o coinvolto in attività rilevanti per la tesoreria, ivi inclusi firma disposizioni, accesso ai conti, ruoli di controllo, utilizzo di sistemi automatizzati o di strumenti IA, deve essere aggiornato.

7 INDICAZIONI COMPORTAMENTALI

Il ciclo di gestione delle risorse finanziarie è svolto dalle varie funzioni aziendali abilitate, nell'ambito dei limiti autorizzativi di importo e nel rispetto della presente procedura, e consiste nelle attività di controllo e monitoraggio delle risorse economiche e finanziarie, nonché dei relativi flussi (ovvero degli incassi e dei pagamenti).

I flussi finanziari 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, ciascuno nell'ambito della propria attività, sono tenuti a:

- evitare di porre in essere comportamenti che possano, anche solo astrattamente, integrare i reati presupposto rilevanti per la tesoreria e, in particolare, quelli richiamati dagli artt. 24-bis, 25-octies, 25-octies.1 e 25-quinquiesdecies del D.Lgs. 231/2001, nonché le fattispecie introdotte in materia di violazione delle misure restrittive dell'Unione europea;

ed hanno espresso <u>divieto</u> di:

- intrattenere rapporti commerciali con soggetti fisici o giuridici dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali di qualsiasi tipo;
- effettuare o ricevere pagamenti in contante, mediante titoli al portatore o con altri strumenti non tracciabili in violazione dei limiti di legge o dei più restrittivi limiti interni stabiliti dalla Società;
- utilizzare strumenti di pagamento diversi dai contanti, inclusi carte, portafogli digitali, moneta elettronica o cripto-attività, in assenza di preventiva autorizzazione aziendale, adeguata identificazione della controparte, tracciabilità e documentazione dell'operazione;
- disporre, accettare o agevolare operazioni in cripto-attività o mediante strumenti digitali non espressamente autorizzati dall'Organo Amministrativo, ovvero utilizzare wallet, account o credenziali personali per operazioni riferibili alla Società
- 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;
- 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;
- 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;
- 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;
- porre in essere una condotta che abbia, anche solo, creato intralcio non definitivo, ma concreto, rispetto all'identificazione della provenienza delittuosa del bene.
- porre in essere negozi simulati, intestazioni fiduciarie non trasparenti o operazioni prive di effettiva giustificazione economica, volte a dissimulare la titolarità o disponibilità di denaro, beni, quote, azioni o altre utilità;
- 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.).

I Destinatari sono tenuti a conformarsi, oltre che alla normativa vigente e al Modello 231, ai principi di legalità, integrità, correttezza, veridicità, tracciabilità delle operazioni, conservazione della documentazione, riservatezza delle informazioni e prevenzione dei conflitti di interesse sanciti dal Codice Etico e dal Codice di Condotta aziendali.

Si rileva altresì che, i pagamenti a favore di terzi devono essere effettuati su conti correnti intestati al beneficiario effettivo, tracciabili e riferiti a obbligazioni contrattuali documentate.
È fatto assoluto divieto di effettuare pagamenti in contante non documentati, pagamenti a soggetti non identificabili o attraverso canali non tracciabili.
È fatto divieto di disporre o autorizzare operazioni finanziarie in assenza di preventiva verifica della controparte, della documentazione giustificativa, della coerenza economica dell'operazione e, ove rilevante, dell'assenza di collegamenti con soggetti o paesi destinatari di misure restrittive dell'Unione Europea.
È fatto divieto di falsificare, alterare, omettere, distruggere o utilizzare documentazione contabile, bancaria, fiscale o contrattuale non veritiera ovvero incompleta, nonché di ostacolare i controlli interni e quelli dell'Organismo di Vigilanza.
I *Destinatari* coinvolti nella gestione delle attività di tesoreria devono garantire, ognuno per le parti di rispettiva competenza, l'esecuzione dei seguenti specifici controlli.

7. BIS PRESIDI SPECIFICI

In considerazione dell'attività di BitControl S.r.l., consistente nella progettazione, nello sviluppo, nell'integrazione, nell'assistenza e nella manutenzione di soluzioni informatiche e di automazione per sistemi di supervisione e telecontrollo, anche nell'ambito di commesse pubbliche e private, nazionali ed estere, i processi di tesoreria devono essere presidiati mediante i seguenti controlli specifici:

• attribuzione di ciascun incasso, pagamento, anticipo, rimborso o movimentazione finanziaria alla relativa commessa, contratto, ordine, centro di costo o codice progetto, al fine di assicurare la piena tracciabilità economico-finanziaria delle attività svolte nei settori idrico, energetico, industriale e dei sistemi di telecontrollo;

• verifica, prima del pagamento di fornitori, subappaltatori, consulenti tecnici e partner di progetto, della corrispondenza tra contratto o ordine, stato di avanzamento delle attività, rapportino tecnico, verbale di collaudo o accettazione, documento di trasporto e fattura, secondo la natura della prestazione;

• divieto di liquidare prestazioni tecniche, licenze software, apparati hardware, PLC, RTU, componenti di automazione, servizi cloud, connettività, manutenzioni o attività di commissioning in assenza della conferma della funzione tecnica o del responsabile di commessa circa l'effettiva esecuzione, consegna, attivazione o collaudo;

• controllo specifico dei pagamenti anticipati e degli acconti relativi a forniture tecnologiche, licenze, apparati o attività da eseguire all'estero, con preventiva autorizzazione dell'Organo Amministrativo, verifica delle condizioni contrattuali e monitoraggio del successivo adempimento della controparte;

• riconciliazione degli incassi provenienti da clienti pubblici, gestori di servizi pubblici, utilities e committenti industriali con fatture, SAL, certificati di pagamento, mandati, CUP, CIG o altri codici identificativi applicabili alla singola commessa, ove previsti;

• verifica della corretta destinazione e contabilizzazione delle somme derivanti da finanziamenti, contributi, anticipazioni contrattuali o risorse pubbliche, con divieto di impiego per finalità estranee alla commessa o al progetto finanziato e con conservazione separata delle relative evidenze;

• controllo rafforzato delle operazioni con controparti estere, agenti, partner, tecnici o fornitori impiegati in attività di commissioning e assistenza fuori dal territorio nazionale, mediante verifica della controparte, del beneficiario effettivo, del Paese, della banca destinataria, della causale e della coerenza dell'importo con il contratto e con l'attività documentata;

• gestione delle spese di trasferta e dei rimborsi relativi a interventi tecnici presso impianti e cantieri sulla base di autorizzazione, nota spese, giustificativi, indicazione della commessa e verifica della coerenza temporale e geografica con l'attività svolta; è vietato il rimborso di spese personali, non documentate o non pertinenti;

• assegnazione nominativa delle carte aziendali, delle carte carburante, dei dispositivi Telepass e degli strumenti di pagamento utilizzati dal personale tecnico, con limiti di spesa, divieto di cessione a terzi, rendicontazione periodica e riconciliazione con la commessa e con i giustificativi;

• separazione, per quanto compatibile con l'assetto organizzativo, tra responsabile di commessa o funzione tecnica che attesta la prestazione, funzione amministrativa che verifica e registra il documento, soggetto che predispone il pagamento e Organo Amministrativo che lo autorizza; eventuali deroghe devono essere motivate, documentate e sottoposte a controllo successivo;

• verifica periodica degli abbonamenti, delle licenze software, dei servizi cloud, dei canoni di connettività e dei contratti di manutenzione ricorrenti, al fine di evitare rinnovi automatici non autorizzati, duplicazioni, pagamenti per utenze non più attive o servizi non utilizzati;

• protezione dei flussi finanziari connessi alle commesse mediante utilizzo esclusivo di sistemi gestionali, remote banking e archivi aziendali autorizzati, in coerenza con il sistema di gestione della sicurezza delle informazioni adottato dalla Società; è vietato utilizzare account personali, caselle e-mail non aziendali o dispositivi non autorizzati per impartire, modificare o confermare disposizioni di pagamento;

• verifica indipendente di ogni richiesta di variazione delle coordinate bancarie proveniente da clienti, fornitori, partner o personale impegnato su commesse, con particolare attenzione alle comunicazioni ricevute durante trasferte, attività da remoto o rapporti internazionali, al fine di prevenire frodi informatiche e compromissioni della posta elettronica aziendale;

• monitoraggio degli scostamenti tra budget di commessa, costi sostenuti, pagamenti effettuati, ricavi fatturati e incassi, con tempestiva segnalazione all'Organo Amministrativo e all'Organismo di Vigilanza di sovrafatturazioni, duplicazioni, pagamenti frazionati, beneficiari anomali o operazioni prive di giustificazione economica.

7.1 LA GESTIONE DEI PAGAMENTI E L'UTILIZZO DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

La Funzione aziendale autorizzata a predisporre o disporre un pagamento è tenuta al rispetto delle fasi di seguito indicate, assicurando la separazione, ove organizzativamente possibile, tra chi inserisce la disposizione, chi verifica la documentazione e chi autorizza l'operazione:

1. Il RAM deve predisporre un piano di pagamenti mensile, che verrà condiviso in una piattaforma digitale (come ad esempio TEAMS o similari) e che dovrà essere validato, con firma digitale o con firma olografa, dal Presidente;
2. per quanto concerne il pagamento dei dipendenti, è necessario acquisire – prima di effettuare 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 (o di altro supporto documentale idoneo);
   - la regolare emissione della fattura;
   - l'effettiva esecuzione della prestazione per la quale si richiede o si effettua il pagamento (in 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.
   - Prima del pagamento deve essere verificata la coincidenza tra intestatario del conto, controparte contrattuale e beneficiario della fattura. Ogni richiesta di modifica dell'IBAN o delle coordinate di pagamento deve essere verificata attraverso un canale indipendente e già

noto, mediante contatto con un referente autorizzato della controparte, e deve essere documentata. Non è sufficiente la sola comunicazione ricevuta via e-mail.

4. in caso di pagamenti superiori a euro 15.000,00 giornalieri, sarà necessario chiedere apposita autorizzazione per iscritto al PRES, salvo il caso di pagamenti per beni/investimenti finanziati dalla P.A. per cui è sempre necessaria la predetta autorizzazione (cfr. PMOG 03). I pagamenti di importo superiore ad euro 15.000,00 dovranno essere oggetto di specifico *report* semestrale che dovrà essere trasmesso all'OdV.
   Si precisa che per i predetti pagamenti di importo superiore ad euro 15.000,00, 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.

Prima di disporre o autorizzare pagamenti, in particolare in favore di controparti estere o comunque esposte a rischio, devono essere effettuati controlli di screening sulla controparte, sul beneficiario effettivo, sui dati identificativi del conto di destinazione, sulla coerenza tra causale, contratto, fattura e flusso finanziario, nonché sulla eventuale riconducibilità del soggetto a liste di sanzioni o misure restrittive applicabili.

In presenza di elementi di anomalia, incongruenze documentali, utilizzo di intermediari non coerenti con l'operazione, controparti non chiaramente identificabili, richieste di pagamento verso soggetti diversi dal beneficiario contrattuale ovvero indicatori di possibile elusione di misure restrittive o di normativa antiriciclaggio, l'operazione deve essere immediatamente sospesa e sottoposta a escalation al Responsabile amministrativo/finanziario, all'Ufficio Legale e all'Organismo di Vigilanza.

Le verifiche effettuate, le autorizzazioni rilasciate, le eventuali sospensioni e le decisioni assunte devono essere tracciate e conservate agli atti, in modo da consentire la ricostruzione del processo decisionale e dei soggetti intervenuti.

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

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

Ai sensi del D. Lgs 231/2001, il processo relativo all'esecuzione di operazioni di pagamento, 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; per tale ragione BitControl S.r.l. pone in essere procedure specifiche finalizzate a prevenire e ad ostacolare gli utilizzi fraudolenti degli strumenti di pagamento e quindi l'esecuzione di operazioni di pagamento non autorizzate, in osservanza alla normativa vigente ed ai principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività di pagamento.

INVERO, 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).

7.2 GESTIONE INCASSI

Il RAM/RRU, o altra funzione eventualmente incaricata per iscritto, assicura che per ciascun incasso si controlli l'identità della controparte, sia essa persona giuridica che persona fisica, ed in particolare deve assicurare l'inserimento del soggetto interessato nell'anagrafica aziendale.
Il RAM/RRU, o altra funzione eventualmente incaricata per iscritto, verifica che per ciascun incasso corrisponda un documento giustificativo.
Il RAM deve predisporre accanto al "piano pagamenti mensile", anche un "piano degli incassi mensile"; il suddetto piano degli incassi verrà condiviso in una piattaforma digitale (come ad esempio TEAMS o similari) 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.

È, altresì, previsto che si registrino e si documentino in maniera corretta e accurata tutti i pagamenti di questo genere e che sia sempre certa l'identificazione della loro provenienza, così da potere escludere una provenienza delittuosa.
In ultimo, si precisa che per ogni incasso deve essere verificata e registrata l'identità della controparte, la riconducibilità dell'incasso al rapporto contrattuale o al titolo giustificativo, nonché la coerenza tra soggetto pagatore, causale dell'operazione e documentazione commerciale o contabile di riferimento.
Nel caso di incassi provenienti da soggetti terzi non coincidenti con la controparte contrattuale, da paesi esteri, da canali di pagamento atipici o da soggetti non previamente censiti, devono essere eseguite verifiche rafforzate e, in caso di anomalia, l'operazione deve essere segnalata internamente secondo i flussi previsti dalla presente procedura e dalla Procedura Whistleblowing.

7.3 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 di libretti di risparmio anche al portatore, la costituzione e la stipulazione di finanziamenti e di fidi, *etc.*) è di esclusiva competenza dell'Organo Amministrativo.
L'Organo Amministrativo ha il potere di firmare contratti con gli Istituti di Credito (come l'apertura di c/c bancari, la costituzione di depositi e di libretti di risparmio anche al portatore, di costituzione e di stipulazione di finanziamenti e di fidi, *etc.*).
L'Organo Amministrativo sottoscrive o autorizza i contratti con gli Istituti di Credito e definisce i soggetti abilitati, i limiti operativi, i poteri di firma e i meccanismi di controllo, nel rispetto delle deleghe e procure vigenti.
L'apertura di nuovi conti, la modifica delle condizioni bancarie, l'abilitazione di nuovi utenti, la variazione dei poteri di firma, l'attivazione di dispositivi di remote banking o di strumenti di autorizzazione da remoto devono essere formalmente autorizzate, documentate e tracciate, con assegnazione nominativa dei profili di accesso e separazione delle funzioni tra disposizione, controllo e autorizzazione.
Qualora le attività di tesoreria siano svolte, anche in parte, in lavoro agile o da remoto, devono essere applicate le misure di sicurezza informatica, firma elettronica, protezione credenziali, riservatezza e tracciabilità previste dai regolamenti aziendali e dai presidi organizzativi richiamati dall'OdV.

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*.

7.4 GESTIONE CASSA

I prelevamenti di cassa sono eseguiti dall'Organo Amministrativo e qualora siano eseguiti da soggetti diversi (in possesso di bancomat e relativo codice pin), questi devono essere espressamente autorizzati dallo stesso Organo Amministrativo. Per le spese impreviste verrà istituito un fondo cassa, di ammontare non superiore ad € 300,00 mensili, che potrà essere utilizzato, senza la previa autorizzazione dell'Organo Amministrativo, ma con obbligo di annotare il prelevamento eseguito, il soggetto che lo ha eseguito e la causale.

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.

7.5 FATTURAZIONE E TRASMISSIONE PERIODICA LIQUIDAZIONE IVA

La corretta gestione dei processi di fatturazione attiva e passiva richiede la differenziazione delle funzioni incaricate delle fasi di emissione/ricezione e di registrazione dei pagamenti, e specificamente:

- i controlli sulle fatture emesse/ricevute ed i controlli di registrazione delle stesse vengono svolte da funzioni diverse (ovvero dal REC e dal RAM/RRU);
- i controlli eseguiti dovranno accertare, in particolare, la coerenza delle informazioni contenute nei documenti giustificativi delle operazioni e la conformità dei dati inseriti nei medesimi documenti.

Qualora venissero riscontrate delle anomalie, le funzioni incaricate sono obbligate a dare immediata comunicazione all'OdV.

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

7.6 SISTEMA GESTIONALE

Il sistema gestionale adottato dalla Società per la gestione di tutte le attività fiscali-amministrativo-contabili, ed in particolare per le attività di fatturazione attiva e passiva e dei relativi incassi ed acquisti, verrà implementato attraverso un processo elettronico che dovrà garantire:

- l'identificazione dei ruoli dei soggetti incaricati di tali adempimenti all'interno della Società o per conto di essa, con specifico riferimento alle attività di formazione, trasmissione, archiviazione ed eventuale aggiornamento della documentazione rilevante (nello specifico, la registrazione avverrà anche attraverso l'estrazione di copie di *backup* ad opera delle funzioni incaricate, quali il REC e il RAM/RRU);
- la registrazione di tutte le fasi del procedimento, ivi compresa, ove prevista, l'eventuale fase autorizzativa;

- l'esistenza di appositi supporti (sia analogici che digitali), finalizzati a garantire, attraverso la compilazione *ad hoc*, la tracciabilità delle fatture emesse e/o ricevute dalla Società;
- 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;
- 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.

Il sistema gestionale e i sistemi di remote banking devono garantire la tracciabilità univoca degli accessi, delle operazioni inserite, modificate, autorizzate o annullate, con conservazione dei log, dei metadata e delle evidenze utili alla ricostruzione delle attività svolte.

Devono inoltre essere assicurati controlli sugli accessi, autenticazione forte, segregazione dei profili autorizzativi, conservazione delle evidenze informatiche, gestione degli incidenti e tempestiva comunicazione all'OdV degli eventi informatici che incidano o possano incidere sui processi di tesoreria.

Si precisa che, l'utilizzo di strumenti di Intelligenza Artificiale o di automazione avanzata nei processi di tesoreria è consentito esclusivamente nel rispetto della Policy IA aziendale, del Codice Etico, del Codice di Condotta, del Modello 231 e delle ulteriori procedure aziendali vigenti.

L'IA deve operare sempre sotto il controllo di una persona autorizzata. Ogni output generato da un sistema di IA deve essere validato da un essere umano prima di produrre effetti giuridici, economici o significativi sulle persone.

È consentito l'utilizzo degli strumenti di IA esclusivamente per attività di supporto, analisi preliminare, predisposizione di bozze, riassunti o classificazioni, purché non comportino decisioni autonome di autorizzazione di pagamenti, esecuzione di disposizioni bancarie, firma elettronica automatica, apertura di rapporti o assunzione di decisioni con effetti economici o giuridici.

È espressamente vietato utilizzare strumenti di IA non approvati, account personali, ovvero inserire in tali strumenti dati personali non anonimizzati, credenziali, dati bancari riservati, contratti bancari, condizioni economiche non pubbliche, piani finanziari, offerte, documentazione di gara o altre informazioni classificate come riservate o confidenziali.

Ogni attività di tesoreria svolta con il supporto di strumenti di IA deve essere soggetta a logging, tracciabilità dei prompt e degli output rilevanti, conservazione documentale, revisione umana e, ove necessario, valutazione preventiva del rischio e degli impatti ai sensi della Policy IA.

Qualsiasi uso improprio, violazione di dati o anomalia relativa a strumenti di IA impiegati nei processi di tesoreria deve essere segnalata immediatamente al Responsabile Sicurezza Informatica, al DPO e all'Organismo di Vigilanza.

8 TRASFERIMENTO FRAUDOLENTO DI VALORI (EX ART. 512 BIS C.P.)

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).

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.

Il secondo comma dell'art. 512-bis c.p., introdotto nel 2024, estende la pena prevista dal primo comma 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 cariche sociali, qualora l'imprenditore o la società partecipi a procedure di aggiudicazione o di esecuzione di appalti o concessioni.

Dunque, i *Destinatari* della presente procedura, ciascuno nell'ambito della propria attività, sono tenuti a:

- non attribuire fittiziamente a terzi la titolarità o disponibilità di denaro, beni, imprese, quote, azioni, cariche sociali o altre utilità, né utilizzare soggetti interposti, al fine di eludere misure di prevenzione patrimoniali, disposizioni antimafia, obblighi di contrabbando, misure restrittive o controlli interni, ovvero di agevolare delitti di ricettazione, riciclaggio o impiego di utilità di provenienza illecita.

Le verifiche sul trasferimento fraudolento di valori devono essere coordinate con i controlli sull'effettiva titolarità dei rapporti, sulla corrispondenza tra soggetto formalmente destinatario e beneficiario effettivo dell'operazione, sulla liceità della causa dell'operazione e sulla eventuale interposizione fittizia o utilizzo di soggetti terzi al fine di eludere misure di prevenzione, misure restrittive, obblighi di tracciabilità o controlli interni.

SUL SISTEMA SANZIONATORIO:

Si precisa 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, LA CONFIGURAZIONE DEI CITATI REATI PRESUPPOSTI COMPARTANO L'APPLICAZIONE DELLE 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.

9 ACQUISIZIONE DI NUOVI CESPITI

Oltre a quanto sopra riportato, tutte le operazioni relative all'acquisizione o dismissione di cespiti prevedono l'emanazione di un atto da parte della funzione interessata, vistato dal PRES.
Le decisioni di acquisizioni e dismissione di nuovi cespiti hanno origine nella formazione del piano investimenti all'uopo predisposto e nei successivi procedimenti autorizzativi, che vengono comunicati dalla Società allo Studio di consulenza incaricato della tenuta della contabilità.

10 DISMISSIONE DEI CESPITI

Il RATTR - o altra Funzione autorizzata ed incaricata per iscritto – comunica al PRES ed al RAM/RRU l'esigenza di dismissione del bene e predispone una scheda del bene a cespite, ponendo la firma e caricando la suddetta copia nell'archivio informatico della piattaforma digitale, 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.

11 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutti i *Destinatari* coinvolti e, precisamente coloro che hanno rilevato una situazione anomala o una violazione del Modello nella gestione degli aspetti fiscali-amministrativo-contabili, sono tenuti ad informare tempestivamente l'Organismo di Vigilanza delle situazioni anomale e/o effettuate in contrasto con la presente procedura, nonché eseguite in violazione delle disposizioni del Modello e del Codice Etico.

Fermo quanto sopra, devono essere sempre comunicati all'OdV:

- i pagamenti superiori ad euro 15.000,00 (attraverso l'invio di appositi *report* semestrali);
- con cadenza annuale, l'elenco dei conti correnti "temporanei" o inattivi (ad es. da 6 mesi) o poco movimentati (ad es. ≤ 2 operazioni in un anno);
- tempestivamente, eventuali operazioni frequenti e/o di significativo ammontare su conti correnti indicati come temporanei o inattivi o poco movimentati, con espressa indicazione delle modalità di trasferimento, dei destinatari e dei beneficiari dei flussi finanziari;
- 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.

– operazioni sospese, bloccate o sottoposte a escalation per rischio di collegamento con soggetti sanzionati, misure restrittive dell'Unione Europea, incongruenze documentali, anomalia della controparte o possibile elusione della normativa applicabile;

– anomalie o incidenti informatici che coinvolgano sistemi di tesoreria, remote banking, firme elettroniche, workflow autorizzativi o dati finanziari;

– utilizzo di sistemi di IA nei processi di tesoreria, con indicazione delle finalità, degli strumenti autorizzati impiegati, dei controlli svolti sugli output e delle eventuali criticità riscontrate;

- variazioni dei soggetti autorizzati a operare sui conti, a impartire disposizioni, a utilizzare firme digitali o a gestire sistemi informatici di tesoreria;

– segnalazioni whistleblowing ricevute o comunque fatti rilevanti in materia di frodi, falsificazioni documentali, violazioni contabili, antiriciclaggio, sicurezza informatica, uso improprio dell'IA o violazioni del Modello 231 attinenti ai processi di tesoreria.

In ogni caso, 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.

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.

Le segnalazioni aventi ad oggetto anomalie di tesoreria, frodi finanziarie, falsificazioni documentali, operazioni sospette, violazioni contabili, violazioni delle misure restrittive dell'Unione Europea, utilizzo improprio di strumenti di IA, sicurezza informatica o altre condotte rilevanti ai sensi del Modello 231 devono essere effettuate attraverso il canale interno di whistleblowing gestito dall'Organismo di Vigilanza, secondo la Procedura Whistleblowing.

Restano fermi l'avviso di ricevimento entro 7 giorni, il riscontro entro 3 mesi, la conservazione della documentazione per 5 anni, il divieto di ritorsione e le misure di riservatezza dell'identità del segnalante, della persona coinvolta e del contenuto della segnalazione.

La segnalazione è obbligatoria quando il destinatario abbia conoscenza diretta di condotte corruttive, reati presupposto ai sensi del D.Lgs. 231/2001, frodi o falsificazioni documentali a danno della Società, dei clienti o di enti pubblici.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev.1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev.7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev.8	CDA DEL 27.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

La presente procedura definisce i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento adottati dalla BITCONTROL S.r.l. nell'ambito dei processi societari e fiscali-amministrativo-contabili ed in particolare dell'attività di predisposizione del bilancio.

Il documento viene posto in essere nel rispetto di quanto previsto dal Codice Etico e dal Modello adottati dalla Società in coordinamento con il il Codice di Condotta aziendale, la Policy IA aziendale, la Procedura Whistleblowing vigente, i flussi informativi verso l'Organismo di Vigilanza e ogni altra procedura interna rilevante adottata dalla Società e, particolarmente, nel rispetto dei principi dettati dalla parte speciale n. 5 *"Reati societari e corruzione tra privati"* e n. 8 *"Reati tributari"*.

Dunque, tutti i soggetti che in ragione del proprio incarico o della propria funzione sono coinvolti nella gestione del processo in oggetto devono:

- nell'ambito degli adempimenti fiscali-amministrativo-contabili della BITCONTROL S.r.l., osservare le regole di corretta, completa e trasparente esecuzione delle operazioni e registrazione delle stesse;
- assicurare che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, tracciabile, verificabile, legittima e congrua.

La procedura assicura altresì il presidio dei rischi derivanti dall'utilizzo di strumenti digitali e di intelligenza artificiale nei processi contabili e di bilancio, nonché dei nuovi rischi-presupposto 231.

2 ACRONIMI AZIENDALI

CDA	Consiglio di Amministrazione
PRES	Presidente CDA
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale – Approvvigionamento
RGAD	Responsabili Gestione Archivi e Documenti
REC	Responsabile Esterno Contabilità
SOC	Soci

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

3 RIFERIMENTI NORMATIVI DEL MODELLO

- DECRETO LEGISLATIVO 231/2001 E S.S. MM.II (DI SEGUITO ANCHE D.LGS 231/01);
- CODICE ETICO DI BITCONTROL S.R.L.

- CODICE DISCIPLINARE DI BITCONTROL S.R.L.

- MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO DI BITCONTROL S.R.L..

- REGOLAMENTO (UE) 2024/1689 (AI ACT), LEGGE 23 SETTEMBRE 2025, N. 132 E POLICY IA AZIENDALE, LIMITATAMENTE AI PROFILI DI UTILIZZO DI SISTEMI DI IA NEI PROCESSI AMMINISTRATIVO-CONTABILI;

- CODICE DI CONDOTTA AZIENDALE, PROCEDURA WHISTLEBLOWING E PROCEDURA SUI FLUSSI INFORMATIVI VERSO L'ODV;

- D.LGS. 5 NOVEMBRE 2024, N. 173, TESTO UNICO DELLE SANZIONI TRIBUTARIE AMMINISTRATIVE E PENALI, EFFICACE PER LA DISCIPLINA PENALE TRIBUTARIA DAL 1° GENNAIO 2026, E SUCCESSIVE MODIFICHE;

- D.LGS. 10 MARZO 2000, N. 74, ESCLUSIVAMENTE PER I RINVII STORICI E PER I PERIODI DI VIGENZA ANTERIORI AL 1° GENNAIO 2026.

- D.LGS. 14 GIUGNO 2024, N. 87, PER LE MODIFICHE AL SISTEMA SANZIONATORIO TRIBUTARIO, PER QUANTO ANCORA APPLICABILI E COORDINATE NEL TESTO UNICO.

4 CAMPO DI APPLICAZIONE E DESTINATARI DELLAPROCEDURA

La presente procedura si applica a tutti i soggetti coinvolti nelle attività di contabilità generale e predisposizione del bilancio della Società, con lo scopo di definire le procedure necessarie ad assicurare la prevenzione della commissione dei reati societari contemplati nell'art. 25 ter del D.Lgs. 231/2001, alla luce della modifica normativa di cui all'art. 4 del D.Lgs. 38/2017 che ha introdotto una nuova fattispecie di reato ("istigazione alla corruzione tra privati") e previsto la possibilità di comminare per alcune fattispecie illecite anche sanzioni interdittive, oltre a quelle pecuniarie già contemplate.

Dunque, tutte le Funzioni Aziendali, 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 BITCONTROL S.R.L., come ad es. il bilancio di esercizio, relazione sulla gestione, relazioni trimestrali e semestrali, ecc., sono tenute ad osservare le modalità esposte nella presente procedura, nelle previsioni di legge esistenti in materia, nonché in tutte le norme 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, tutte le Funzioni Aziendali sono tenute 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 di BITCONTROL S.R.L..

La presente procedura si applica anche alle attività di supporto esternalizzate e a tutti i soggetti che, a qualunque titolo, intervengono nei processi di rilevazione contabile, registrazione, stima,

classificazione, controllo, chiusura contabile, redazione del bilancio, note integrative, relazioni, comunicazioni sociali e fiscali, nonché alle attività propedeutiche o di supporto eventualmente svolte con strumenti digitali o con sistemi di intelligenza artificiale.

5 REATI ASTRATTAMENTE IPOTIZZABILI

Si elencano di seguito i possibili reati configurabili con riferimento alle attività sensibili individuate nella presente area a rischio:

➢ Art 2621 c.c. - False Comunicazioni Sociali

➢ Art 2621-bis c.c. – Fatti di lieve entità

➢ Art 2625 c.c. – Impedito Controllo

➢ Art. 2626 c.c. - Indebita restituzione dei conferimenti

➢ Art. 2627 c.c. - Illegale ripartizione degli utili e delle riserve

➢ Art 2628 c.c. – Illecite operazioni sulle azioni o quote sociali o della società controllante

➢ Art. 2629 c.c. - Operazioni in pregiudizio dei creditori

➢ Art. 2629 bis c.c. - ➢ fattispecie non concretamente applicabile a BitControl, in quanto società non quotata e non appartenente ai soggetti vigilati indicati dalla norma; resta fermo il presidio generale dei conflitti di interessi.

➢ Art. 2632 c.c. - Formazione fittizia del capitale

➢ Art. 2633 c.c. - indebita ripartizione dei beni sociali da parte dei liquidatori

➢ Art. 2635 c.c. – Corruzione tra privati

➢ Art. 2635 bis c.c. - istigazione alla corruzione tra privati.

➢ Art. 2636 c.c. - illecita influenza sull'assemblea

➢ Art. 2637 c.c. – Aggiotaggio

➢ Art. 2638 c.c. – ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza.

A TITOLO ESEMPLIFICATIVO SI POTREBBERO CONFIGURARE LE SEGUENTI MODALITÀ DI REALIZZAZIONE DEI REATI:

➢ modifica o alterazione dei dati contabili al fine di fornire una rappresentazione della situazione patrimoniale, economica e finanziaria della società difforme dal vero;

➢ iscrizione di poste contabili aventi ad oggetto operazioni inesistenti, sopravvalutate o sottostimate (es.: fondi per passività potenziali, fondi rischi su crediti, fondi titoli, riserve sinistri, capitalizzazione costi, costi pluriennali, altri stanziamenti per fatture da emettere o da ricevere) ovvero occultamento di fatti rilevanti tali da mutare la rappresentazione delle effettive condizioni economiche della società, rappresentazione alterata di utili e riserve distribuibili;

➢ ripartizione da parte degli amministratori di utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartizione di riserve non distribuibili per legge, indebita restituzione dei conferimenti;

➢ esposizione di dati idonei a pregiudicare i diritti dei creditori sociali, adozione di procedure che violano i diritti previsti dalla legge a favore dei creditori sociali (ad es. in caso di fusioni, scissioni, riduzioni del capitale);

➢ attribuzione di quote sociali possedute per somma inferiore al valore nominale delle stesse; sopravvalutazione dei conferimenti di beni in natura o dei crediti.

Assumono inoltre rilievo, per i riflessi che possono produrre sulla correttezza, completezza, trasparenza e veridicità delle scritture e delle comunicazioni sociali, le condotte relative a violazioni delle misure restrittive UE, impiego irregolare di cittadini di Paesi terzi, fatti ambientali rilevanti, violazioni in materia di salute e sicurezza sul lavoro anche in modalità agile, nonché uso improprio o non autorizzato di sistemi di intelligenza artificiale nei processi amministrativo-contabili.

6 I REATI SOsocietari - LE FATTISPECIE DI REATO DI CUI ALL'ART. 25-TER D.LGS. 231/2001

ART. 2621. FALSE COMUNICAZIONI SOCIALI.

"*Fuori dai casi previsti dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettono fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore, sono puniti con la pena della reclusione da uno a cinque anni. La stessa pena si applica anche se le falsità o le omissioni riguardano beni posseduti o amministrati dalla società per conto di terzi*".

Dunque, il reato di false comunicazioni sociali si configura quando si procede alla esposizione, all'interno dei bilanci, delle relazioni o delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero (ancorché oggetto di valutazione), ovvero alla mancata indicazione, nei medesimi documenti, di informazioni, la cui comunicazione è prescritta dalla legge, riguardanti la situazione economica, patrimoniale o finanziaria della società o del gruppo a cui appartiene, con modalità idonee ad indurre in errore i destinatari. Il reato si perfeziona nel momento in cui "consapevolmente" (così come recita la nuova formulazione dell'art. 2621 c.c.) siano esposti fatti non rispondenti al vero, oppure vengono omesse informazioni dovute per legge nell'ambito delle comunicazioni sociali. Soggetti attivi sono "… gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i

liquidatori …". La fattispecie di cui all'art. 2621 c.c. sanziona la condotta ivi indicata a prescindere dal verificarsi del danno.

Pertanto il reato può configurarsi nelle seguenti ipotesi:

1. **RICAVI SOVRASTIMATI** attraverso la registrazione di fatture relative ad operazioni inesistenti e ciò al fine di migliorare il risultato d'esercizio. Tale operazione costituisce una falsa rappresentazione della situazione economica della società;
2. **COSTI O PERDITE OCCULTATE** attraverso l'omessa contabilizzazione di perdite su crediti o degli accantonamenti a fondi rischi e ciò al fine di far apparire il bilancio appare artificiosamente positivo. Tale operazione si configura come una consapevole omissione di informazioni rilevanti;
3. **ATTIVITÀ PATRIMONIALI FITTIZIE** attraverso l'iscrizione in bilancio di beni o immobilizzazioni che non esistono. Tale operazione si configura come una falsa rappresentazione del patrimonio;
4. **DEBITI NON INDICATI** attraverso l'omessa indicazione di debiti verso banche, fornitori o l'erario e ciò al fine di migliorare l'indice di solvibilità. Tale operazione si configura come una comunicazione socialmente rilevante non veritiera.

PRESIDI DI CONTROLLO:

1. Chiarezza di ruoli e responsabilità per la tenuta della contabilità, per la redazione del bilancio, per l'approvazione dei documenti contabili;
2. Controlli contabili e amministrativi al fine di assicurare una contabilità aggiornata e tempestiva e supportata da documenti giustificativi;
3. Controlli su ricavi e costi mediante una verifica periodica della competenza economica e dell'esistenza delle operazioni;
4. Controlli sulle informazioni verso soci e terzi mediante la completezza delle comunicazioni sociali.

Pertanto, la Società adotta procedure e controlli idonei a garantire la veridicità, completezza e correttezza delle comunicazioni sociali, assicurando la tracciabilità delle operazioni, la segregazione delle funzioni, il controllo delle poste valutative e adeguati flussi informativi verso l'Organismo di Vigilanza.

L'ART. 25-TER INCLUDE TRA I REATI IDONEI A CONFIGURARE LA RESPONSABILITÀ DELL'ENTE ANCHE IL NUOVO ART. 2621-BIS (FATTI DI LIEVE ENTITÀ):

"*Salvo che costituiscano più grave reato, si applica la pena da sei mesi a tre anni di reclusione se i fatti di cui all'articolo 2621 sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta. Salvo che costituiscano più grave reato, si applica la stessa pena di cui al comma precedente quando i fatti di cui all'articolo 2621 riguardano società che non superano i limiti indicati dal secondo comma dell'articolo 1 del regio decreto 16 marzo 1942,*

n. 267. In tale caso, il delitto è procedibile a querela della società, dei soci, dei creditori o degli altri destinatari della comunicazione sociale."

Le sanzioni previste dall'art. 2621 c.c. sono ridotte se i fatti sono di lieve entità, tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta (art. 2621-bis c.c.). inoltre, è, prevista l'ipotesi della non punibilità dei fatti di cui agli articoli sopra citati, rimessa all'apprezzamento del giudice che valuta, a tal fine, l'entità dell'eventuale danno cagionato alla società, ai soci o ai creditori (art. 2621-ter c.c.).

Tale ipotesi può configurarsi nelle seguenti ipotesi:

1. sottovalutazione dell'importanza informativa;
2. gestione "semplificata" della nota integrativa;
3. chiusure contabili rapide;
4. pressioni sulla marginalità;
5. assenza di controlli di secondo livello.

In particolare, il rischio di commissione del reato di cui all'art. 2621-bis c.c. si configura in relazione a possibili errori, omissioni o valutazioni non corrette di lieve entità nelle comunicazioni sociali, idonee a fornire una rappresentazione non pienamente veritiera della situazione economica, patrimoniale o finanziaria della Società, in considerazione delle dimensioni e della struttura organizzativa della SRL.

PRESIDI DI CONTROLLO

- **Formalizzazione minima dei ruoli contabili** mediante l'attribuzione scritta delle responsabilità su:
    - rilevazioni contabili
    - stime di bilancio
    - predisposizione dei documenti informativi ai soci.
- Presìdi sulle comunicazioni ai soci e ai terzi mediante comunicazioni sociali improntate a prudenza, completezza e chiarezza;
- **Presìdi di controllo di secondo livello** mediante il coinvolgimento del consulente esterno;
- **Presìdi contabili e amministrativi** mediante verifiche periodiche di coerenza attraverso il confronto periodico di budget contro consuntivo, di esercizio corrente contro esercizi precedenti, nonché mediante l'analisi degli scostamenti anche se di importo contenuto.

Pertanto, la Società ha adottato presìdi di controllo proporzionati alle proprie dimensioni, idonei a prevenire errori, omissioni o valutazioni non corrette di lieve entità nelle comunicazioni sociali, assicurando la tracciabilità delle stime, la completezza dell'informativa e adeguati controlli sulle poste sensibili di bilancio.

ART. 2625. IMPEDITO CONTROLLO.

"*Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali*

sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 euro. Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa. La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58."

Tale fattispecie di reato si configura quando si ostacoli o si impedisca lo svolgimento delle attività di controllo e/o di revisione, legalmente attribuite ai soci e agli organi sociali. La condotta può essere integrata mediante l'occultamento di documenti o l'utilizzo di altri idonei artifici. La pena è aumentata qualora sia cagionato un danno ai soci. Soggetti attivi del reato sono gli amministratori. Il reato può essere commesso mediante qualsiasi condotta idonea ad ostacolare lo svolgimento delle attività di controllo riconosciute ai soci.

Ferma restando la rilevanza di qualsiasi condotta idonea a determinare l'evento sopra indicato, assumono particolare rilevanza:

- l'occultamento di documenti (ad es., dei libri sociali);
- l'adozione di altri artifici;
- l'ostruzionismo in sede di verifica e di controllo dell'assemblea (in ordine ai chiarimenti richiesti e all'esibizione di documentazione rilevante)

PRESÌDI DI CONTROLLO

- **Recepimento in procedure interne di:**
  - diritti informativi dei soci (art. 2476 c.c.)

 Esplicito divieto di:

  - ostacolo
  - ritardo ingiustificato
  - limitazione arbitraria delle informazioni

- **Convocazione tempestiva degli organi di controllo**
  - nei casi previsti dalla legge
  - su richiesta degli stessi
  - Conservazione delle evidenze di convocazione.

La Società ha adottato presìdi di controllo idonei a garantire l'effettivo esercizio dei diritti di controllo da parte dei soci e degli organi di controllo, assicurando l'accesso tempestivo e completo alle informazioni e alla documentazione societaria, nonché la tracciabilità delle richieste e delle risposte, al fine di prevenire il reato di impedito controllo ex art. 2625 c.c.

ART. 2626. INDEBITA RESTITUZIONE DEI CONFERIMENTI

"*Gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli, sono puniti con la reclusione fino ad un anno*".

Il reato si configura quando si proceda, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli. Soggetto attivo del reato è l'Amministratore Unico.

Il reato può essere commesso mediante:

- restituzione, anche simulata, dei conferimenti effettuati dai soci;
- liberazione dei soci dall'obbligo di eseguire i conferimenti.

Il reato si perfeziona con l'esecuzione di una delle condotte tipiche previste dalla norma.

PRESÌDI ORGANIZZATIVI E DI GOVERNANCE

- **Procedura per la distribuzione di utili e riserve**

- Verifica preventiva di:
  - esistenza di utili distribuibili
  - rispetto dei vincoli di legge
- Delibera assembleare formale
- Divieto di "anticipi su utili" non consentiti

Presìdi contabili e finanziari

Verifica periodica dell'integrità del capitale sociale

- Monitoraggio di:
  - patrimonio netto
  - perdite
  - riserve disponibili
- Segnalazione tempestiva di situazioni di rischio.

- **Tracciabilità delle operazioni con soci e parti correlate**

- Evidenza contabile separata per:
  - crediti verso soci
  - debiti verso soci
- Divieto di compensazioni informali.

- **Procedura per variazioni del capitale sociale**

- Rispetto rigoroso di:
  - delibere assembleari
  - tutela dei creditori

- formalità di legge

- Coinvolgimento del consulente legale/contabile.

ART. 2627. ILLEGALE RIPARTIZIONE DEGLI UTILI E DELLE RISERVE.

"*Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite, sono puniti con l'arresto fino ad un anno. La restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato*".

Tale comportamento criminoso consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite. In ogni caso, la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Soggetto attivo del reato è l'Amministratore Unico.

Il reato può essere commesso mediante:

- ripartizione di utili, o di acconti su utili, non effettivamente conseguiti o destinati per legge a riserva;

- ripartizione di riserve che per legge non possono essere distribuite.

PRESÌDI DI GOVERNANCE E AUTORIZZATIVI

➢ **Delibera assembleare obbligatoria e motivata**

- Distribuzione di utili e riserve ammessa solo previa:
  - delibera assembleare;
  - indicazione puntuale delle voci distribuite;
- Divieto di distribuzioni "di fatto" o informali.

➢ **Verifica preventiva della distribuibilità**

- Verifica documentata di:
  - utili realmente conseguiti;
  - assenza di perdite pregresse non coperte;
  - natura disponibile delle riserve.
- Supporto del consulente contabile.

➢ **Procedura di approvazione del bilancio**

- Procedura formalizzata che disciplini:
  - chiusura contabile
  - verifiche su patrimonio netto e riserve
  - proposta di destinazione dell'utile

Presìdi contabili e finanziari

- **Monitoraggio continuo del patrimonio netto**
- Controllo periodico di:
  - capitale sociale;
  - riserva legale;
  - riserve vincolate:
  - perdite.

La Società ha adottato presìdi di controllo idonei a prevenire la distribuzione, anche indiretta, di utili non realmente conseguiti o di riserve non distribuibili, assicurando il rispetto delle procedure di approvazione del bilancio, la verifica della distribuibilità e la tracciabilità delle operazioni di destinazione dell'utile.

ART. 2628. ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE

"*Gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge, sono puniti con la reclusione fino ad un anno. La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.*

Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto".

Tale fattispecie di reato si configura allorquando si proceda, fuori dei casi previsti dalla legge, all'acquisto o alla sottoscrizione di azioni o quote emesse dalla società o della controllante, così da cagionare una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge. Si precisa che, se il capitale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio riferito all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

Inoltre, si precisa che il reato potrebbe essere commesso mediante acquisto o sottoscrizione di azioni o quote emesse dalla società, fuori dai casi previsti dalla legge, così da cagionare una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Soggetti attivi del reato sono gli amministratori, ovvero i componenti del CDA.

Nel caso di specie, il citato reati si può configurare solo per le operazioni sulle quote proprie, in particolare il reato si configura quando la società:

1. LA SOCIETÀ

acquista quote di un socio uscente, utilizzando risorse che:

- intaccano il capitale sociale

- o riducono il patrimonio netto sotto i limiti di legge

2. GLI AMMINISTRATORI:

- procedono all'acquisto di quote proprie
- senza autorizzazione assembleare
- o in violazione dello statuto

3. LA SOCIETÀ:

- rimborsa il valore delle quote a un socio
- senza procedura di recesso o riduzione del capitale
- mascherando l'operazione come:
    - finanziamento
    - consulenza
    - rimborso spese
    - acquista quote proprie
    - in una fase di difficoltà finanziaria
    - riducendo le garanzie per i creditori

PRESÌDI DI GOVERNANCE E AUTORIZZATIVI

- **Delibera assembleare obbligatoria:**

- Ogni operazione su quote proprie ammessa solo previa:
    - delibera assembleare
    - verifica di conformità a statuto e legge
- Divieto di iniziative autonome degli amministratori

- **Verifica preventiva dell'integrità del capitale**

  Verifica documentata di:
    - patrimonio netto**;**
    - riserve disponibili
    - assenza di pregiudizio per i creditori

- **Divieto di utilizzo di riserve indisponibili**

  Contabilità separata tra:
    - riserve disponibili
    - riserve vincolate
    - Blocco automatico di utilizzo improprio.

La Società ha adottato presìdi di controllo idonei a prevenire il compimento di operazioni illecite sulle quote sociali proprie, assicurando che ogni operazione sia previamente autorizzata dall'assemblea, supportata da verifiche di legge e pareri qualificati, nonché tracciata e coerente con la tutela dell'integrità del capitale sociale e dei creditori

ART. 2629. OPERAZIONI IN PREGIUDIZIO DEI CREDITORI.

"*Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato.*"

La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori.

In ogni caso, il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono gli amministratori, ovvero i componenti del CDA.

La fattispecie potrebbe essere commessa qualora, in violazione delle disposizioni di legge a tutela dei creditori, sia cagionato un danno a questi ultimi mediante:

- riduzione del capitale sociale;
- realizzazione di operazioni di fusione o scissione.

PRESÌDI DI GOVERNANCE E AUTORIZZATIVI

- **Delibera assembleare rafforzata**

Ogni operazione di riduzione del capitale, fusione o scissione deve essere:

- deliberata dall'assemblea;
- adeguatamente motivata;
- verbalizzata in modo completo

- **Verifica della conformità alle norme di tutela dei creditori**

Controllo del rispetto di:

- termini per opposizione dei creditori;
- obblighi di informativa;
- eventuali garanzie richieste.

- **Presìdi contabili e finanziari**

Monitoraggio del patrimonio netto, attraverso la verifica prima e dopo l'operazione di:

- capitale sociale;
- riserve disponibili;
- perdite.

La Società ha adottato presìdi di controllo idonei a prevenire operazioni in pregiudizio dei creditori, assicurando che le operazioni di riduzione del capitale, fusione o scissione siano deliberate nel rispetto delle norme di legge, precedute da adeguate verifiche patrimoniali e dall'analisi dell'impatto sui creditori, nonché supportate da pareri qualificati e da flussi informativi verso l'Organismo di Vigilanza.

ARTICOLO 2629-BIS. OMESSA COMUNICAZIONE DEL CONFLITTO D'INTERESSI

"*L'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1 settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005, n. 209, del decreto legislativo 21 aprile 1993, n. 124, che viola gli obblighi previsti dall'articolo 2391, primo comma, è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi.*"

Il reato si configura allorquando l'amministratore ometta di comunicare la titolarità di un proprio interesse, personale o per conto di terzi, in una determinata operazione della società. La fattispecie sanziona, inoltre, la condotta dell'Amministratore Delegato/Direttore Generale che, essendo portatore di analogo interesse, ometta di astenersi dal compiere l'operazione.

Soggetti attivi del reato sono gli amministratori, ovvero i componenti del CDA.

In particolare il reato si configura quando:

1. L'amministratore stipula un contratto di fornitura con una società di cui è socio o amministratore senza comunicare il proprio interesse agli altri soci;
2. L'amministratore attribuisce a sé stesso o a un proprio familiare incarichi di consulenza senza informare formalmente la società;
3. La società acquista o prende in locazione un immobile di proprietà dell'amministratore a condizioni non di mercato senza dichiarazione del conflitto;
4. L'amministratore partecipa a una decisione nella quale ha un interesse in conflitto senza astenersi né informare;
5. L'amministratore promuove una fusione o cessione che favorisce un proprio interesse personale senza informare adeguatamente l'assemblea.

Pur non essendo la fattispecie di cui all'art. 2629-bis c.c. concretamente applicabile a BitControl, la Società presidia ogni conflitto di interessi mediante dichiarazione preventiva, astensione del soggetto interessato, motivazione della decisione, verifica della congruità economica dell'operazione, tracciabilità documentale e informativa all'OdV nei casi rilevanti.

ART. 2632. FORMAZIONE FITTIZIA DEL CAPITALE.

"*Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono puniti con la reclusione fino ad un anno.*"

La fattispecie di reato si realizza quando si procede alla formazione o all'aumento in modo fittizio del capitale sociale mediante:

• attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale;

• sottoscrizione reciproca di azioni o quote;

• sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori, ovvero i componenti del CDA e i soci conferenti.

Tale ipotesi di reato è integrata dalla condotta di formazione o aumento, in modo fittizio, del capitale sociale, effettuata mediante:

- attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale;
- sottoscrizione reciproca di azioni o quote;
- sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

In particolare il citato reato si configura quando:

1. viene formato o aumentato il capitale sociale mediante conferimenti fittizi, sopravvalutazione dei conferimenti in natura, compensazioni non consentite con apparente rispetto formale delle regole ma con capitale solo nominale, non reale, idoneo a trarre in inganno i creditori.
2. Conferimenti in denaro mai effettivamente versati;
3. Conferimenti in natura (es. macchinari, software, marchi)sopravvalutati;
4. Compensazione illegittima del conferimento (con crediti inesistenti, crediti non liquidi o non esigibili in violazione delle regole sui conferimenti);
5. Operazioni simulate di aumento di capitale;
6. Utilizzo di riserve indisponibili come capitale.

La Società ha adottato presìdi di controllo idonei a garantire che la formazione e gli aumenti del capitale sociale avvengano esclusivamente mediante conferimenti reali ed effettivi, correttamente valutati e tracciati, nel rispetto delle norme di legge e a tutela dei creditori, al fine di prevenire il reato di cui all'art. 2632 c.c.

ART. 2633. INDEBITA RIPARTIZIONE DEI BENI SOCIALI DA PARTE DEI LIQUIDATORI

"*I liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Il risarcimento del danno ai creditori prima del giudizio estingue il reato*".

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Soggetti attivi del reato sono i liquidatori.

La fattispecie è integrata nel caso in cui, durante la fase della liquidazione, i liquidatori cagionano un danno ai creditori sociali mediante la ripartizione dei beni sociali tra i soci:

- prima del pagamento dei creditori sociali;
- prima dell'accantonamento delle somme necessarie a soddisfarli.

Il rischio di commissione del reato di indebita ripartizione dei beni sociali da parte dei liquidatori ex art. 2633 c.c. si configura in relazione a operazioni di distribuzione, anche anticipata, di beni o somme ai soci effettuate prima dell'integrale soddisfacimento dei creditori sociali o senza l'accantonamento delle passività certe e potenziali, con conseguente pregiudizio per i creditori.

ART. 2635. CORRUZIONE TRA PRIVATI.

"*Salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società, sono puniti con la reclusione da uno a tre anni.*

Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma.

Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.

Le pene stabilite nei commi precedenti sono raddoppiate se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 del testo unico delle disposizioni in materia di intermediazione finanziaria, di cui al decreto legislativo 24 febbraio 1998, n. 58, e successive modificazioni.

Si procede a querela della persona offesa, salvo che dal fatto derivi una distorsione della concorrenza nella acquisizione di beni o servizi".

Il comportamento illecito consiste, dal lato passivo, nell'accettare denaro o altra utilità per sé o altri (o la relativa promessa) per compiere od omettere atti in violazione degli obblighi inerenti l'ufficio o degli obblighi di fedeltà, che comportino un nocumento per la società.
Quanto agli obblighi violati questi possono avere fonte legislativa (codice civile artt. 2390-2392 c.c. per gli amministratori), o anche extra-codicistica (i.e. ambiente, sicurezza sul lavoro, etc.), o non legislativa (i.e. provvedimenti di autorità di vigilanza, etc.).
Quanto agli obblighi di fedeltà si fa riferimento agli obblighi collegati ai principi di correttezza e buona fede di cui agli artt. 1175, 1375 e 2105 del codice civile.
Dal lato attivo ("corruttore") la condotta consiste nell'offrire o promettere danaro o qualsiasi altra utilità (favori, assunzione di personale, offerta di contratti di consulenza ecc..).
I soggetti attivi del reato, dal lato passivo, possono essere gli "apicali" (amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori), ma anche i sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati (quindi i dipendenti ma anche i collaboratori esterni come agenti, concessionari, etc.). Il corruttore può essere chiunque.
Si precisa altresì che è importante evidenziare che il bene giuridico che la fattispecie mira a tutelare è il patrimonio sociale. In particolare, si rileva che l'estraneità dell'atto ai doveri sociali oggetto di scambio non rileva di per sé, ma in quanto comporti un nocumento alla società, che conserva nella maggior parte dei casi il potere di decidere se i comportamenti corruttivi debbano o meno essere puniti.
Inoltre, si segnala che, ai fini della responsabilità amministrativa, può essere sanzionato solo l'ente cui appartiene il "corruttore" (l'unico che può essere avvantaggiato dalla condotta corruttiva), mentre la società di riferimento del corrotto, essendo danneggiata dalla condotta delittuosa, non sarà punibile ex Decreto.
Infatti, a titolo di esempio il reato potrebbe realizzarsi qualora il dipendente di una società offra omaggi o danaro all'amministratore di un'altra società che ha indetto una gara o sta svolgendo una trattativa privata per una fornitura, al fine di indurre l'amministratore della società che ha indetto la gara/trattativa a violare le procedure dell'azienda che regolano lo svolgimento o l'aggiudicazione per avvantaggiare la società del corruttore, concludendo un contratto svantaggioso per la società.

In relazione al reato di corruzione tra privati, la Società rinvia integralmente alla Procedura speciale PMOG15 "Gestione e prevenzione dei reati di corruzione", che disciplina i principi di comportamento, i presìdi di controllo e i flussi informativi idonei a prevenire la commissione del reato.

ART. 2635 BIS. ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI.

"*Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo.*

La pena di cui al primo comma si applica agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi attività lavorativa con l'esercizio di funzioni direttive, che sollecitano per sé o per altri, anche per interposta persona, una promessa o dazione di denaro o di altra utilità, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, qualora la sollecitazione non sia accettata.

Si procede a querela della persona offesa".

La norma, inserita dall'art. 4 del D.Lgs. 15.03.2017, n. 38 (in vigore dal 14.04.2017), introduce la fattispecie dell'istigazione alla corruzione tra privati.

Si rileva che, sotto il profilo attivo, la condotta sanzionabile penalmente in capo a chiunque consiste nell'offrire o promettere denaro o altre utilità non dovuti ad uno dei soggetti interni elencati al fine del compimento o dell'omissione di atti in violazione degli obblighi inerenti il proprio ufficio o degli obblighi di fedeltà, qualora l'offerta o la promessa non sia accettata (art. 2635-bis, comma 1, c.c.). Sotto il profilo passivo, di contro, è prevista la punibilità del soggetto interno che solleciti una promessa o dazione di denaro o altra utilità, al fine del compimento o dell'omissione di atti in violazione dei medesimi obblighi, qualora tale proposta non sia accettata (art. 2635-bis, comma 2, c.c.). Tale norma incriminatrice ha essenzialmente la finalità di evitare che rimangano impuniti i comportamenti di offerta non accettata (dal lato attivo) e di sollecitazione non accolta (dal lato passivo), che erano privi in precedenza di sanzione penale. Il momento consumativo, essendo la condotta di natura istantanea, coincide, in entrambe le fattispecie, con la formulazione dell'offerta, da un lato, o con la formulazione della sollecitazione, dall'altro.

PRINCIPALI AREE A RISCHIO E ATTIVITÀ SENSIBILI INTERESSATE PER GLI ARTICOLI 2635 C.C. E 2635-BIS C.C.

- Adozione del Sistema di Gestione UNI ISO 37001:2025: eludere e/o manipolare il Sistema di Gestione (es. occultare una segnalazione o inibire lo svolgimento delle indagini o manipolare l'attività di formazione)
- Adozione e gestione del sistema disciplinare e di meccanismi sanzionatori: eludere misure disciplinari o sanzionatorie
- Gestione delle attività di ricerca del personale: formulare criteri ad hoc per favorire una determinata candidatura o persona
- Definizione delle politiche di valutazione del personale e sviluppo di carriera: definizione delle politiche di valutazione del personale e sviluppo di carriera per favorire alcune persone
- Attribuzione di ruoli, compiti e responsabilità e gestione dei flussi informativi: favorire l'attribuzione di un ruolo, compiti o responsabilità ad un determinato dipendente
- Gestione delle attività di formazione e sviluppo delle competenze del personale: manipolare l'informazione o la formazione nei confronti dei dipendenti a fini speculativi
- Rilascio, revoca e gestione dei poteri di firma e autorizzativi: assegnare poteri di firma o autorizzativi ad organi aziendali o soci in affari non appropriati
- Formalizzazione degli incarichi di consulenza conferiti: escludere o penalizzare determinate offerte di consulenza o favorire determinate offerte
- Monitoraggio dei servizi di consulenza: sovrastimare o falsare la valutazione del professionista
- Gestione omaggi, spese di attenzione verso i terzi: ottenere un indebito vantaggio dalla concessione di un omaggio
- Gestione sponsorizzazioni ed erogazioni liberali: ottenere un indebito vantaggio dalla concessione di sponsorizzazioni e erogazioni liberali.

In relazione al reato di Istigazione alla corruzione tra privati, la Società rinvia integralmente alla Procedura speciale PMOG15 “Gestione e prevenzione dei reati di corruzione”, che disciplina i principi di comportamento, i presìdi di controllo e i flussi informativi idonei a prevenire la commissione del reato.

ART. 2636. ILLECITA INFLUENZA SULL'ASSEMBLEA.

“*Chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto, è punito con la reclusione da sei mesi a tre anni*”.

Tale ipotesi di reato in esame tende a tutelare che la volontà dell’organo deliberativo della società sia espressa attraverso l’esercizio di voti validi e nel rispetto della regola di maggioranza (o principio maggioritario). Soggetto attivo può essere «chiunque» e, quindi, anche un soggetto non socio ed estraneo alla società. Il reato si perfeziona nel momento in cui, a seguito di atti simulati o fraudolenti, si determina fittiziamente la maggioranza assembleare idonea ad adottare una o più

delibere. Vale precisare, peraltro, che il reato non si configura se la delibera sarebbe stata comunque adottata dall'assemblea anche in mancanza della maggioranza "fraudolentemente orientata" (al fine di accertare tale ultima circostanza è necessario procedere alla c.d. "prova di resistenza" che consiste nel verificare se, sottraendo i voti espressi in virtù degli atti simulati o fraudolenti, la delibera raggiunge comunque le maggioranze prescritte per la sua regolare adozione).
Il rischio di commissione del reato di illecita influenza sull'assemblea ex art. 2636 c.c. si configura in relazione a condotte fraudolente o simulatorie idonee a determinare artificiosamente la maggioranza assembleare, alterando la libera formazione della volontà dei soci e conseguendo un vantaggio ingiusto.

ART. 2637. AGGIOTAGGIO - MODIFICATO DA LEGGE N.32 DEL 23 SETTEMBRE 2025)

La configurazione di tale reato prevede che 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.
Si precisa che, 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.
Il reato si configura allorquando si proceda alla diffusione di notizie false ovvero alla realizzazione di operazioni simulate o ad altri artifici, idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari ovvero a incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.
La condotta deve avere ad oggetto strumenti finanziari non quotati o per i quali non è stata presentata domanda di ammissione alla negoziazione in un mercato regolamentato.
Il reato si potrebbe configurare anche nel caso in cui l'azienda diffonde al mercato la notizia del mancato rilascio da parte societaria di una polizza fideiussoria richiesta nell'ambito di un'operazione avente ad oggetto il trasferimento di azioni di una società non quotata. A causa di tale comunicazione il potenziale acquirente rinuncia a concludere il contratto di compravendita dei suddetti titoli
Soggetto attivo del reato può essere chiunque.

LA CONDOTTA PENALMENTE SANZIONATA PUÒ ESSERE INTEGRATA MEDIANTE:
- diffusione di notizie false;
- realizzazione di operazioni simulate (ad es., compravendita di azioni o altri strumenti con mutamento soltanto apparente della proprietà degli stessi);
- compimento di altri artifici (ad es., diffusione di una serie di comunicazioni idonee ad ingenerare il convincimento circa la realizzazione di operazioni straordinarie).

LE ATTIVITÀ INDICATE DEVONO ESSERE CONCRETAMENTE IDONEE:
- a determinare 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);
- ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari.

Con la modifica del 2025 il reato di aggiotaggio si configura anche per le società non quotate tutelando l'affidamento economico dei terzi, configurandosi nelle seguenti ipotesi:

1. Falsi annunci per attrarre investitori;
2. Comunicazioni fuorvianti verso banche o finanziatori;
3. Operazioni simulate per aumentare il valore aziendale;
4. Manipolazione in operazioni di aumento di capitale;
5. Comunicazioni fuorvianti tramite canali digitali;
6. Occultamento di perdite.

La Società ha adottato presìdi di controllo idonei a prevenire il reato di agiotaggio, assicurando la veridicità, completezza e coerenza delle informazioni economico-finanziarie diffuse all'esterno, nonché il divieto di operazioni simulate o artificiose idonee ad alterare l'affidamento di investitori, finanziatori o altri operatori economici.

L'incremento di pena in caso di utilizzo di sistemi di intelligenza artificiale impone che gli output generati da strumenti di IA, ove impiegati in attività di supporto a relazioni, comunicazioni societarie, dati economico-finanziari o altre informazioni rilevanti verso terzi, non possano essere utilizzati senza controllo umano, validazione del soggetto competente e conservazione delle evidenze della verifica effettuata.

ART. 2638. OSTACOLO ALL'ESERCIZIO DELLE FUNZIONI DELLE AUTORITÀ PUBBLICHE DI VIGILANZA.

"*Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi. Sono puniti con la stessa pena gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne*

ostacolano le funzioni. La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58".

La condotta tipica è quella dell'impedito e/o ostacolato controllo cd. "esterno" (ossia il controllo svolto dalle autorità pubbliche di vigilanza), non anche il controllo cd. "interno" (ossia quello esercitato da organi interni alla compagine sociale). La condotta criminosa si realizza attraverso l'esposizione nelle comunicazioni alle autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

Soggetti attivi del reato possono essere gli amministratori, ovvero i componenti del CDA e coloro che sono preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società sottoposte per legge alle autorità pubbliche di vigilanza.

Il reato in questione può essere realizzato attraverso due distinte modalità, entrambe finalizzate ad ostacolare l'attività di vigilanza delle Autorità Pubbliche preposte:

- la comunicazione alle Autorità Pubbliche di Vigilanza di fatti non rispondenti al vero, sulla situazione economica, patrimoniale o finanziaria, ovvero con l'occultamento di fatti che avrebbero dovuto essere comunicati;
- l'ostacolo all'esercizio delle funzioni di vigilanza svolte da Pubbliche Autorità, attuato consapevolmente ed in qualsiasi modo, anche omettendo le comunicazioni dovute alle medesime Autorità.

In particolare il reato si configura nell'ipotesi di:

1. Comunicazioni non veritiere all'Autorità;
2. Omissione di informazioni rilevanti;
3. Ritardi intenzionali nelle risposte;
4. Esibizione parziale o selettiva della documentazione;
5. Manipolazione o distruzione di documenti;
6. Fornire una rappresentazione fuorviante della realtà aziendale;
7. Interferenze durante ispezioni o controlli.

Il rischio di commissione del reato di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza ex art. 2638 c.c. si configura in relazione a condotte volte a impedire, ostacolare o condizionare l'attività di vigilanza mediante comunicazioni non veritiere, omissioni informative, ritardi ingiustificati o limitazioni nell'accesso alle informazioni e alla documentazione.

Nelle comunicazioni verso autorità pubbliche di vigilanza, organi di controllo o soggetti terzi qualificati, è vietato recepire automaticamente dati, elaborazioni o output provenienti da sistemi

automatizzati o di IA senza previa verifica di coerenza, completezza e attendibilità da parte della funzione competente

6 RESPONSABILE DELLA PROCEDURA

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*.

I ruoli, le deleghe, gli accessi ai sistemi, i livelli autorizzativi e le responsabilità nelle attività contabili e di bilancio devono essere formalizzati e mantenuti aggiornati anche a seguito di nuove assunzioni, mutamenti organizzativi o introduzione di strumenti digitali e di IA a supporto dei processi.

Qualora nei processi contabili o di predisposizione del bilancio siano utilizzati strumenti di IA, devono essere distinti il soggetto utilizzatore dello strumento, il soggetto revisore dell'output e il soggetto responsabile della validazione finale, fermo restando che la responsabilità dell'atto o documento finale rimane integralmente in capo al soggetto umano competente.

7 INDICAZIONI COMPORTAMENTALI

L'obbligo di osservare i principi di comportamento qui di seguito indicati, sussiste sia nel caso in cui la contabilità sia tenuta internamente, sia nel caso in cui sia affidata a professionisti esterni.

Ai suddetti soggetti è fatto divieto di porre in essere, concorrere o dare causa alla realizzazione di comportamenti tali che, considerati individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra elencate (art. 25 ter del D. Lgs. 231/2001); è altresì proibita la violazione dei principi e delle procedure aziendali previste nella presente Parte Speciale.

Conformemente a quanto previsto dal Codice Etico e dalle altre procedure aziendali, i soggetti sopra individuati dovranno:

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) fornire informazioni complete, trasparenti, comprensibili ed accurate;

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

d) assicurarsi che per ogni operazione sia conservata agli atti un'adeguata documentazione di supporto dell'attività svolta in modo da consentire l'agevole registrazione contabile, l'individuazione dei diversi livelli di responsabilità e la ricostruzione accurata dell'operazione;

e) 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;
f) 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.
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 predisposizione del Bilancio.
g) Integrare i presìdi già esistenti su manuale contabile / controlli / dichiarazioni con:
dati, prospetti o elaborazioni provenienti da consulenti esterni, provider software, sistemi automatizzati o strumenti di IA non possono essere recepiti automaticamente nei processi di bilancio, ma devono essere sottoposti a verifica di coerenza, completezza, attendibilità e conformità normativa da parte della funzione competente.

Il presidio IA:

L'utilizzo di sistemi di intelligenza artificiale nelle attività di contabilità, analisi, riconciliazione, predisposizione di bozze, classificazione documentale, supporto informativo, redazione di relazioni o altra attività connessa alla predisposizione del bilancio è consentito esclusivamente nei limiti della Policy IA aziendale, del Codice Etico, del GDPR, del Regolamento UE 2024/1689 e della presente procedura.
È vietato utilizzare strumenti di IA non approvati, account personali o piattaforme esterne non autorizzate per attività che coinvolgano dati o documenti contabili, fiscali, societari o comunque rilevanti ai fini del bilancio.
È vietato inserire in strumenti di IA dati personali non anonimizzati, categorie particolari di dati, credenziali, dati fiscali individuali, bozze di bilancio, documentazione sensibile o altre informazioni classificate come riservate o confidenziali.
Ogni output generato da sistemi di IA destinato a confluire, anche indirettamente, in scritture, stime, analisi, prospetti, relazioni o documentazione di supporto al bilancio deve essere sottoposto a controllo preventivo di accuratezza, pertinenza, coerenza normativa e tecnica, nonché a controllo successivo sulla corretta incorporazione nel documento finale.
Qualora sia autorizzato l'uso dell'IA, devono essere conservate evidenze idonee a ricostruire finalità d'uso, strumento impiegato, soggetto utilizzatore, output rilevanti, eventuali modifiche umane, verifiche svolte e soggetto validatore.

7.1 LA TENUTA DELLA CONTABILITÀ INTERNA O PRESSO UN CONSULENTE

Nel caso in cui la Società affidi la tenuta della contabilità a professionisti esterni, la stessa dovrà conferire mandato con apposito contratto o lettera di incarico professionale contenente specifiche clausole relative alla necessaria osservanza dei principi di cui al Modello e al Codice Etico.

In tale ambito, sarà necessario garantire che l'attività di registrazione dei dati contabili sia svolta in aderenza agli obblighi di legge ed ai principi contabili nazionali e sia finalizzata ad assicurare la correttezza e l'affidabilità delle registrazioni contabili e dei *report* gestionali, nonché il tempestivo adempimento di tutti gli obblighi previsti dalle vigenti disposizioni di legge.
Tutte le comunicazioni contabili e societarie, incluse scritture, prospetti, bilanci, note, relazioni, stime, documentazione di supporto e dati trasmessi a consulenti, revisori, organi sociali o autorità, devono essere veritiere, complete, accurate, coerenti, documentate e non fuorvianti.
È fatto assoluto divieto di falsificare, alterare, omettere, occultare, distruggere o ritardare dati, scritture, rendiconti, evidenze, documenti contabili, fiscali o societari, nonché di rappresentare fatti non veri o di omettere informazioni la cui comunicazione è imposta dalla legge, dai principi contabili, dal Modello 231 o dalle procedure aziendali.
Ogni operazione, registrazione, valutazione, rettifica, storno, stima, riconciliazione o approvazione rilevante ai fini del bilancio deve essere adeguatamente documentata, tracciabile, verificabile ex post e riconducibile al soggetto che l'ha effettuata, verificata o autorizzata.

7.2 PROTOCOLLI DI PREVENZIONE E PRESIDI 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.
BITCONTROL S.R.L. si impegna ad adottare ed implementare i protocolli aziendali di prevenzione, che:

- ✓ determinino con chiarezza e completezza i dati che ciascuna funzione deve fornire per la redazione del bilancio e delle dichiarazioni tributarie e fiscali;
- ✓ prevedano la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema (anche informatico) che consenta di tracciare i singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema;
- ✓ prevedano l'adozione di un manuale operativo contabile (o altro idoneo documento), nel quale vengano individuati compiti e responsabilità di ciascuna funzione, sia assicurata la separazione delle funzioni coinvolte, e venga previsto un sistema di controllo che garantisca, per quanto possibile, la correttezza e la veridicità delle informazioni e dei dati forniti e la certezza della provenienza degli stessi dal responsabile di ciascuna funzione;
- ✓ prevedano la messa a disposizione di tutti i componenti del Consiglio di Amministrazione con congruo anticipo rispetto alla riunione programmata, della bozza di bilancio;
- ✓ ogni operazione sia sottoposta ed approvata dal Consiglio di amministrazione delle società interessate all'operazione straordinaria;

- ✓ prevedano la predisposizione di 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;
- ✓ verificare, 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: (1) garantisca un regime di trasparenza dell'informazione societaria compatibile con il regime di trasparenza in materia garantito dagli Stati dell'Unione Europea;
  (2) non sia presente nell'elenco dei Paesi a regime fiscale privilegiato (c.d. "black list");
- ✓ definire le ragioni di natura o dei crediti imprenditoriali che giustifichino le operazioni intraprese in tutte le 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.
- ✓ Verificare, preliminarmente, da parte della funzione aziendale competente, la completezza, inerenza e correttezza della documentazione di supporto dell'operazione, ai fini della registrazione contabile;
- ✓ Prevedere, in caso di operazioni straordinarie, anche attraverso il supporto di eventuali Advisor specialistici, l'avvio di attività di Due Diligence sull'oggetto della compravendita.

La *due diligence* è un processo finalizzato ad indagare ed accertare i contenuti di una attività di impresa al fine di permettere una valutazione, in particolar modo di natura economica, dell'attività stessa.

In linea di massima si può affermare che la principale finalità della *due diligence* è quella di accertare attraverso una raccolta mirata ed analitica di informazioni se vi siano le effettive condizioni di fattibilità dell'operazione programmata ovvero se sussistano elementi e profili di criticità che possano comprometterne il buon esito (ad esempio, l'adeguatezza dei fondi appostati in bilancio in relazione a determinati rischi), costruendo al contempo una solida base per l'eventuale negoziazione delle condizioni contrattuali dell'operazione.

Naturalmente i risultati della *due diligence* non impediscono al compratore di richiedere garanzie e conseguentemente ampliare la sfera di responsabilità del venditore anche rispetto a passività non emerse o non contemplate nell'ambito di detto processo di indagine.

Gli obiettivi della due diligence possono essere molteplici: vagliare possibili operazioni di acquisizione di partecipazioni, totalitarie, di maggioranza ovvero integranti una minoranza qualificata, oppure valutare la fattibilità di operazioni straordinarie (ad esempio fusioni o scissioni), o considerare l'opportunità di aderire ad una quotazione in borsa o ancora ad un aumento di capitale.

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.

Il CDA ha il dovere di vigilare sull'intero procedimento che porta alla formazione del bilancio.

In generale, l'intera procedura si basa sui seguenti presidi:

1. identificazione e monitoraggio dei dati e delle notizie ricevute dal RAM/RRU e dal REC ai fini della predisposizione del bilancio;
2. i documenti analizzati devono essere caricati e tenuti in apposito archivio informatico all'uopo predisposto nella piattaforma digitale di condivisione;
3. effettuazione, a campione, di un controllo sulla correttezza delle registrazioni contabili, eseguite dalle funzioni preposte;
4. applicazione dei principi di trasparenza e veridicità nei controlli effettuati dall'CDA;
5. svolgimento, precedentemente all'assemblea per l'approvazione del bilancio, di una o più riunioni tra 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.

Qualora dal processo di tenuta della contabilità e dalla redazione del Bilancio risultino voci/movimenti non giustificati – ad esempio *"sopravvenienze attive apparentemente non giustificate"* o casi "*di registrazioni di incassi (e pagamenti)"* di cui non si riscontri una contropartita di credito (o debito) corrispondente, sarà necessario comunicarli all'OdV con apposita segnalazione.

7.1.2 PRESIDI SPECIFICI DI BITCONTROL

A) CICLO ATTIVO E COMMESSE: ogni fattura deve essere riconciliata con contratto/ordine, SAL, verbale di collaudo o altra evidenza della prestazione; per le commesse pluriennali il RAM/RRU e il responsabile di commessa verificano avanzamento, competenza economica, ricavi da fatturare e fatture da emettere.

B) CICLO PASSIVO: l'anagrafica fornitore è soggetta a verifica preventiva; ogni pagamento richiede corrispondenza tra ordine o incarico, documento di trasporto/attestazione del servizio, fattura e autorizzazione. Le variazioni di IBAN devono essere validate mediante canale indipendente.

C) SEGREGAZIONE DEI COMPITI: chi dispone o autorizza l'acquisto non può, da solo, creare/modificare l'anagrafica, registrare la fattura e autorizzare il pagamento. Le eccezioni, dovute alle dimensioni organizzative, sono documentate e compensate da un controllo successivo del PRES.

D) TESORERIA: pagamenti e incassi avvengono su conti intestati alla Società; sono vietati conti personali, pagamenti frazionati artificiosamente e utilizzo non documentato di contanti. Le riconciliazioni bancarie sono eseguite almeno mensilmente e riesaminate dal RAM/RRU.

E) IMPOSTE E DICHIARAZIONI: il REC predispone un calendario fiscale condiviso; F24, liquidazioni IVA, dichiarazioni e compensazioni sono sottoposti a controllo documentato del RAM/RRU e all'autorizzazione del PRES. Ogni credito utilizzato in compensazione deve essere supportato da fascicolo probatorio e verifica di spettanza.

F) CREDITI D'IMPOSTA, CONTRIBUTI E AGEVOLAZIONI: è istituito un fascicolo per ciascuna misura, contenente presupposti, calcoli, certificazioni, perizie, documenti di spesa, pagamenti tracciabili, dichiarazioni e controlli sull'assenza di doppio finanziamento.

G) CESPITI E IMMOBILIZZAZIONI IMMATERIALI: acquisti di hardware, licenze, software sviluppato internamente e costi di sviluppo sono capitalizzati solo previa verifica dei requisiti contabili, dell'effettiva utilità pluriennale e della documentazione tecnica; inventario e dismissioni sono periodicamente riconciliati.

H) COSTI DI TRASFERTA E DI COMMESSA: note spese, timesheet, trasferte e costi riaddebitabili sono verificati rispetto a incarico, commessa, giustificativi e policy aziendali; sono vietati documenti duplicati, alterati o non inerenti.

I) PARTI CORRELATE E CONFLITTI DI INTERESSI: operazioni con soci, amministratori, familiari o imprese collegate richiedono dichiarazione del conflitto, verifica di congruità, motivazione e approvazione dell'organo competente.

L) OPERAZIONI ESTERE: per clienti, fornitori e partner esteri sono svolti controlli su titolarità effettiva, Paese, coordinate bancarie, coerenza economica, fiscalità applicabile e misure restrittive; le anomalie bloccano l'operazione sino alla verifica.

M) SISTEMI INFORMATIVI: accessi ai gestionali contabili e bancari sono nominativi, profilati e riesaminati periodicamente; sono attivi backup, conservazione dei log, gestione delle modifiche e divieto di utenze condivise, in coordinamento con il sistema ISO/IEC 27001.

N) INTELLIGENZA ARTIFICIALE: l'IA non può sostituire la valutazione del RAM/RRU, del REC, del PRES o del CDA; è vietato inserire dati riservati in strumenti non autorizzati. Ogni output utilizzato per bilancio, fiscalità o reporting deve essere verificato integralmente, validato e conservato con evidenza dello strumento e del revisore umano.

O) CHIUSURE PERIODICHE: sono effettuate riconciliazioni almeno trimestrali di banche, clienti, fornitori, IVA, ritenute, cespiti, ratei/risconti, fondi rischi, magazzino ove presente e lavori in corso/commesse; gli scostamenti rilevanti sono motivati e approvati.

P) REPORTING ALL'ODV: sono comunicati senza ritardo rilievi del REC, contestazioni fiscali, ravvedimenti significativi, ritardi o omissioni nei versamenti, utilizzi anomali di crediti, operazioni

con parti correlate, modifiche ai poteri bancari, incidenti informatici e violazioni della presente procedura.

7.2 LA FORMAZIONE DEI DIPENDENTI

I dipendenti coinvolti nella redazione del bilancio devono, previamente, seguire dei corsi di formazione, organizzati all'uopo dal PRES e/o RAM/RRU, in ordine alle principali nozioni e problematiche giuridiche e contabili del bilancio.

7.3 CONTROLLO DEI BILANCI INFRANNUALI

Il REC, previo confronto con il RAM/RRU, dovrà fornire, con cadenza trimestrale, al PRES le liquidazioni periodiche IVA, caricandole nell'apposito archivio informatico all'uopo predisposto nella piattaforma digitale di condivisione.

Le predette dichiarazioni dovranno essere controllate e vistate, con firma digitale o con firma olografa, per presa visione, salvo che non emergano difformità che dovranno essere tempestivamente comunicate all'OdV.

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.

7.4 DICHIARAZIONI DI VERIDICITÀ SUL BILANCIO

Le funzioni coinvolte nel processo di formazione del bilancio, nonché nelle altre comunicazioni/dichiarazioni fiscali-amministrativo-contabili obbligatorie, sono tenute ad operare nel rispetto dei principi di trasparenza, veridicità e completezza dei dati e dei documenti in possesso della Società.

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. Le attestazioni di veridicità e completezza già previste dalla procedura devono estendersi anche all'eventuale utilizzo di strumenti di IA o di altri sistemi di supporto automatizzato, dichiarando se essi siano stati utilizzati e confermando l'avvenuta validazione umana degli output.

7.5 LA DISTRIBUZIONE DI DIVIDENDI E L'EFFETTUAZIONE DI 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.*).
Nelle operazioni straordinarie e nei flussi amministrativo-contabili connessi devono essere previste verifiche proporzionate sulla regolarità e tracciabilità delle controparti, dei flussi finanziari e delle eventuali operazioni internazionali o con soggetti esteri, al fine di prevenire la rappresentazione in bilancio di rapporti, crediti, debiti, ricavi, costi o transazioni affetti da irregolarità o divieti normativi, incluse le misure restrittive dell'Unione europea.
Le verifiche devono riguardare, ove pertinenti, beneficiario effettivo, intermediari impiegati, documentazione commerciale, natura dell'operazione, autorizzazioni eventualmente richieste, coerenza dei flussi finanziari e presenza di anomalie meritevoli di segnalazione interna.

7.6 MANCATO PAGAMENTO DI IMPOSTE

Nel caso di mancato pagamento di imposte, il PRES deve verificare, annualmente, ai sensi del D.Lgs. 74/2000, 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:

- 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;

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

È fatto, inoltre, espresso divieto alle funzioni incaricate di indicare, nella documentazione presentata nell'ambito di contenziosi fiscali, elementi attivi o passivi diversi da quelli reali.
In ogni caso, l'OdV deve essere, tempestivamente, informato di tutti i contenziosi della Società con l'Erario.

8 I REATI TRIBUTARI – ATTIVITA' SENSIBILI

La disciplina dei reati tributari, che la 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.
In ultimo, si osserva che la normativa in materia è stata 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 BitControl S.r.l. i seguenti reati:
Ai fini dell'art. 25-quinquiesdecies D.Lgs. 231/2001, sono rilevanti in via ordinaria i delitti di dichiarazione fraudolenta mediante fatture o altri documenti, dichiarazione fraudolenta mediante altri artifici, emissione di fatture per operazioni inesistenti, occultamento o distruzione di documenti contabili e sottrazione fraudolenta al pagamento di imposte. Dichiarazione infedele, omessa dichiarazione e indebita compensazione rilevano per l'ente nei casi di sistemi fraudolenti transfrontalieri con evasione IVA complessiva non inferiore alla soglia prevista dalla legge.

DICHIARAZIONE FRAUDOLENTA MEDIANTE FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 74 D.LGS. 173/2024; GIÀ ART. 2 D.LGS. 74/2000)

Il reato di cui all'art. 2 commi 1, 2 e 2-bis del D. Lgs. 74/2000, si realizza con la condotta di chi, al fine di evadere le imposte sui redditi o sul valore aggiunto, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti. 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.

DICHIARAZIONE FRAUDOLENTA MEDIANTE ALTRI ARTIFICI (ART. 75 D.LGS. 173/2024; GIÀ ART. 3 D.LGS. 74/2000)

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.

Orbene, la fattispecie in esame potrebbe realizzarsi nel caso in cui venissero esposti dei crediti di imposta, ritenute d'acconto, compensazioni, rimborsi e/o detrazioni non spettanti o comunque 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. 76 D.LGS. 173/2024; GIÀ ART. 4 D.LGS. 74/2000)

Il reato di cui all'art. 4 del D.Lgs. 74/2000 si realizza con la condotta di chi, fuori dei casi previsti dagli articoli 2 e 3, 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 o elementi passivi inesistenti, quando l'imposta evasa è superiore ad euro 100.000,00 e l'ammontare complessivo degli elementi attivi sottratti all'imposizione – anche mediante indicazione di elementi passivi inesistenti - è superiore al 10% dell'ammontare complessivo degli elementi attivi indicati in dichiarazione o, comunque, è superiore ad euro 2 milioni. In forza dell'aggiunta del comma 1-bis all'art. 25-quinquiesdecies del D. Lgs. 231 del 2001 ad opera dall'art. 5, comma 1, lett. c), n. 1), D. Lgs. 75/2020, la responsabilità dell'ente risulta limitata ai fatti di dichiarazione infedele commessi nell'ambito di sistemi fraudolenti transnazionali e diretti ad evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore ad euro 10 milioni.

OMESSA DICHIARAZIONE (ART. 77 D.LGS. 173/2024; GIÀ ART. 5 D.LGS. 74/2000)

Il reato di cui all'art. 5 del D. Lgs. 74/2000 si realizza con la condotta di chi, 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 ad euro cinquantamila. Il comma 1-bis punisce la condotta di chi non presenta, essendovi obbligato, la dichiarazione di sostituto di imposta. In forza dell'aggiunta del comma 1-bis all'art. 25-quinquiesdecies del D. Lgs. 231 del 2001 ad opera dall'art. 5, comma 1, lett. c), n. 1), D. Lgs. 75/2020, la responsabilità dell'ente risulta limitata ai fatti di omessa dichiarazione commessi nell'ambito di sistemi fraudolenti transnazionali e diretti ad evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore ad euro 10 milioni.

EMISSIONE DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 79 D.LGS. 173/2024; GIÀ 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. 81 D.LGS. 173/2024; GIÀ ART. 10 D.LGS. 74/2000)

Il reato di cui all'art. 10 D. Lgs 74/2000 si realizza con la condotta di chi, 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.

SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DI IMPOSTE (ART. 85 DEL D.LGS. 173/2024; GIÀ ART. 11 D.LGS. 74/2000)

Il reato di cui all'art. 11 comma 1 e 2 D. Lgs 74/2000, che si realizza con la condotta di chi, 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, ovvero, costituito dalla condotta di chi, 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.

Le attività sensibili in materia tributaria e fiscale devono essere presidiate anche rispetto ai rischi derivanti da utilizzo improprio di strumenti digitali o di IA, da anomalie nei flussi finanziari internazionali, da passività e costi non correttamente rilevati per fatti ambientali o giuslavoristici, nonché da operazioni con controparti o flussi potenzialmente interessati da misure restrittive UE.

8.1 PRINCIPI GENERALI DI COMPORTAMENTO PRESCRITTI NELLE ATTIVITÀ SENSIBILI

DIVIETI

La presente Parte Speciale prevede l'espresso divieto - a carico degli Esponenti Aziendali, in via diretta, e a carico dei Collaboratori esterni e Partner, tramite apposite clausole contrattuali - di:

 porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-quinquiesdecies del d.lgs. 231/2001);

 porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

INOLTRE A TUTTI I SOGGETTI È FATTO DIVIETO DI:

- perseguire finalità di evasione di imposte sui redditi o sul valore aggiunto, o di altre imposte in generale, né nell'interesse o vantaggio della Società né nell'interesse o vantaggio di terzi;
- compiere operazioni simulate oggettivamente o soggettivamente;
- registrare nelle scritture contabili obbligatorie, detenere a fini di prova nei confronti dell'Amministrazione finanziaria, fatture o altri documenti per operazioni inesistenti o falsi. Deve sempre essere verificata la regolare e corretta applicazione dell'imposta sul valore aggiunto su tutti i documenti contabili della Società;
- presentare dichiarazioni incomplete o comunque non veritiere ad organismi pubblici nazionali o comunitari, al fine di conseguire vantaggi o la non applicazione di una sanzione.

È vietato utilizzare strumenti di IA per generare, modificare, completare o integrare dati, scritture, stime, prospetti o documenti fiscali e societari in modo non conforme alla realtà, non verificato o non validato dal soggetto umano competente.

È vietato utilizzare strumenti di IA per generare, modificare, completare o integrare dati, scritture, stime, prospetti o documenti fiscali e societari in modo non conforme alla realtà, non verificato o non validato dal soggetto umano competente.

DOVERI

La presente sezione prevede, altresì, l'espresso obbligo a carico dei soggetti sopra indicati di conoscere e rispettare tutte le misure atte a garantire la corretta gestione degli obblighi tributari.

Le condotte di ordine generale sopra descritte integrano e non sostituiscono i principi previsti dal Codice Etico, nonché le eventuali procedure di maggiore tutela previste all'interno di BITCONTROL e relative alle attività sensibili.

Inoltre, tutti i soggetti devono:

- rispettare i criteri di trasparenza nell'esercizio dell'attività aziendale e nella scelta del partner finanziario e/o commerciale, prestando la massima attenzione alle notizie riguardanti i soggetti terzi con i quali BITCONTROL ha rapporti di natura finanziaria che possano anche solo generare il sospetto della commissione di uno dei reati di cui alla presente parte speciale;
- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, con particolare riferimento alle attività finalizzate alla gestione anagrafica di Fornitori/Clienti/Consulenti esterni/Terze parti/Partner anche stranieri;
- assicurare la tracciabilità delle fasi del processo decisionale relativo all'adempimento degli obblighi tributari in particolar modo delle dichiarazioni fiscali e versamento delle imposte.

È obbligatorio assicurare trasparenza, tracciabilità, conservazione delle evidenze, separazione delle funzioni, corretta gestione degli accessi e rispetto delle procedure aziendali anche quando le attività siano svolte in modalità agile o con strumenti tecnologici avanzati.

Le funzioni competenti devono assicurare che eventuali passività, fondi rischi, costi, sanzioni, obblighi di ripristino, contestazioni o esposizioni rilevanti derivanti da violazioni ambientali o da irregolarità nell'impiego di lavoratori, inclusi cittadini di Paesi terzi, siano tempestivamente comunicati alle funzioni amministrativo-contabili per le valutazioni di competenza e per la corretta rappresentazione contabile e informativa.

È obbligatorio assicurare trasparenza, tracciabilità, conservazione delle evidenze, separazione delle funzioni, corretta gestione degli accessi e rispetto delle procedure aziendali anche quando le attività siano svolte in modalità agile o con strumenti tecnologici avanzati.

Le funzioni competenti devono assicurare che eventuali passività, fondi rischi, costi, sanzioni, obblighi di ripristino, contestazioni o esposizioni rilevanti derivanti da violazioni ambientali o da irregolarità nell'impiego di lavoratori, inclusi cittadini di Paesi terzi, siano tempestivamente comunicati alle funzioni amministrativo-contabili per le valutazioni di competenza e per la corretta rappresentazione contabile e informativa.

9 ARCHIVIAZIONE

La documentazione relativa alla tenuta della contabilità, alla predisposizione del bilancio e dei relativi allegati, è archiviata a cura del RAM/RRU, o della funzione eventualmente incaricata dal PRES, e del RGAD, e tenuta a disposizione dell'OdV.

I dati e documenti rilevanti ai fini del bilancio devono essere trattati secondo le procedure aziendali in materia di gestione accessi, classificazione delle informazioni, segregazione dei ruoli, gestione

incidenti, continuità operativa, backup, cifratura e logging, in coerenza con i sistemi di gestione adottati dalla Società.

L'accesso ai dati e ai documenti di bilancio è consentito ai soli soggetti autorizzati secondo il principio del need to know.

Devono essere conservati documenti, log, attestazioni, riconciliazioni, evidenze di revisione, validazioni, flussi autorizzativi e documentazione di supporto, ivi comprese le eventuali evidenze relative all'uso autorizzato di strumenti di IA

10 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutti i *Destinatari* coinvolti nella predisposizione del bilancio e dei relativi allegati, devono informare, tempestivamente, l'Organismo di Vigilanza delle situazioni anomale, o di eventuali violazioni della presente procedura, nonché dei comportamenti non conformi a quanto previsto nel Modello e nel 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.

In particolare, devono essere trasmessi all'OdV, con periodicità almeno semestrale e comunque senza ritardo in caso di criticità, flussi informativi relativi a:

anomalie contabili o fiscali significative;

- omissioni, falsificazioni, alterazioni o contestazioni documentali;
- uso di sistemi di IA nei processi di predisposizione del bilancio, ove rilevante;

impiego non autorizzato di strumenti di IA o uso di strumenti diversi da quelli approvati;

incidenti informatici, data breach o violazioni della classificazione delle informazioni che coinvolgano dati o documenti contabili;

- criticità rilevanti in materia di misure restrittive UE, ambiente, lavoro agile/sicurezza o impiego di cittadini di Paesi terzi che possano incidere sui processi di bilancio o sui presìdi 231;
- esiti dei controlli preventivi e successivi sugli output IA, ove utilizzati;
- violazioni della Policy IA, del Codice Etico, del Codice di Condotta o della presente procedura.

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 nell'apposita piattaforma di condivisione - tutta la documentazione necessaria.

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. Resta fermo l'obbligo di segnalazione interna di omissioni, falsificazioni, irregolarità contabili, uso improprio dell'IA, distruzione o occultamento di documenti, anomalie nei flussi finanziari e violazioni della presente procedura secondo i canali interni di whistleblowing adottati dalla Società.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

SOMMARIO

1.OBIETTIVI DELLA PROCEDURA

In tema di reati contro la Pubblica Amministrazione il D. Lgs. 231/2001 prevede due articoli che

individuano i seguenti "reati presupposto":

- Art. 24, indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico.
- Art. 25, Concussione e corruzione, induzione indebita a dare o promettere utilità.

servizio militare.

TRA I REATI POTENZIALMENTE A RISCHIO SI PRENDONO IN CONSIDERAZIONE I SEGUENTI:

MALVERSAZIONE A DANNO DELLO STATO O DELL'UNIONE EUROPEA (ART. 316-BIS C.P.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da

parte dello Stato italiano, di altri enti pubblici o dell'Unione Europea, non si proceda all'utilizzo delle somme ottenute per gli scopi di pubblico interesse cui erano destinate. Tenuto conto che il momento di consumazione del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che non vengano destinati alle finalità per cui erano stati erogati.

INDEBITA PERCEZIONE DI EROGAZIONI IN DANNO DELLO STATO O DELL'UNIONE EUROPEA (ART. 316-TER C.P.)

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, per sé o per altri e senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti pubblici o dall'Unione europea. In questo

caso, non rileva il corretto utilizzo delle erogazioni (come invece previsto dall'art. 316-bis), poiché il reato si concretizza nel momento stesso dell'ottenimento dei finanziamenti in modo indebito. Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie dell'art. 640-bis c.p., con riferimenti a quei casi in cui la condotta non integri gli estremi più gravi della truffa ai danni dello Stato.

TRUFFA IN DANNO DELLO STATO, DI ALTRO ENTE PUBBLICO O DELL'UNIONE EUROPEA (ART. 640, COMMA 2, N.1 C.P.)

La fattispecie di cui all'art. 640 c.p. prevede un reato comune che può essere commesso da chiunque. Il fatto che costituisce reato consiste nel procurare a sé o ad altri un ingiusto profitto a danno di un altro soggetto, inducendo taluno in errore mediante artifici o raggiri. In particolare, nella fattispecie richiamata dall'art. 24 del D.Lgs. 231/2001 (i.e. art. 640 comma 2, n. 1 c.p.), rilevano i fatti commessi a danno dello Stato o di altro ente pubblico.

Con la 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).

In ultimo, è intervenuta la L. n.80 del 9 giugno 2025 che ha convertito il D.L. n. 48 dell'11 aprile 2025 contenente "Disposizioni urgenti in materia di sicurezza pubblica, di tutela del personale in servizio, nonchè di vittime dell'usura e di ordinamento penitenziario";

Tale provvedimento ha comportato anche modifiche all'Art. 640 c.p. (Truffa) facente parte dell'Art. 24 del D. Lgs 231/01 (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).

TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (ART. 640-BIS C.P.)

Tale ipotesi di reato si configura nel caso in cui la truffa (di cui all'art. 640 c.p.) sia posta in essere per conseguire indebitamente, 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.

CORRUZIONE PER L'ESERCIZIO DELLA FUNZIONE (ART. 318 C.P.)

L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale, 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.

CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI DI UFFICIO (ART. 319 C.P.)

L'ipotesi di reato di cui all'art. 319 c.p., si configura nel caso in cui il pubblico ufficiale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri d'ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa.

ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)

Tale ipotesi di reato si configura nei confronti di chiunque offra o prometta denaro o altra utilità non dovuti ad un pubblico ufficiale o incaricato di pubblico servizio per indurlo a compiere, omettere o ritardare un atto del suo ufficio, ovvero a compiere un atto contrario ai propri doveri, qualora l'offerta o la promessa non sia accettata.

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

Tale ipotesi di reato si configura nel caso in cui i fatti indicati negli artt. 318 e 319 c.p sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo. Il reato di corruzione in atti giudiziari può essere commesso nei confronti di giudici o membri del Collegio

Arbitrale competenti a giudicare sul contenzioso/arbitrato nell'interesse dell'Ente (compresi gli ausiliari e i periti d'ufficio), e/o di rappresentanti della Pubblica Amministrazione, quando questa sia una parte nel contenzioso, al fine di ottenere illecitamente decisioni giudiziali e/o stragiudiziali favorevoli.

INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ (319-QUARTER C.P.)

Tale ipotesi di reato si configura, salvo che il fatto costituisca più grave reato, nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, induca taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

PENE PER IL CORRUTTORE (ART. 321 C.P.)

Le pene stabilite nel primo comma dell'articolo 318, nell'art. 319, nell'art. 319-bis, nell'articolo 319-ter e nell'art. 320 c.p. in relazione alle suddette ipotesi degli artt. 318 e 319 c.p., si applicano anche a chi (i.e. corruttore) dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio denaro o altra utilità.

ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)

Tale ipotesi di reato si configura nei confronti di chiunque offra o prometta denaro o altra utilità non dovuti ad un pubblico ufficiale o incaricato di pubblico servizio per indurlo a compiere, omettere o ritardare un atto del suo ufficio, ovvero a compiere un atto contrario ai propri doveri, qualora l'offerta o la promessa non sia accettata.

Orbene, la presente procedura ha lo scopo di definire i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento che dovranno essere osservati, nei casi in cui un pubblico ufficiale o un incaricato di pubblico servizio si rechi presso BITCONTROL s.r.l. per effettuare accertamenti, ispezioni o verifiche di qualsiasi natura, legislativamente previste. Tra le ispezioni prese in esame nella presente procedura rientrano, a titolo meramente esemplificativo, gli accertamenti e le verifiche di tipo fiscale e tributario, in materia di lavoro, previdenza, igiene e sicurezza sui luoghi di lavoro, tutela dei dati personali, *etc.*

La procedura disciplina, inoltre, i rapporti con la Pubblica Amministrazione in tutte le fasi delle procedure di affidamento e dell'esecuzione dei contratti pubblici, l'ottenimento e la gestione di autorizzazioni e provvedimenti, la richiesta e rendicontazione di contributi pubblici, nonché l'impiego di sistemi di Intelligenza Artificiale nella predisposizione di offerte o documenti destinati alla P.A., in coordinamento con il Codice Etico, la Politica Anticorruzione e le Misure Integrative del Modello 231.

2. ACRONOMI 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
RCA	Responsabile interno conformità anticorruzione

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

3.RIFERIMENTI NORMATIVI E DOCUMENTI AZIENDALI DI RIFERIMENTO

- Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche e integrazioni, con particolare riferimento agli artt. 24 e 25;

- Codice penale, con particolare riferimento agli artt. 316-bis, 316-ter, 318, 319, 319-ter, 319-quater, 320, 321, 322, 322-bis, 346-bis, 353, 353-bis, 356, 640, comma 2, n. 1, 640-bis e 640-ter;
- D.Lgs. 31 marzo 2023, n. 36 e s.m.i. (Codice dei contratti pubblici), incluso il D.Lgs. 31 dicembre 2024, n. 209;
- Legge 6 novembre 2012, n. 190; D.Lgs. 14 marzo 2013, n. 33, per quanto applicabili; D.Lgs. 10 marzo 2023, n. 24 in materia di whistleblowing; art. 53, comma 16-ter, D.Lgs. 30 marzo 2001, n. 165 in materia di pantouflage; Regolamento (UE) 2024/1689; Legge 23 settembre 2025, n. 132; Delibera ANAC n. 148 del 1° aprile 2026 e Bando-tipo n. 1/2023 aggiornato.
- Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001; Codice Etico approvato il 25.06.2026; Codice Disciplinare; Politica Anticorruzione; Misure Integrative del Modello 231 in materia di anticorruzione e trasparenza 2025-2028; Procedura Whistleblowing; Policy e procedura aziendale per il corretto utilizzo dei sistemi di Intelligenza Artificiale; procedure relative a gare, omaggi, selezione dei partner, incarichi e flussi finanziari.

4.CAMPO DI APPLICAZIONE E RESPONSABILE DELLA PROCEDURA

Rientrano nel campo di applicazione della procedura tutti coloro (compresi i Responsabili di funzione ed i Consulenti esterni all'uopo caricati) 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 deve essere informato di tutti i procedimenti e assicura il coordinamento con le funzioni competenti, con il Responsabile IA, ove nominato, con il Responsabile della conformità anticorruzione e con l'Organismo di Vigilanza, nel rispetto dei rispettivi ruoli e dell'autonomia dell'OdV.

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

5.INDICAZIONI COMPORTAMENTALI

I Destinatari che, per ragione del proprio incarico o della propria Funzione, siano coinvolti nella gestione dei rapporti con la Pubblica Amministrazione, devono rispettare le prescrizioni di cui alla presente procedura ed in particolare devono:

- prestare completa e immediata collaborazione alle Autorità, fornendo puntualmente ed esaustivamente la documentazione e le informazioni richieste;
- garantire la tracciabilità degli atti, compresa la fase autorizzativa degli stessi, a garanzia della trasparenza delle scelte effettuate.
- operare nel rispetto dei principi di legalità, imparzialità, correttezza, trasparenza, segregazione delle funzioni e tracciabilità, evitando qualsiasi contatto non autorizzato o non documentato con esponenti della P.A.;
- dichiarare tempestivamente situazioni, anche potenziali, di conflitto di interessi e astenersi dal compimento di atti sino alla valutazione della funzione competente;
- verificare, prima del conferimento di incarichi o dell'assunzione di ex dipendenti pubblici, l'assenza delle condizioni ostative previste dall'art. 53, comma 16-ter, del D.Lgs. 165/2001 e acquisire la relativa dichiarazione;

in caso di utilizzo di sistemi di IA nella predisposizione di offerte o documenti destinati alla P.A., utilizzare esclusivamente strumenti autorizzati, non inserire dati riservati o personali non anonimizzati, conservare i log rilevanti, assicurare la revisione umana integrale degli output e rendere le dichiarazioni richieste dalla lex specialis e dalla disciplina ANAC applicabile.

AI DESTINATARI INTERESSATI È VIETATO:

- autorizzare, sollecitare, offrire, promettere di concedere, 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 aiuterebbero la Società ad ottenere, promuovere, mantenere le proprie attività o ad assicurarsi vantaggi illegittimi o indebiti nello svolgimento delle stesse. Parimenti, i Destinatari sono tenuti a segnalare qualsiasi tentativo di estorsione o concussione da parte di un pubblico ufficiale di cui dovessero essere destinatari o a conoscenza;
- offrire o corrispondere a soggetti operanti nella P.A. (o a soggetti loro congiunti, affini, conviventi e soggetti ad essi in qualche modo collegati) omaggi, trattamenti di favore e/o regalie di valore più che simbolico, nell'intento di favorire in modo illecito la Società;
- rivolgersi a soggetti che sfruttano o vantano relazioni esistenti o asserite con pubblici ufficiali, incaricati di pubblici servizi, ovvero con uno degli altri soggetti di cui all'art. 322 bis c.p., concedendo o promettendo loro (o ad altri) denaro o altra utilità, quale prezzo per la propria mediazione illecita nei confronti di detti soggetti operanti nella P.A. o per la remunerazione di questi ultimi in relazione all'esercizio delle loro funzioni o dei propri poteri.
- alterare, omettere o occultare dati, documenti o informazioni richiesti dalla P.A., presentare dichiarazioni non veritiere o utilizzare documenti falsi, anche mediante strumenti informatici o sistemi di IA;
- ricorrere a sistemi di IA per generare contenuti ingannevoli, manipolativi o non verificati, ovvero per eludere controlli, requisiti di gara o obblighi di trasparenza;

 intrattenere interlocuzioni informali o riservate con funzionari pubblici finalizzate a ottenere informazioni privilegiate, trattamenti preferenziali o vantaggi indebiti.

6.AREE SENSIBILI AI FINI DELLA COMMISSIONE DEI REATI PRESUPPOSTO DI CUI AL D.LGS 231/2001

Ai fini della prevenzione dalla commissione dei reati in esame, sono state individuate tutte le aree aziendali potenzialmente a rischio, ovvero tutte quelle attività tipiche consistenti nell'intrattenimento di rapporti con la P.A. (c.d. rischio diretto).

Allo stesso modo, sono da considerarsi a rischio le aree aziendali che, pur non implicando direttamente l'instaurazione di rapporti con la P.A., gestiscono strumenti di tipo finanziario o utilità di altro genere che potrebbero essere impiegati per attribuire vantaggi e utilità a pubblici

ufficiali (c.d. rischio indiretto).

Quindi, dall'esame delle attività aziendali, sono state considerate

ATTIVITÀ A RISCHIO DIRETTO:

- la partecipazione a procedure di gara, affidamenti diretti, consultazioni preliminari di mercato, soccorso istruttorio, stipula, esecuzione, collaudo, varianti, riserve, subappalti, pagamenti e contenzioso relativi a contratti pubblici;
- la predisposizione e trasmissione di dichiarazioni, offerte tecniche ed economiche, documentazione amministrativa e giustificativi alla P.A., anche con il supporto di sistemi di IA;
- la selezione e gestione di consulenti, intermediari, partner, raggruppamenti temporanei, subappaltatori e fornitori coinvolti nei rapporti con la P.A.;
- il conferimento di incarichi o l'assunzione di dipendenti ed ex dipendenti pubblici, nonché la gestione di conflitti di interessi, omaggi, ospitalità, sponsorizzazioni e liberalità;
- la richiesta, percezione, utilizzazione e rendicontazione di finanziamenti, sovvenzioni e contributi pubblici;

- effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri;
- 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 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 05 "Scelta Partner Commerciali e Omaggi";

ALL'UOPO SI PRECISA CHE:

- **il reato di corruzione** potrebbe essere consumato attraverso il contatto con i rappresentanti della Pubblica Amministrazione, con la finalità di influenzare posizioni e decisioni a favore per la Società;
- **il reato di truffa a danno dello Stato** potrebbe in una rappresentazione non trasparente dei fatti, tramite l'emissione di documenti o la specifica condotta ingannevole nei confronti dei rappresentanti della Pubblica Amministrazione, da cui derivi un danno allo Stato;
- **il reato di indebita percezione di erogazioni** potrebbe essere commesso al momento della richiesta dello stanziamento del finanziamento concesso e dell'acquisizione del finanziamento agevolato, mediante la presentazione di richieste di finanziamento che contengano dichiarazioni o documenti falsi che attestino dati o fatti non veri o omettano informazioni dovute;
- **il reato di malversazione** potrebbe essere commesso nel caso in cui i fondi agevolati ottenuti vengano destinati, in tutto o in parte, a scopi diversi da quelli dichiarati.

 rapporti con Pubblici Ufficiali in occasione di verifiche ed ispezioni (si considerano in tale area qualsiasi ispezione, accertamento, verifica tecnica, giudiziaria, tributaria, amministrativa, relativa alla normativa sulla sicurezza e salute del lavoro, o della normativa ambientale, condotta dall' ASL, ispettorato del lavoro, dall'INPS, INAIL, Agenzia delle Entrate, Guardia di Finanza, polizia municipale o provinciale, vigili del fuoco, ecc.).

ORBENE, IN RELAZIONE A QUESTE ATTIVITÀ, I REATI IPOTIZZABILI, IN LINEA DI PRINCIPIO, POTREBBERO ESSERE:

- **il reato di corruzione** che potrebbe essere consumato attraverso il contatto con i rappresentanti della Pubblica Amministrazione, con la finalità di influenzare posizioni e decisioni a favore (o a minor sfavore) per la Società.
- **Il reato di truffa a danno dello Stato** che potrebbe configurarsi in una rappresentazione non trasparente dei fatti, tramite l'emissione di documenti o la specifica condotta ingannevole nei confronti dei rappresentanti della Pubblica Amministrazione, da cui derivi un danno all'Ente pubblico ed un vantaggio ingiusto per la Società.

 rapporti con soggetti pubblici per l'ottenimento, il mantenimento ed il rinnovo di autorizzazioni, concessioni, licenze, servitù, provvedimenti amministrativi e permessi necessari o utili per l'esercizio delle attività aziendali.

Si comprendono in tali attività le richieste di autorizzazioni ai Comuni, alla Provincia, alla Regione ed altri Enti Pubblici.

7. PRESIDI DI CONTROLLO

I *Destinatari* coinvolti nella gestione di rapporti con la Pubblica Amministrazione sono tenuti ad osservare i seguenti principi di comportamento e controllo nella gestione dei rapporti con i rappresentanti della Pubblica Amministrazione.

In linea generale, è fatto divieto ai Destinatari di influenzare le decisioni dei Rappresentanti della

Pubblica Amministrazione in maniera impropria o illecita.

IN PARTICOLARE, NEI RAPPORTI CON LA P.A. È FATTO LORO 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 ovvero nella prassi vigenti;
• 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 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 (nell'ambito dei procedimenti di qualsiasi natura) sono gestiti esclusivamente da persone munite di idonei poteri o da coloro che siano da queste formalmente delegati.

Per ogni procedura di gara deve essere individuato un responsabile interno, devono essere tracciate le autorizzazioni e le interlocuzioni con la stazione appaltante e deve essere conservato un fascicolo digitale completo della documentazione trasmessa, ricevuta e approvata.

Qualora siano utilizzati sistemi di IA, il fascicolo di gara deve contenere almeno: l'indicazione dello strumento autorizzato, le parti dell'offerta supportate dall'IA, la verifica dell'assenza di dati riservati nei prompt, i log rilevanti, l'attestazione di revisione e validazione umana e la dichiarazione richiesta dalla documentazione di gara in conformità alla Delibera ANAC n. 148/2026.

Prima dell'affidamento di incarichi a consulenti, intermediari o partner che possano interagire con la P.A. sono svolte verifiche proporzionate di integrità, competenza, titolarità effettiva, conflitti di interessi e assenza di indicatori di rischio corruttivo; il contratto deve prevedere obblighi di conformità al Modello 231, al Codice Etico e alla Politica Anticorruzione.

Ogni omaggio, ospitalità, sponsorizzazione o liberalità connessa, anche indirettamente, a soggetti pubblici deve essere preventivamente autorizzata, di modico valore, occasionale, lecita, tracciata e mai collegata a procedimenti, gare, verifiche o decisioni pendenti.

Le dichiarazioni relative a conflitti di interessi, incompatibilità e pantouflage sono acquisite, verificate e archiviate dalla funzione competente; ogni anomalia è comunicata al PRES e all'OdV.

I Destinatari coinvolti nella gestione di rapporti con la Pubblica Amministrazione sono tenuti ad osservare i seguenti principi di comportamento e controllo nella gestione degli adempimenti richiesti in sede di verifiche ispettive:

- predisposizione e continuo aggiornamento, a cura del PRES o di altro soggetto all'uopo incaricato, di un elenco di persone che l'Amministrazione deve contattare in occasione di visite e ispezioni da parte di funzionari della Pubblica Amministrazione. Il *Destinatario* che per primo entra in contatto con la Pubblica Amministrazione deve avvertire il responsabile della presente procedura;
- allestimento di un registro, anche digitale, in cui sono annotati gli accessi alla Società da parte di Funzionari pubblici o assimilabili, con l'indicazione dei nominativi, dell'orario di accesso e di uscita e dell'Ente di appartenenza;
- la possibilità per il Responsabile della funzione aziendale interessata, eventualmente dotata degli adeguati poteri, di presidiare lo svolgimento delle attività ispettive, nonché la presenza del PRES nella fase iniziale ed in quella conclusiva dell'ispezione;
- durante l'ispezione devono essere presenti, ove possibile, almeno due soggetti aziendali; ogni consegna documentale deve essere previamente verificata, annotata in apposito elenco e accompagnata da ricevuta o evidenza di trasmissione, senza alterare, distruggere, occultare o retrodatare documenti;
- l'archiviazione da parte del Responsabile della funzione aziendale interessata dell'evidenza documentale delle richieste ricevute, dei verbali predisposti dai

funzionari pubblici in occasione delle visite ispettive, nonché delle informazioni, dei dati e dei documenti consegnati, resi disponibili e/o comunicati. Il PRES, o il soggetto dotato degli adeguati poteri (es. professionista cui è conferita delega), unitamente al Responsabile della Funzione aziendale interessata presente durante l'ispezione, dovrà siglare i verbali predisposti dai funzionari.

Qualora si tratti di accertamenti, ispezioni o verifiche di durata prolungata la compresenza del PRES (o di altra funzione aziendale all'uopo preposta) e del professionista incaricato deve essere garantita almeno nelle fasi più importanti (ovvero durante l'apertura e la chiusura dell'ispezione), nonché, al termine di ogni giornata per la verifica del verbale e per la consegna della documentazione ai funzionari pubblici.

La funzione aziendale interessata dovrà redigere un *report* informativo dell'attività svolta nel corso dell'ispezione, contenente, fra l'altro, i nominativi dei funzionari incontrati, i documenti richiesti e/o consegnati, i soggetti coinvolti e una sintesi delle informazioni verbali richieste e/o fornite; tale *report* dovrà essere vistato dal professionista incaricato o dal PRES.

8. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Resta fermo l'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. 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 invia all'OdV, senza ritardo e comunque entro cinque giorni lavorativi, una relazione riepilogativa contenente l'oggetto della verifica, i funzionari intervenuti, i

documenti richiesti e consegnati, i rilievi formulati, le eventuali contestazioni e le azioni correttive programmate.

In ogni caso, il Responsabile della procedura informa tempestivamente l'Organismo di Vigilanza sulle ispezioni, sulle richieste della P.A. e su ogni evento anomalo, incluse richieste indebite, tentativi di concussione, conflitti di interessi, omissioni o falsità documentali, violazioni degli obblighi di gara e irregolarità nell'uso di sistemi di IA.

Con cadenza almeno annuale, il responsabile della procedura trasmette all'OdV un flusso riepilogativo relativo a: gare e affidamenti pubblici; finanziamenti e contributi; autorizzazioni e concessioni; ispezioni e contenziosi con la P.A.; omaggi e ospitalità verso soggetti pubblici; incarichi a ex dipendenti pubblici; dichiarazioni sull'uso dell'IA; anomalie e azioni correttive.

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 relativi ai flussi e alle segnalazioni verso l'Organismo di Vigilanza sono disciplinati dalle procedure "Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/2001" e "Procedura di gestione del whistleblowing". Le segnalazioni sono trattate nel rispetto del D.Lgs. 24/2023, con tutela della riservatezza e divieto di 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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 05	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DELL'31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

Ai sensi del D.Lgs. 231/2001, il processo relativo alla gestione dei contenziosi giudiziali e stragiudiziali, degli arbitrati, delle procedure di mediazione e negoziazione assistita, degli accordi transattivi, delle ispezioni e delle dichiarazioni da rendere alle Autorità può presentare occasioni per la commissione, tra gli altri, dei reati contro la Pubblica Amministrazione, dei delitti di corruzione e istigazione alla corruzione tra privati, del traffico di influenze illecite, della truffa ai danni dello Stato o di altro ente pubblico, dell'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria, nonché dei reati tributari, di riciclaggio e autoriciclaggio e delle violazioni delle misure restrittive dell'Unione europea, ove connessi alla definizione o esecuzione della controversia.

Inoltre, sussiste, altresì, il rischio della commissione dei reati di "*Corruzione tra privati*" e "*Istigazione alla corruzione tra privati*".

Dunque, la presente procedura definisce i ruoli, le responsabilità operative, le attività di controllo e i principi di comportamento adottati da BITCONTROL S.r.l. per la gestione dell'intero ciclo di vita del contenzioso e degli accordi transattivi, nonché dei rapporti con l'Autorità giudiziaria, la polizia giudiziaria, le Autorità amministrative indipendenti e gli organi di vigilanza e controllo.

I *Destinatari* che, per ragione del proprio incarico o della propria funzione, devono interfacciarsi con l'Autorità Giudiziaria, dovranno rispettare le seguenti prescrizioni:

- assicurare che tali rapporti avvengano nell'assoluto rispetto della legge, nonché del Modello e del Codice Etico;
- prestare una fattiva collaborazione e rendere dichiarazioni veritiere, trasparenti e rappresentative dei fatti;

È FATTO DIVIETO DI:

- porre in essere attività che possano favorire o danneggiare, direttamente o indirettamente, una delle parti in causa nel corso del procedimento penale;
- condizionare, in qualsiasi forma e con qualsiasi modalità, la volontà dei soggetti chiamati a rispondere all'Autorità Giudiziaria, al fine di non rendere dichiarazioni o di dichiarare fatti non rispondenti al vero;
- promettere o offrire denaro, omaggi o altra utilità a soggetti coinvolti in procedimenti penali e/o a persone a loro vicine;
- accettare denaro o qualsivoglia utilità da soggetti coinvolti in procedimenti penali o da persone a loro vicine.

La presente Procedura si coordina con il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 aggiornato, con il Codice Etico, con il Codice di Condotta, con la Policy sull'Intelligenza Artificiale, con la Procedura Whistleblowing e con le ulteriori procedure aziendali approvate.

La presente Procedura si applica anche alle attività di supporto, preparazione documentale e comunicazione nelle quali siano utilizzati strumenti digitali o di Intelligenza Artificiale, ivi incluse la predisposizione di memorie, note difensive, schede di sintesi, reportistica verso l'autorità giudiziaria, raccolta e organizzazione di documentazione probatoria o di altra documentazione rilevante nell'ambito di contenziosi, ispezioni, accertamenti, procedimenti amministrativi o penali.

2 ACRONOMI 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
RGAD	Responsabili Gestione Archivi e Documenti
REC	Responsabile Esterno Contabilità
RCL	Responsabile Consulente Legale Esterno
RCA	Responsabile interno conformità aziendale
RIA	Responsabile IA

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

3 RIFERIMENTI NORMATIVI DEL MODELLO

- DECRETO LEGISLATIVO 231/2001 E S.S. MM.II (DI SEGUITO ANCHE D.LGS 231/01);
- CODICE ETICO DI BITCONTROL S.R.L.;
- CODICE DISCIPLINARE DI BITCONTROL S.R.L.
- MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO DI BITCONTROL S.R.L..
- D.LGS. 10 MARZO 2023, N. 24 IN MATERIA DI TUTELA DELLE PERSONE CHE SEGNALANO VIOLAZIONI DEL DIRITTO DELL'UNIONE E DI DISPOSIZIONI NORMATIVE NAZIONALI (WHISTLEBLOWING), CHE DISCIPLINA I CANALI DI SEGNALAZIONE, LA PROTEZIONE DEL SEGNALANTE, LA RISERVATEZZA DELL'IDENTITÀ, I TERMINI PROCEDIMENTALI E I DIVIETI DI RITORSIONE;

- D.LGS. 24/2023; VOCE ELIMINATA PERCHÉ DUPLICATA RISPETTO AL PRECEDENTE RICHIAMO AL D.LGS. 10 MARZO 2023, N. 24.
- D.LGS. 30 DICEMBRE 2025, N. 211, IN VIGORE DAL 24 GENNAIO 2026, IN MATERIA DI REATI E SANZIONI PER LA VIOLAZIONE DELLE MISURE RESTRITTIVE DELL'UNIONE EUROPEA, INCLUSI I CONSEGUENTI AGGIORNAMENTI AL D.LGS. 231/2001 E AL D.LGS. 24/2023;
- CODICE PENALE, CON PARTICOLARE RIFERIMENTO AGLI ARTT. 318, 319, 319-TER, 319-QUATER, 322, 322-BIS, 346-BIS, 377-BIS, 378, 640, 648-BIS, 648-TER.1 E ALLE ULTERIORI FATTISPECIE APPLICABILI;
- LEGGE 9 AGOSTO 2024, N. 114, CHE HA RIFORMULATO L'ART. 346-BIS C.P. IN MATERIA DI TRAFFICO DI INFLUENZE ILLECITE;
- REGOLAMENTO (UE) 2024/1689 (AI ACT), LEGGE 23 SETTEMBRE 2025, N. 132, REGOLAMENTO (UE) 2016/679 E POLICY IA AZIENDALE, PER L'EVENTUALE UTILIZZO DI SISTEMI DI IA NELLE ATTIVITÀ LEGALI E DOCUMENTALI;
- CODICE DI PROCEDURA CIVILE, CODICE DI PROCEDURA PENALE, D.LGS. 28/2010, D.L. 132/2014 CONVERTITO DALLA L. 162/2014 E NORMATIVA SPECIALE APPLICABILE ALLA SINGOLA CONTROVERSIA

4 CAMPO DI APPLICAZIONE E DESTINATARI DELLA PROCEDURA

La presente procedura si applica a tutti i *Destinatari* (compresi i Collaboratori ed i Consulenti esterni all'uopo incaricati) che, 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.

Per BITCONTROL, la procedura comprende in particolare le controversie e i reclami connessi a gare e contratti pubblici, commesse di progettazione, sviluppo, integrazione, assistenza e manutenzione di sistemi SCADA, PLC, RTU, DCS, telecontrollo, IoT e infrastrutture di comunicazione, inclusi contestazioni tecniche, ritardi, livelli di servizio, sicurezza informatica, proprietà intellettuale, riservatezza, trattamento dei dati, subappalti, forniture, personale e attività svolte presso impianti di clienti pubblici o privati, anche all'estero.

Dunque, la presente procedura si applica altresì a tutti coloro che intrattengono con la Società un rapporto di lavoro subordinato (dipendenti), ivi compresi coloro che sono distaccati, in Italia e all'estero, per lo svolgimento dell'attività.

Si precisa, altresì, che ogni accordo transattivo deve essere preceduto da una verifica di legittimità e di merito, deve essere autorizzato secondo la catena delle deleghe interne, deve essere formalizzato in forma scritta e documentato, con conservazione delle evidenze relative al processo decisionale, ai soggetti intervenuti, alle verifiche effettuate e all'iter autorizzativo seguito.

È vietata la stipula di accordi transattivi che abbiano lo scopo o l'effetto di occultare condotte illecite, di rinunciare ad azioni di recupero del danno erariale, di condizionare o influenzare procedimenti giudiziari o amministrativi in corso, ovvero di remunerare, sotto qualsiasi forma, soggetti pubblici o privati per il compimento o l'omissione di atti connessi alle loro funzioni o attribuzioni.

5 RESPONSABILE DELLA PROCEDURA

Il responsabile della procedura è il PRES.

Le figure aziendali coinvolte nei processi disciplinati dalla presente Procedura operano in coordinamento con i presidi organizzativi adottati o aggiornati nel 2026, inclusi Modello 231, Codice Etico, Codice di Condotta, Procedura Whistleblowing, Policy IA e regolamenti aziendali applicabili.

L'elenco dei soggetti autorizzati a gestire contenziosi, a firmare atti processuali o transattivi, a rappresentare la Società nei rapporti con l'autorità giudiziaria o con le autorità di controllo, nonché a conferire mandati difensivi, deve essere aggiornato includendo le nuove risorse inserite in organico ove assegnate a processi rilevanti per la presente Procedura.

6 INDICAZIONI COMPORTAMENTALI

La gestione del contenzioso giudiziale e stragiudiziale deve avvenire in coordinamento con i professionisti esterni all'uopo incaricati e si articola:

1. nell' apertura del contenzioso giudiziale o stragiudiziale:

- raccolta delle informazioni e della documentazione relative alla vertenza;
- analisi, valutazione e produzione degli elementi probatori;

o predisposizione degli scritti difensivi e successive integrazioni, direttamente o in collaborazione con i professionisti esterni;

2. nella gestione della vertenza;
3. nella ricezione, analisi e valutazione degli atti relativi alla vertenza;
4. nella predisposizione dei fascicoli documentali;
5. nella partecipazione, ove utile o necessario, alla causa, in caso di contenzioso giudiziale;
6. nell'intrattenimento di rapporti costanti con gli eventuali professionisti incaricati, individuati nell'ambito dell'apposito albo;

7. nella chiusura della vertenza.

Il processo di gestione degli accordi transattivi riguarda tutte le attività necessarie per prevenire o dirimere una controversia attraverso accordi o reciproche rinunce e concessioni, al fine di evitare l'instaurarsi o il proseguire di procedimenti giudiziari e si articola nelle seguenti fasi:

- ✓ analisi dell'evento da cui deriva la controversia e verifica dell'esistenza di presupposti per addivenire alla transazione;
- ✓ gestione delle trattative finalizzate alla definizione e alla formalizzazione della transazione;
- ✓ redazione, stipula ed esecuzione dell'accordo transattivo.

Mentre, nel caso in cui qualunque Destinatario del Modello è chiamato - in qualità di imputato o coimputato in un procedimento penale connesso o collegato - a rendere dichiarazioni innanzi all'Autorità Giudiziaria, lo stesso deve osservare i seguenti principi comportamentali:

- ➢ garantire che ogni attività collaborativa su richiesta dell'Autorità Giudiziaria e secondo le indicazioni formulate dalla stessa, deve essere svolta nell'assoluto rispetto dei principi di comportamento delineati dalla presente procedura, dal Modello e dal Codice Etico;
- ➢ riferire le principali notizie, informazioni e/o dati in proprio possesso connessi all'oggetto del procedimento penale, nonché consegnare (ove possibile) l'eventuale documentazione a supporto dell'autenticità delle proprie dichiarazioni;
- ➢ segnalare all'Autorità Giudiziaria ogni notizia relativa a presunte pressioni a non rendere dichiarazioni ovvero a rendere dichiarazioni mendaci da parte di terzi (ad es. aver subito violenze, minacce, dazioni di danaro o altra utilità, *etc.*).

Ancora, va precisato che ogni dichiarazione resa all'autorità giudiziaria o agli organi di controllo deve essere documentata, tracciata e conservata agli atti della Società, con indicazione del soggetto dichiarante, della data, dell'autorità destinataria, del contenuto essenziale e dei soggetti aziendali che ne hanno preso conoscenza.

Prima di rendere qualsiasi dichiarazione all'autorità giudiziaria o agli organi di vigilanza in nome o per conto della Società, il soggetto incaricato deve ricevere istruzioni specifiche dall'Organo Amministrativo o dal legale incaricato, secondo le procedure interne e il Modello 231.

In caso di ispezioni, accertamenti, richieste documentali, perquisizioni o qualsiasi altra attività degli organi di polizia giudiziaria o delle autorità di controllo presso le sedi aziendali, deve essere immediatamente informato l'Organo Amministrativo e, ove possibile, il legale incaricato. L'Organismo di Vigilanza deve essere informato tempestivamente dell'evento attraverso il relativo flusso informativo.

È vietato esercitare pressioni, indebite influenze o condizionamenti nei confronti di soggetti chiamati a rendere dichiarazioni all'autorità giudiziaria o di controllo, inclusi dipendenti, collaboratori, consulenti, testimoni o segnalanti.

PER QUANTO CONCERNE GLI ASPETTI OPERATIVI:

- i legali esterni devono essere nominati con apposita procura; solo i legali esterni ed esterni all'uopo autorizzati, si possono interfacciare con i soggetti coinvolti in procedimenti giudiziari o che sono chiamati a rendere dichiarazioni davanti all'Autorità Giudiziaria;
- la documentazione da inviare all'Autorità Giudiziaria (come ad es. mezzi probatori, atti di causa, scritti difensivi, *etc.*) deve essere verificata dai legali e sottoscritta dai soggetti coinvolti nel procedimento;
- in ogni caso, la Società verifica tutta la documentazione richiesta dall'Autorità Giudiziaria procedente.

In particolare, i Destinatari devono conformarsi, oltre che alla normativa vigente e al Modello 231, ai principi di legalità, integrità, lealtà processuale, veridicità, correttezza, riservatezza e prevenzione dei conflitti di interesse sanciti dal Codice Etico e dal Codice di Condotta aziendali.
È fatto divieto di introdurre, produrre o utilizzare nell'ambito di procedimenti giudiziari, arbitrali o amministrativi prove, documenti, dichiarazioni o elementi di prova che si sappia o si apprenda essere falsi, alterati o non corrispondenti al vero.
È fatto divieto di occultare, distruggere, alterare o sottrarre documentazione rilevante nell'ambito di contenziosi, ispezioni, accertamenti o procedimenti in corso o prevedibilmente imminenti.
Le dichiarazioni rese all'autorità giudiziaria, agli organi di polizia giudiziaria, alle autorità amministrative indipendenti, agli organi di vigilanza e di controllo devono essere veritiere, complete e non fuorvianti. È vietato rendere dichiarazioni non veritiere, reticenti, incomplete o idonee a indurre in errore l'autorità procedente, anche mediante condotte omissive.
Il dipendente o collaboratore che, nel corso di procedimenti giudiziari o ispettivi, venga a conoscenza di fatti rilevanti ai sensi del Modello 231, incluse condotte illecite di terzi, anomalie documentali o violazioni della normativa applicabile, è tenuto a informare tempestivamente l'Organismo di Vigilanza attraverso i canali previsti dalla Procedura Whistleblowing.
In ultimo, si precisa che è garantito il diritto al silenzio del soggetto che potrebbe essere accusato di un illecito passibile di sanzioni, nel rispetto dei principi costituzionali e convenzionali applicabili, come confermato dalla Corte Costituzionale con sentenza n. 84/2021.

6.1 PRESIDI ORGANIZZATIVI SPECIFICI DI BITCONTROL

Segregazione dei compiti: il PRES autorizza la strategia e gli atti dispositivi; il RCL cura l'analisi legale e il coordinamento difensivo; le funzioni tecniche competenti validano i fatti e gli aspetti progettuali; RAM/RRU e REC verificano gli impatti economici, contabili, fiscali e i pagamenti; RGAD assicura protocollo, fascicolazione, accessi e conservazione; l'OdV riceve i flussi informativi senza assumere compiti gestori.

REGISTRO CONTENZIOSI: ogni vertenza, reclamo rilevante, arbitrato, mediazione, ispezione e accordo transattivo è registrato con numero univoco, controparte, oggetto, commessa/CIG/CUP se presenti, valore, rischio, responsabile interno, legale incaricato, scadenze, stato, accantonamenti, coperture assicurative, esito e flussi all'OdV.

CANALIZZAZIONE DEGLI ATTI: PEC, notifiche, richieste delle Autorità e contestazioni devono essere protocollate il giorno della ricezione e inoltrate senza ritardo al PRES, al RCL e alle funzioni interessate; le scadenze sono inserite in uno scadenzario condiviso con almeno un controllo di secondo livello.

LEGAL HOLD: al sorgere o alla ragionevole prevedibilità di una controversia è disposto il blocco della cancellazione di documenti, e-mail, log, configurazioni, versioni software, ticket, report di collaudo, verbali, fotografie e ulteriori evidenze pertinenti. Sono documentati fonte, data di estrazione, integrità, custodia e accessi, evitando alterazioni degli originali.

PRESIDIO TECNICO: per controversie su sistemi di telecontrollo e automazione, la funzione tecnica redige una relazione oggettiva che ricostruisca requisiti contrattuali, versioni software, modifiche, test, collaudi, log di sistema, SLA, interventi e dipendenze da infrastrutture del cliente o di terzi; ogni valutazione tecnica è separata dalla decisione negoziale o transattiva.

CONSULENTI ESTERNI: gli incarichi sono conferiti per iscritto a professionisti qualificati, previa verifica di competenza, indipendenza, conflitti di interesse, congruità del compenso, riservatezza, sicurezza informatica, obblighi 231 e tracciabilità. L'eventuale deroga all'albo fornitori deve essere motivata e autorizzata.

PAGAMENTI E TRANSAZIONI: sono vietati pagamenti in contanti, su conti non intestati alla controparte o al professionista incaricato, in Paesi diversi da quello della controparte senza giustificazione, nonché compensi collegati all'ottenimento di favori o decisioni. Ogni pagamento è riconciliato con incarico, fattura, accordo e autorizzazione.

CONFLITTI DI INTERESSE: chiunque partecipi alla gestione della vertenza dichiara tempestivamente rapporti personali, professionali o economici con controparti, legali, consulenti, periti, arbitri, mediatori, pubblici ufficiali o incaricati di pubblico servizio coinvolti e si astiene fino alla decisione del PRES.

COPERTURE ASSICURATIVE: il responsabile interno verifica tempestivamente obblighi e termini di denuncia del sinistro, preservando i diritti della Società e coordinando ogni comunicazione con il broker o l'assicuratore.

SICUREZZA E RISERVATEZZA: i fascicoli sono conservati nella piattaforma aziendale autorizzata con accessi profilati, autenticazione, backup e logging coerenti con il sistema ISO/IEC 27001; è vietato utilizzare account personali, dispositivi o canali non autorizzati per scambiare documenti di causa.

6.1.1 PRESIDI SPECIFICI PER GLI ACCORDI TRANSATTIVI

La proposta di transazione è corredata da una nota motivata contenente fatti, pretese contrapposte, probabilità di soccombenza, valore economico, costi e tempi attesi, alternative disponibili, effetti fiscali e contabili, impatti su commesse pubbliche, certificazioni, reputazione e continuità del servizio.

La congruità economica è verificata mediante criteri documentati e, per operazioni rilevanti o atipiche, con un secondo parere legale, tecnico o economico indipendente.

L'accordo è autorizzato dal soggetto munito di poteri coerenti con valore e oggetto; quando comporta rinunce, riconoscimenti di responsabilità, cessione di diritti di proprietà intellettuale, impegni pluriennali o importi significativi, è richiesta specifica delibera del CDA.

La transazione non può contenere clausole dirette a impedire segnalazioni alle Autorità, all'OdV o tramite whistleblowing, né a occultare illeciti, alterare prove, eludere sanzioni, obblighi fiscali, contributivi, di sicurezza, ambientali o di protezione dei dati.

Prima della firma sono verificati poteri di rappresentanza della controparte, coordinate bancarie, assenza di conflitti, adempimenti sanzionatori e, quando applicabile, compatibilità con il contratto pubblico, con l'autorizzazione della stazione appaltante e con i vincoli di tracciabilità finanziaria.

Mentre, nel caso in cui qualunque Destinatario del Modello è chiamato - in qualità di imputato o coimputato in un procedimento penale connesso o collegato - a rendere dichiarazioni innanzi all'Autorità Giudiziaria, lo stesso deve osservare i seguenti principi comportamentali:

garantire che ogni attività collaborativa su richiesta dell'Autorità Giudiziaria e secondo le indicazioni formulate dalla stessa, deve essere svolta nell'assoluto rispetto dei principi di comportamento delineati dalla presente procedura, dal Modello e dal Codice Etico;

riferire le principali notizie, informazioni e/o dati in proprio possesso connessi all'oggetto del procedimento penale, nonché consegnare (ove possibile) l'eventuale documentazione a supporto dell'autenticità delle proprie dichiarazioni;

segnalare all'Autorità Giudiziaria ogni notizia relativa a presunte pressioni a non rendere dichiarazioni ovvero a rendere dichiarazioni mendaci da parte di terzi (ad es. aver subito violenze, minacce, dazioni di danaro o altra utilità, etc.).

Ancora, va precisato che ogni dichiarazione resa all'autorità giudiziaria o agli organi di controllo deve essere documentata, tracciata e conservata agli atti della Società, con indicazione del soggetto dichiarante, della data, dell'autorità destinataria, del contenuto essenziale e dei soggetti aziendali che ne hanno preso conoscenza.

Prima di rendere qualsiasi dichiarazione all'autorità giudiziaria o agli organi di vigilanza in nome o per conto della Società, il soggetto incaricato deve ricevere istruzioni specifiche dall'Organo Amministrativo o dal legale incaricato, secondo le procedure interne e il Modello 231. Prima di rendere dichiarazioni in nome o per conto della Società, il soggetto autorizzato si coordina con il PRES e con il legale incaricato, fermo restando che le dichiarazioni personali devono essere rese

liberamente, senza istruzioni sul contenuto e nel rispetto del diritto di difesa, del diritto al silenzio e del divieto di qualsiasi pressione o condizionamento.
In caso di ispezioni, accertamenti, richieste documentali, perquisizioni o qualsiasi altra attività degli organi di polizia giudiziaria o delle autorità di controllo presso le sedi aziendali, deve essere immediatamente informato l'Organo Amministrativo e, ove possibile, il legale incaricato. L'Organismo di Vigilanza deve essere informato tempestivamente dell'evento attraverso il relativo flusso informativo.

PROTOCOLLO OPERATIVO IN CASO DI ACCESSO O ISPEZIONE:

1. verificare l'identità e il titolo degli operanti, acquisire copia del provvedimento o della richiesta e annotare orario di ingresso e uscita, locali interessati e documenti richiesti;
2. assicurare piena collaborazione senza ostacolare le operazioni, senza distruggere, occultare o modificare dati e senza rendere dichiarazioni improvvisate per conto della Società;
3. designare un referente aziendale e, ove possibile, far intervenire il legale; mantenere un elenco dei documenti e dispositivi consegnati o acquisiti, richiedendo ricevuta o verbale;
4. preservare continuità e sicurezza degli impianti e dei sistemi dei clienti, informando gli operanti degli eventuali rischi operativi senza opporre esigenze tecniche come pretesto per ritardare o impedire l'attività;
5. redigere al termine un rapporto interno riservato, conservarlo nel fascicolo e trasmettere il flusso informativo all'OdV.

È vietato esercitare pressioni, indebite influenze o condizionamenti nei confronti di soggetti chiamati a rendere dichiarazioni all'autorità giudiziaria o di controllo, inclusi dipendenti, collaboratori, consulenti, testimoni o segnalanti.

PER QUANTO CONCERNE GLI ASPETTI OPERATIVI:

1. i legali esterni devono essere nominati con apposita procura; solo i legali esterni ed esterni all'uopo autorizzati, si possono interfacciare con i soggetti coinvolti in procedimenti giudiziari o che sono chiamati a rendere dichiarazioni davanti all'Autorità Giudiziaria; i legali esterni devono essere incaricati con lettera di incarico e, quando necessario, apposita procura. I rapporti con Autorità, controparti, testimoni, consulenti tecnici e altri soggetti coinvolti sono tenuti esclusivamente dai soggetti autorizzati, nel rispetto delle prerogative difensive e senza interferire con la libertà delle dichiarazioni;

2. la documentazione da inviare all'Autorità Giudiziaria (come ad es. mezzi probatori, atti di causa, scritti difensivi, etc.) deve essere verificata dai legali e sottoscritta dai soggetti coinvolti nel procedimento;

3. in ogni caso, la Società verifica tutta la documentazione richiesta dall'Autorità Giudiziaria procedente.

In particolare, i Destinatari devono conformarsi, oltre che alla normativa vigente e al Modello 231, ai principi di legalità, integrità, lealtà processuale, veridicità, correttezza, riservatezza e prevenzione dei conflitti di interesse sanciti dal Codice Etico e dal Codice di Condotta aziendali.
È fatto divieto di introdurre, produrre o utilizzare nell'ambito di procedimenti giudiziari, arbitrali o amministrativi prove, documenti, dichiarazioni o elementi di prova che si sappia o si apprenda essere falsi, alterati o non corrispondenti al vero.
È fatto divieto di occultare, distruggere, alterare o sottrarre documentazione rilevante nell'ambito di contenziosi, ispezioni, accertamenti o procedimenti in corso o prevedibilmente imminenti.
Le dichiarazioni rese all'autorità giudiziaria, agli organi di polizia giudiziaria, alle autorità amministrative indipendenti, agli organi di vigilanza e di controllo devono essere veritiere, complete e non fuorvianti. È vietato rendere dichiarazioni non veritiere, reticenti, incomplete o idonee a indurre in errore l'autorità procedente, anche mediante condotte omissive.
Il dipendente o collaboratore che, nel corso di procedimenti giudiziari o ispettivi, venga a conoscenza di fatti rilevanti ai sensi del Modello 231, incluse condotte illecite di terzi, anomalie documentali o violazioni della normativa applicabile, è tenuto a informare tempestivamente l'Organismo di Vigilanza attraverso i canali previsti dalla Procedura Whistleblowing.
In ultimo, si precisa che è garantito il diritto al silenzio del soggetto che potrebbe essere accusato di un illecito passibile di sanzioni, nel rispetto dei principi costituzionali e convenzionali applicabili, come confermato dalla Corte Costituzionale con sentenza n. 84/2021.

6.2 UTILIZZO DI STRUMENTI DI IA NELLA GESTIONE DEL CONTENZIOSO E NELLA PREPARAZIONE DI DICHIARAZIONI

L'utilizzo di strumenti di Intelligenza Artificiale nella gestione dei contenziosi, nella predisposizione di memorie difensive, dichiarazioni, note, schede di sintesi, reportistica legale o di altra documentazione da trasmettere all'autorità giudiziaria, agli organi di vigilanza o alle controparti è consentito esclusivamente nel rispetto della Policy IA aziendale, del Codice Etico, del Codice di Condotta e del Modello 231.
Ogni output generato da un sistema di IA deve essere validato da una persona autorizzata prima di essere trasmesso all'esterno, sottoscritto, depositato o utilizzato come documento ufficiale. L'IA non

può assumere decisioni autonome che producano effetti giuridici o rilevanti nell'ambito di procedimenti giudiziari o amministrativi.

È espressamente vietato inserire in strumenti di IA esterni non approvati: atti giudiziari riservati, estratti di procedimenti penali o civili, informazioni su indagini in corso, dati personali delle parti, testimoni o segnalanti, contenuto di dichiarazioni all'autorità, documentazione relativa a contenziosi riservati, condizioni di accordi transattivi, pareri legali riservati o qualsiasi altra informazione classificata come confidenziale o soggetta al segreto professionale.

Tutti i processi di preparazione di atti, dichiarazioni o documenti nei quali siano impiegati strumenti di IA devono essere soggetti a logging, tracciabilità dei prompt e degli output, conservazione documentale, revisione umana e, ove necessario, valutazione preventiva del rischio ai sensi della Policy IA.

Qualsiasi anomalia, incidente informatico o uso improprio di strumenti di IA connesso ai processi disciplinati dalla presente Procedura deve essere segnalato immediatamente al Responsabile Sicurezza Informatica, al DPO ove coinvolti dati personali e all'Organismo di Vigilanza.

7 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutti i *Destinatari* coinvolti nella gestione dei rapporti con l'Autorità Giudiziaria, nel caso di procedimenti penali, informano tempestivamente l'Organismo di Vigilanza di situazioni anomale e/o in contrasto con la presente procedura, nonché di eventuali comportamenti non conformi alle disposizioni del Codice Etico.

Inoltre, i *Destinatari* devono informare tempestivamente l'Organismo di Vigilanza di essere a conoscenza di procedimenti giudiziari incardinati nei confronti dei soggetti che operano nella BitControl S.r.l.

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 nell'apposita piattaforma informatica di condivisione – tutta la documentazione necessaria.

L'ODV DOVRÀ, IN PARTICOLARE, 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.
- notifica di ogni atto giudiziario, avviso di garanzia, richiesta di informazioni, comunicazione di ispezione o accertamento, atto di indagine o provvedimento cautelare ricevuto dalla Società o da suoi esponenti in ragione delle funzioni aziendali;

– esito di ogni procedimento giudiziario, arbitrale o amministrativo rilevante ai fini del Modello 231, ivi incluse sentenze, provvedimenti disciplinari o accordi transattivi conclusi;

- anomalie rilevate nella gestione documentale dei contenziosi, nella predisposizione di atti o dichiarazioni, nella selezione o nel coordinamento dei consulenti legali, incluse eventuali pressioni o interferenze indebite;

- utilizzo di strumenti di IA nei processi disciplinati dalla presente Procedura, con indicazione delle finalità, degli strumenti autorizzati impiegati, dei controlli svolti sugli output e delle eventuali criticità riscontrate;

- segnalazioni whistleblowing ricevute aventi ad oggetto fatti rilevanti per i processi di contenzioso, accordi transattivi e dichiarazioni all'autorità;

- variazioni dei soggetti delegati alla gestione del contenzioso, alla firma di atti processuali o transattivi e ai contatti con l'autorità giudiziaria, incluse le nuove assunzioni formalizzate dal 01.04.2026 ove inserite in processi rilevanti.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

Sommario

1 OBIETTIVI E FINALITÀ DELLA PROCEDURA

La presente procedura definisce i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento adottati dalla BITCONTROL S.r.l. nell'ambito del processo di gestione e di selezione dei fornitori di beni, servizi ed incarichi professionali (definiti ai fini della presente procedura, "partner commerciali").

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 IN OGGETTO 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 la BITCONTROL 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;

 scegliere i partner commerciali solo dopo aver svolto idonee verifiche sulla reputazione e sulla affidabilità sul mercato degli stessi.

Ai fini della presente procedura, per consulenza si intende la richiesta di prestazione rivolta ad un professionista o ad una società di consulenza, che consiglia ed assiste il proprio cliente nello svolgimento delle proprie attività o fornisce informazioni e pareri che possono migliorare l'migliorare l'attività della società, promuovendone lo sviluppo.

Elemento caratterizzante del rapporto di consulenza è la fiducia tra committente e consulente, che può fondarsi su un rapporto consolidato, sulla notorietà del consulente o sui titoli accademici e professionali posseduti dallo stesso.

È, comunque, 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.

Dunque, la presente procedura disciplina la selezione e la gestione dei partner commerciali e, con specifico riguardo ai rischi di corruzione pubblica e privata, regola l'offerta, la promessa, la concessione, la ricezione e la restituzione di omaggi, ospitalità, spese di rappresentanza, liberalità, contributi, donazioni e sponsorizzazioni.

La procedura è finalizzata a garantire che tali iniziative siano lecite, trasparenti, proporzionate, coerenti con l'attività e con l'immagine di BITCONTROL S.r.l., correttamente autorizzate, documentate e contabilizzate, nonché inidonee a influenzare l'indipendenza di giudizio del destinatario o a conseguire vantaggi impropri per la Società o per terzi.

Restano ferme le disposizioni della PMOG 01 in materia di tesoreria e pagamenti, nonché le ulteriori procedure aziendali applicabili ai processi di acquisto, contabilità, gare, whistleblowing e gestione documentale.

2 DEFINIZIONI E ACRONIMI

OMAGGI: beni o utilità concessi o ricevuti senza corrispettivo, compresi gadget, buoni, voucher, prodotti, servizi, agevolazioni e altri vantaggi economicamente apprezzabili.

OSPITALITÀ: pasti, rinfreschi, pernottamenti, trasferimenti, partecipazioni a eventi, fiere o iniziative di rappresentanza offerti o ricevuti nell'ambito di relazioni istituzionali o commerciali.

SPESE DI RAPPRESENTANZA: spese sostenute per finalità promozionali, istituzionali o di pubbliche relazioni, coerenti con l'attività e con l'immagine della Società.

LIBERALITÀ/BENEFICENZA: erogazioni gratuite in denaro o natura prive di controprestazione, effettuate per finalità solidaristiche, sociali, culturali o di interesse generale.

SPONSORIZZAZIONE: contratto a prestazioni corrispettive mediante il quale BITCONTROL sostiene un soggetto o un'iniziativa ricevendo una controprestazione promozionale e documentabile.

PUBBLICA AMMINISTRAZIONE O P.A.: qualsiasi amministrazione, ente, autorità, società pubblica o soggetto che eserciti pubbliche funzioni o servizi, inclusi pubblici ufficiali, incaricati di pubblico servizio, funzionari dell'Unione europea e soggetti a essi collegati.

SOGGETTI COLLEGATI: coniuge, convivente, parenti, affini, società, associazioni o altri soggetti riconducibili al destinatario dell'utilità.

REGISTRO OMAGGI: archivio aziendale nel quale sono annotati gli omaggi e le altre utilità offerte, promesse, ricevute, rifiutate, restituite o devolute.

CDA	Consiglio di Amministrazione
PRES	Presidente del CDA
RSPP	Responsabile del Servizio di Prevenzione e Protezione
RSGQ	Responsabile del 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
OdV	Organismo di Vigilanza

RCA	Responsabile Interno Conformità Anticorruzione

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E AI RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RINVIA ALL'ORGANIGRAMMA AZIENDALE VIGENTE DI BITCONTROL S.R.L.

3 RIFERIMENTI NORMATIVI E DOCUMENTI AZIENDALI

- D.Lgs. 8 giugno 2001, n. 231 e successive modifiche e integrazioni, con particolare riferimento agli artt. 24 e 25 e ai reati di corruzione, induzione indebita e istigazione alla corruzione;
- artt. 318, 319, 319-ter, 319-quater, 320, 321, 322, 322-bis e 346-bis c.p.; artt. 2635 e 2635-bis c.c.;
- Legge 6 novembre 2012, n. 190; D.P.R. 16 aprile 2013, n. 62, come modificato dal D.P.R. 13 giugno 2023, n. 81, quale parametro di prudenza nei rapporti con dipendenti pubblici;
- D.Lgs. 31 marzo 2023, n. 36 e s.m.i., con particolare riguardo ai principi di imparzialità, trasparenza, conflitto di interessi e tracciabilità nelle procedure di affidamento ed esecuzione;
- D.Lgs. 10 marzo 2023, n. 24 in materia di segnalazioni whistleblowing;
- art. 108, comma 2, D.P.R. 22 dicembre 1986, n. 917, ai soli fini fiscali e senza automatica coincidenza con le soglie autorizzative della presente procedura;
- Codice Etico BITCONTROL approvato il 25 giugno 2026; Politica Anticorruzione; Misure Integrative del Modello 231 in materia di anticorruzione e trasparenza 2025-2028; PMOG 03 Rev. 8; Procedura Whistleblowing; PMOG 01 Gestione tesoreria.

4 CAMPO DI APPLICAZIONE E DESTINATARI

La procedura si applica agli amministratori, ai dipendenti, ai collaboratori, ai consulenti, ai procuratori e a chiunque operi, anche occasionalmente, in nome o per conto di BITCONTROL, nonché, per quanto compatibile, ai partner commerciali e ai terzi coinvolti nelle attività disciplinate.

Rientrano nel campo di applicazione tutte le utilità offerte o ricevute in occasione di rapporti con clienti, fornitori, consulenti, partner, concorrenti, pubbliche amministrazioni, autorità, stazioni appaltanti, enti concedenti, organismi ispettivi e soggetti che esercitano funzioni pubbliche.

5 RUOLI E RESPONSABILITÀ

- Il CDA approva la presente procedura e le sue revisioni, definisce gli indirizzi generali e autorizza le operazioni riservate alla propria competenza.

- Il PRES autorizza gli omaggi, le ospitalità, le liberalità e le sponsorizzazioni secondo le soglie e le condizioni previste; assicura che non sussistano finalità improprie o conflitti di interesse.
- Il RCOM/APVG cura la fase istruttoria, verifica il destinatario, la finalità, il valore, la congruità, l'eventuale collegamento con gare o procedimenti e aggiorna il Registro Omaggi.
- Il RAM/RRU assicura la diffusione della procedura, la formazione e la raccolta delle dichiarazioni dei Destinatari.
- Il RGAD assicura la conservazione ordinata della documentazione nella piattaforma aziendale.
- Il REC verifica la corretta imputazione contabile e fiscale e la coerenza tra autorizzazione, giustificativo, fattura e pagamento.
- L'OdV vigila sull'osservanza della procedura, riceve i flussi informativi e può richiedere documenti, chiarimenti e controlli a campione.

6 PRINCIPI GENERALI E DIVIETI

Ogni omaggio o utilità deve rispettare congiuntamente i principi di legalità, correttezza, trasparenza, ragionevolezza, occasionalità, proporzionalità, tracciabilità, sobrietà e coerenza con le ordinarie relazioni istituzionali o commerciali.

- offrire, promettere, sollecitare o ricevere denaro contante, strumenti equivalenti al contante, carte prepagate, criptovalute, prestiti personali o altri vantaggi facilmente monetizzabili;
- offrire o ricevere utilità per ottenere, mantenere o remunerare un trattamento favorevole, influenzare una decisione, accelerare una pratica o aggirare controlli e procedure;
- frazionare omaggi, spese o rimborsi per eludere soglie autorizzative, controlli o registrazioni;
- utilizzare fondi personali, note spese, intermediari, consulenti, partner, familiari o soggetti collegati per effettuare utilità che la Società non potrebbe legittimamente concedere;
- offrire utilità durante gare, affidamenti, rinnovi contrattuali, contenziosi, ispezioni, verifiche, procedimenti autorizzativi o richieste di contributi, salvo meri gadget istituzionali preventivamente autorizzati e comunque mai destinati al soggetto coinvolto nella decisione;
- concedere o ricevere utilità in forma anonima, non documentata, non contabilizzata o mediante descrizioni generiche o non veritiere;
- offrire utilità a partiti, movimenti politici, organizzazioni sindacali o loro esponenti, salvo quanto consentito dalla legge e previa specifica delibera del CDA.

Il superamento delle soglie economiche indicate non rende automaticamente lecita o illecita l'operazione: anche un'utilità di valore inferiore è vietata quando, per contesto, frequenza, destinatario o finalità, possa apparire idonea a influenzare l'indipendenza di giudizio.

7 SELEZIONE E GESTIONE DEI PARTNER COMMERCIALI

La selezione dei partner commerciali deve essere effettuata sulla base di esigenze effettive, criteri oggettivi di competenza, affidabilità, qualità, convenienza e reputazione, garantendo la tracciabilità dell'iter decisionale e l'assenza di conflitti di interesse.

- Per importi superiori a euro 5.000,00 è richiesta una valutazione comparativa o una motivazione scritta della scelta, privilegiando i fornitori qualificati, ove disponibili.
- I contratti o i preventivi accettati devono essere sottoscritti dal soggetto munito dei necessari poteri e contenere clausole 231, anticorruzione, tracciabilità, whistleblowing e risoluzione in caso di violazioni rilevanti.
- Prima dell'affidamento devono essere svolte verifiche proporzionate sul titolare effettivo, sulla reputazione, sulle eventuali relazioni con pubblici ufficiali e sull'assenza di indicatori di rischio o richieste anomale.
- Sono vietati compensi non congrui, commissioni prive di giustificazione, pagamenti su conti di terzi o in Paesi non collegati alla prestazione, nonché prestazioni immateriali prive di evidenze verificabili.

8 GESTIONE DEGLI OMAGGI E DELLE UTILITÀ - REGOLE GENERALI

Gli omaggi aziendali sono ammessi soltanto quando di modico valore, occasionali, destinati a finalità istituzionali o promozionali, coerenti con le consuetudini lecite e privi di qualsiasi collegamento con decisioni o vantaggi attesi.

Ai fini della presente procedura, costituisce soglia ordinaria di modico valore l'importo massimo di euro 50,00 per singolo omaggio, IVA inclusa. Tale soglia è un limite interno e non costituisce un'automatica autorizzazione: restano necessari la verifica del contesto, l'autorizzazione prevista e la registrazione.

Il valore complessivo degli omaggi offerti allo stesso destinatario o a soggetti a esso collegati non può superare euro 100,00 nell'arco di dodici mesi, salvo iniziative istituzionali rivolte indistintamente a una pluralità di destinatari e preventivamente autorizzate dal PRES.

Sono comunque vietati denaro, buoni acquisto, voucher generici, titoli, sconti personali non commerciali, servizi gratuiti, assunzioni o incarichi a favore del destinatario o di soggetti collegati, salvo che rientrino in processi ordinari, trasparenti e indipendenti.

9 OMAGGI E UTILITÀ NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

Nei rapporti con la Pubblica Amministrazione si applicano criteri di massima prudenza e le prescrizioni della PMOG 03. È vietato offrire, promettere o concedere denaro, omaggi, ospitalità o altre utilità a pubblici ufficiali, incaricati di pubblico servizio, funzionari europei o soggetti collegati quando l'utilità sia correlata, anche indirettamente, all'esercizio della funzione o a una decisione di interesse per BITCONTROL.

Gli omaggi di cortesia a soggetti pubblici sono ammessi solo se simultaneamente: di valore unitario non superiore a euro 25,00; recanti il marchio aziendale o aventi natura meramente istituzionale; non ripetuti; non offerti durante o in prossimità di gare, verifiche, ispezioni, autorizzazioni, contenziosi, pagamenti, rinnovi o altri procedimenti; preventivamente autorizzati per iscritto dal PRES e registrati.

Qualora il codice di comportamento o la disciplina interna dell'amministrazione destinataria preveda limiti inferiori o divieti più rigorosi, prevalgono tali disposizioni. In caso di dubbio, l'omaggio non deve essere effettuato e deve essere richiesto il parere dell'Ufficio Legale o dell'OdV.

È vietata qualsiasi utilità richiesta o suggerita dal soggetto pubblico. Ogni richiesta anomala, sollecitazione o promessa di trattamento favorevole deve essere immediatamente interrotta, documentata e segnalata al PRES e all'OdV, oltre che mediante il canale whistleblowing ove ne ricorrano i presupposti.

10 OMAGGI E UTILITÀ NEI RAPPORTI CON SOGGETTI PRIVATI

Nei rapporti con clienti, fornitori e partner privati, gli omaggi sono ammessi entro il limite ordinario di euro 50,00 per singolo omaggio e nel limite cumulativo annuo di euro 100,00 per destinatario, purché non siano idonei a condizionare scelte commerciali o professionali.

Gli omaggi rivolti a soggetti che partecipano alla selezione di fornitori, alla negoziazione di contratti, alla validazione di prestazioni o all'autorizzazione di pagamenti sono vietati nel periodo compreso tra l'avvio della procedura e i trenta giorni successivi alla decisione o al pagamento finale.

Gli omaggi collettivi o promozionali destinati a una categoria omogenea di clienti o partner devono essere previamente pianificati, autorizzati e documentati mediante elenco dei destinatari, costo unitario, finalità e materiale promozionale utilizzato.

11 OMAGGI E UTILITÀ RICEVUTI DAI DESTINATARI

I Destinatari non possono sollecitare omaggi o utilità. Gli omaggi ricevuti di valore presumibilmente non superiore a euro 50,00 possono essere accettati soltanto se occasionali, conformi alle normali relazioni di cortesia e non collegati a decisioni di competenza del ricevente.

Ogni omaggio ricevuto deve essere comunicato entro cinque giorni lavorativi al RCOM/APVG o al RAM/RRU per la registrazione. Gli omaggi di valore superiore a euro 50,00, ripetuti o comunque inopportuni devono essere rifiutati o restituiti con comunicazione scritta. Se la restituzione non è possibile o risulta sconveniente, il bene è consegnato alla Società per la devoluzione a finalità aziendali o benefiche, con tracciabilità della destinazione.

Sono sempre vietati e devono essere immediatamente restituiti denaro, buoni, voucher, prestazioni personali, viaggi, soggiorni, sconti non commerciali, opportunità di investimento, incarichi o vantaggi a favore di familiari o soggetti collegati.

12 OSPITALITÀ, PASTI, TRASFERTE E SPESE DI RAPPRESENTANZA

Pasti, eventi e forme di ospitalità possono essere offerti o accettati soltanto quando funzionali a un incontro di lavoro, proporzionati, non lussuosi, occasionali, con presenza del referente aziendale e documentati mediante indicazione dei partecipanti, della finalità e del collegamento con l'attività svolta.

Salvo preventiva autorizzazione del PRES, il valore massimo è fissato in euro 75,00 per persona per pasti e rinfreschi e in euro 150,00 per persona per eventi o iniziative comprensive di più servizi. Per i soggetti pubblici si applicano limiti più restrittivi e, di regola, BITCONTROL sostiene esclusivamente le spese direttamente connesse all'incontro istituzionale, evitando trasferte, pernottamenti o intrattenimenti.

È vietato rimborsare direttamente al destinatario spese non documentate. Le spese devono essere pagate, ove possibile, direttamente al fornitore del servizio e contabilizzate in modo analitico.

13 LIBERALITÀ, BENEFICENZA E SPONSORIZZAZIONI

Le liberalità e le sponsorizzazioni devono rispondere a finalità lecite, coerenti con i valori aziendali, non discriminatorie e non possono costituire mezzo per ottenere vantaggi impropri, creare fondi occulti o remunerare decisioni favorevoli.

- Il beneficiario deve essere identificato e sottoposto a verifica reputazionale, con acquisizione di statuto, finalità, dati fiscali, titolarità effettiva e dichiarazione sull'assenza di conflitti di interesse o collegamenti impropri con pubblici ufficiali.

- La sponsorizzazione deve essere regolata da contratto scritto che descriva le controprestazioni, gli obblighi di rendicontazione, le modalità di utilizzo del marchio e il diritto di controllo e risoluzione.
- Le erogazioni devono essere effettuate esclusivamente con strumenti tracciabili sul conto intestato al beneficiario; sono vietati pagamenti in contanti o a soggetti diversi.
- Devono essere acquisite evidenze dell'effettiva realizzazione dell'iniziativa: report, fotografie, materiali, pubblicazioni, dati di visibilità e rendiconto delle attività.

L'importo annuo complessivo destinato a liberalità e sponsorizzazioni è definito dal CDA in sede di budget. Ogni singola iniziativa è autorizzata dal PRES fino a euro 1.000,00; oltre tale importo è richiesta preventiva delibera del CDA. È eliminato il precedente automatismo che fissava in euro 1.000,00 il limite annuo complessivo, sostituito da un sistema di budget, istruttoria e autorizzazione.

14 ITER AUTORIZZATIVO E REGISTRO OMAGGI

Prima di offrire, promettere o sostenere una spesa rientrante nella presente procedura, il richiedente compila il Modulo di cui all'Allegato A indicando: soggetto proponente; destinatario e organizzazione di appartenenza; eventuale qualifica pubblica; descrizione e valore; finalità; data; rapporto in corso; presenza di gare, procedimenti, verifiche o decisioni pendenti; precedenti utilità nei dodici mesi; centro di costo e documenti giustificativi.

L'autorizzazione deve precedere l'acquisto o l'impegno di spesa. Le urgenze devono essere motivate e autorizzate prima della consegna dell'utilità. Non è ammessa la ratifica successiva, salvo eventi eccezionali e documentati sottoposti al PRES e comunicati all'OdV.

Fattispecie	Soglia/condizione	Autorizzazione	Registrazione
Omaggi privati	fino a € 50 per singolo; max € 100 annui	PRES o delegato formalmente	Sempre
Omaggi a soggetti pubblici	fino a € 25 e sole condizioni del § 9	PRES, previa istruttoria scritta	Sempre e flusso OdV
Pasti/ospitalità	entro limiti del § 12	Responsabile di funzione e PRES nei casi PA o oltre soglia	Sempre se verso PA; altrimenti oltre € 50

Liberalità/sponsorizzazioni	fino a € 1.000 singola iniziativa	PRES	Sempre
Liberalità/sponsorizzazioni	oltre € 1.000	CDA	Sempre e flusso OdV
Utilità ricevute	qualsiasi valore	Comunicazione; restituzione/devoluzione oltre € 50	Sempre

15 CONTROLLI, ARCHIVIAZIONE E TRACCIABILITÀ

Il RCOM/APVG mantiene il Registro Omaggi secondo l'Allegato B; il RGAD conserva in piattaforma aziendale le richieste, le autorizzazioni, i documenti fiscali, le comunicazioni di restituzione, le verifiche reputazionali e le evidenze dell'iniziativa.

La documentazione è conservata per almeno dieci anni, salvo termini più lunghi previsti dalla legge o connessi a contenziosi, procedimenti o richieste dell'Autorità. L'accesso è riservato ai soggetti autorizzati e all'OdV.

Il REC esegue controlli di coerenza tra Registro, contabilità, note spese e pagamenti. Almeno annualmente il PRES dispone un controllo a campione su destinatari, cumulo delle utilità, autorizzazioni e congruità dei costi.

16 FLUSSI INFORMATIVI, REPORT ANNUALE ALL'ODV E WHISTLEBLOWING

Devono essere comunicati tempestivamente all'OdV: richieste anomale; omaggi o utilità rifiutati o restituiti; violazioni o deroghe; tentativi di frazionamento; utilità connesse a soggetti pubblici; sponsorizzazioni o liberalità superiori a euro 1.000,00; carenze documentali; anomalie contabili; conflitti di interesse e operazioni con soggetti collegati.

Entro il 31 gennaio di ogni anno, il RCOM/APVG, con il supporto del RAM/RRU, del RGAD e del REC per gli ambiti di rispettiva competenza, predispone e trasmette all'OdV un Report annuale riepilogativo di tutti gli omaggi e delle altre utilità effettuati da BITCONTROL nel corso dell'anno solare precedente, indipendentemente dal relativo valore e dalla natura pubblica o privata del destinatario.

Il Report annuale deve contenere almeno: data dell'operazione; soggetto richiedente e funzione aziendale; destinatario e organizzazione di appartenenza; eventuale qualifica pubblica; descrizione dell'omaggio o dell'utilità; valore unitario e complessivo; finalità e occasione; estremi dell'autorizzazione; indicazione di

eventuali gare, procedimenti, verifiche o rapporti contrattuali in corso; documenti giustificativi; annotazione di eventuali anomalie, rifiuti, restituzioni o deroghe.

Il Report annuale deve essere sottoscritto dal RCOM/APVG e vistato dal PRES prima della trasmissione all'OdV. Qualora nell'anno di riferimento non siano stati effettuati omaggi o altre utilità, deve essere comunque trasmessa all'OdV una dichiarazione negativa espressa.

L'obbligo di reportistica annuale non sostituisce le comunicazioni tempestive all'OdV previste per richieste anomale, violazioni, deroghe, utilità connesse a soggetti pubblici, tentativi di frazionamento, conflitti di interesse o altre circostanze rilevanti ai fini del Modello 231.

Le violazioni della presente procedura possono essere segnalate attraverso il canale interno di whistleblowing, nel rispetto del D.Lgs. 24/2023 e della Procedura Whistleblowing aziendale. Sono vietate ritorsioni nei confronti del segnalante e degli altri soggetti protetti.

17 SISTEMA DISCIPLINARE

La violazione della presente procedura, l'omessa autorizzazione o registrazione, la falsa o incompleta rappresentazione delle circostanze, l'occultamento di utilità o la mancata segnalazione di anomalie costituiscono violazione del Modello 231 e possono determinare l'applicazione delle sanzioni previste dal sistema disciplinare, ferme restando le responsabilità civili, amministrative e penali.

Nei confronti di consulenti, fornitori e partner trovano applicazione i rimedi contrattuali, compresi sospensione dei pagamenti, risoluzione, richiesta di risarcimento e segnalazione alle autorità competenti.

18 ARCHIVIAZIONE

Tutta la documentazione prodotta nell'ambito del processo di approvvigionamento di beni, servizi e incarichi professionali è archiviata a cura del RCOM/APVG, o da Responsabile di funzione eventualmente incaricato, con il supporto del RGAD.

I regali offerti devono essere documentati in modo adeguato per consentire le eventuali verifiche.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

ALLEGATO A MODULO DI RICHIESTA E AUTORIZZAZIONE

Richiedente / funzione	
Tipologia	☐ omaggio ☐ ospitalità ☐ spesa di rappresentanza ☐ liberalità ☐ sponsorizzazione
Destinatario e organizzazione	
Qualifica pubblica o collegamento con P.A.	☐ No ☐ Sì, specificare:
Descrizione dell'utilità	
Valore unitario e complessivo	
Finalità e occasione	
Rapporti/procedimenti/gare in corso	☐ No ☐ Sì, specificare:
Utilità già offerte/ricevute nei 12 mesi	
Documenti allegati	
Valutazione conflitto di interesse	

Esito	☐ Autorizzato ☐ Non autorizzato ☐ Autorizzato con prescrizioni
Data e firma autorizzatore	

ALLEGATO B REGISTRO OMAGGI E UTILITÀ

Il Registro può essere tenuto in formato elettronico nella piattaforma aziendale e deve contenere almeno i seguenti campi:

Data	Offerto/Ricevuto	Destinatario/Mittente	P.A.?	Descrizione	Valore	Autorizzazione/Esito	Note e documenti

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

Sommario

1 OBIETTIVI E FINALITÀ

La presente procedura disciplina la ricerca, selezione e valutazione delle opportunità di gara, la decisione di partecipazione, la predisposizione e presentazione delle offerte, la gestione dei rapporti con le stazioni appaltanti e gli enti concedenti, nonché la stipula e l'esecuzione dei contratti pubblici e privati affidati a BITCONTROL S.r.l.

La procedura è finalizzata a garantire legalità, trasparenza, concorrenza, correttezza, tracciabilità, segregazione delle funzioni, attendibilità delle dichiarazioni, protezione delle informazioni riservate e prevenzione dei reati rilevanti ai sensi del D.Lgs. 231/2001, con particolare riguardo ai reati contro la P.A., alla turbata libertà degli incanti e del procedimento di scelta del contraente,

alla frode nelle pubbliche forniture, ai reati tributari, societari, informatici, di riciclaggio e alle violazioni in materia di salute e sicurezza sul lavoro.

La presente procedura integra il Codice Etico, la Politica Anticorruzione, le Misure Integrative del Modello 231 in materia di anticorruzione e trasparenza, la PMOG 03 sulla gestione dei rapporti con la P.A., la PMOG 05 sulla scelta dei partner e sulla gestione di omaggi e sponsorizzazioni, la Policy sull'utilizzo dell'Intelligenza Artificiale e la Procedura Whistleblowing.

2 ACRONIMI AZIENDALI

ACRONIMO	FUNZIONE
CDA	Consiglio di Amministrazione
PRES	Presidente del 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	Responsabile Progettazione
RSCM	Responsabile della singola commessa
RATTR	Responsabile Attrezzature e Mezzi
PROG	Programmatori
RGAD	Responsabile Gestione Archivi e Documenti
REC	Responsabile Esterno Contabilità

RSUG	Responsabile Specialista Ufficio Gare
RICA	Responsabile Interno della Conformità Anticorruzione
RIA	Responsabile interno per l'Intelligenza Artificiale
OdV	Organismo di Vigilanza
RCA	Responsabile Interno Conformità Anticorruzione

LE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI E AI RELATIVI SOGGETTI AFFIDATARI INDIVIDUATI NELL'ORGANIGRAMMA AZIENDALE E NEGLI ATTI DI NOMINA O DELEGA VIGENTI.

3 RIFERIMENTI NORMATIVI E DOCUMENTI INTERNI

- D.Lgs. 8 giugno 2001, n. 231 e successive modificazioni;
- D.Lgs. 31 marzo 2023, n. 36, nel testo vigente, e relativi allegati;
- D.Lgs. 31 dicembre 2024, n. 209, correttivo del Codice dei contratti pubblici;
- D.Lgs. 6 settembre 2011, n. 159, normativa antimafia;
- Legge 13 agosto 2010, n. 136 sulla tracciabilità dei flussi finanziari;
- D.Lgs. 9 aprile 2008, n. 81, in materia di salute e sicurezza sul lavoro;
- Legge 23 settembre 2025, n. 132, in materia di intelligenza artificiale;
- Regolamento (UE) 2024/1689 (AI Act) e Regolamento (UE) 2016/679 (GDPR);
- Delibera ANAC n. 148 del 1° aprile 2026 e Bando-tipo n. 1/2023 aggiornato nel 2026;
- Delibera ANAC n. 153 del 15 aprile 2026 – Bando-tipo n. 2/2026, ove applicabile;
- atti, comunicati, bandi-tipo, modelli e indicazioni ANAC applicabili alla singola procedura;
- Codice Etico, Politica Anticorruzione, Misure Integrative 2025-2028, Modello 231, Codice Disciplinare, PMOG 03, PMOG 05, Policy IA, Regolamento informatico e Procedura Whistleblowing.

4 CAMPO DI APPLICAZIONE E DESTINATARI

La procedura si applica a tutte le gare pubbliche, agli affidamenti diretti, alle procedure negoziate, agli accordi quadro, ai sistemi dinamici di acquisizione, alle richieste di offerta private, alle concessioni e ai contratti eseguiti da BITCONTROL come operatore singolo o mediante RTI/ATI, consorzio, contratto di rete, avvalimento, subappalto o altra forma di collaborazione.

I PROCESSI AZIENDALI COINVOLTI SONO I SEGUENTI:

- partecipazione ed esecuzione dell'appalto in modo diretto, 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 *auditt*; gestione dei documenti di gara, dei contratti e conservazione della relativa documentazione);
- partecipazione ed esecuzione dei contratti a favore di enti privati.

Sono Destinatari il CDA, il PRES, il RSUG, il RTEC, il RCOM/APVG, il RPROG, il RSCM, il RAM/RRU, il RGAD, il REC, il RICA, il RIA e ogni dipendente, consulente o collaboratore che intervenga nella valutazione, predisposizione, approvazione, sottoscrizione, trasmissione o esecuzione dell'offerta e del contratto.

5 RUOLI E RESPONSABILITÀ

FUNZIONE	RESPONSABILITÀ PRINCIPALI
CDA/PRES	Autorizza la partecipazione secondo le deleghe vigenti; approva le scelte strategiche, la composizione di RTI/reti/consorzi e le deroghe; sottoscrive gli atti per i quali è munito dei poteri.
RSUG	Coordina l'istruttoria di gara, analizza il disciplinare, governa

	scadenze e adempimenti, raccoglie i documenti, verifica la completezza formale e cura la trasmissione telematica.
RTEC/RPROG	Valuta fattibilità tecnica, risorse, tempi, requisiti professionali, soluzioni progettuali e congruità tecnica dell'offerta; valida i contenuti tecnici.
RCOM/APVG	Valuta sostenibilità economica, preventivi, forniture, partner e subappaltatori; verifica la coerenza con il budget e la PMOG 05.
RAM/RRU	Verifica requisiti del personale, CCNL, regolarità contributiva, costi della manodopera e documentazione organizzativa.
REC	Verifica dati economico-finanziari, fiscali, contabili, garanzie, tracciabilità finanziaria e coerenza delle dichiarazioni economiche.
RSCM	Presidia l'avvio e l'esecuzione della commessa, SAL, contestazioni, varianti, collaudi, subappalti e chiusura contrattuale.
RGAD	Garantisce il fascicolo digitale, la corretta classificazione, conservazione, integrità e reperibilità dei documenti.
RICA	Svolge controllo preventivo di conformità anticorruzione sulle gare a rischio elevato, sui rapporti con la P.A., sui partner, sui conflitti di interesse e sulle eventuali anomalie; propone misure correttive e riferisce al PRES e all'OdV.
RIA	Verifica l'eventuale uso di sistemi di IA, la conformità alla Policy IA, la registrazione degli strumenti impiegati, la protezione dei dati, la validazione umana e la corretta dichiarazione richiesta dalla documentazione di gara.
OdV	Esercita autonomi poteri di vigilanza sul rispetto e

	sull'efficacia del Modello e riceve i flussi informativi previsti dalla presente procedura.

6. REATI PRESUPPOSTO RILEVANTI

La presente Procedura Speciale disciplina le attività sensibili connesse alla partecipazione della Società alle procedure di affidamento di contratti pubblici e privati, alla predisposizione delle offerte, alla gestione delle procedure di gara, all'aggiudicazione, alla stipula e all'esecuzione dei contratti, al fine di prevenire la commissione dei reati presupposto previsti dal D.Lgs. 231/2001.

In relazione al processo di gara risultano rilevanti, in particolare, le seguenti categorie di reato.

A. REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ARTT. 24 E 25 D.LGS. 231/2001)

Con particolare riferimento ai rapporti con Stazioni Appaltanti, ANAC, amministrazioni aggiudicatrici, enti concedenti, organismi di controllo e commissioni di gara.

RIENTRANO IN TALE CATEGORIA:

1. corruzione per l'esercizio della funzione;
2. corruzione per atto contrario ai doveri d'ufficio;
3. corruzione di persona incaricata di pubblico servizio;
4. istigazione alla corruzione;
5. induzione indebita a dare o promettere utilità;
6. traffico di influenze illecite:
7. turbata libertà degli incanti (art. 353 c.p.): "*Chiunque, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, impedisce o turba la gara nei pubblici incanti o nelle licitazioni private per conto di pubbliche Amministrazioni, ovvero ne allontanagli offerenti, è punito con la reclusione da sei mesi a cinque anni (2) e con la multa da euro 103 a euro 1.032. Se il colpevole è persona preposta dalla legge o dall'Autorità agli incanti o alle licitazioni suddette, la reclusione è da uno a cinque anni e la multa da*

euro 516 a euro 2.065. Le pene stabilite in questo articolo si applicano anche nel caso di licitazioni private per conto di privati, dirette da un pubblico ufficiale o da persona legalmente autorizzata; ma sono ridotte alla metà".

8. turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.): *"Salvo che il fatto costituisca più grave reato chiunque con violenza o minaccia o con doni promesse collusioni o altri mezzi fraudolenti turba 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 è punito con la reclusione da sei mesi a cinque anni e con la multa da euro 103 a euro 1.032.";*
9. astensione dagli incanti (art. 354 c.p.), inadempimento di contratti di pubbliche forniture (art. 355 c.p.) e frode nelle pubbliche forniture (art. 356 c.p.);
10. indebita percezione di erogazioni pubbliche (art. 316-ter c.p.) e malversazione di erogazioni pubbliche (art. 316-bis c.p.), quando la gara o la commessa comporti anticipazioni, contributi, finanziamenti o altre risorse pubbliche;
11. truffa in danno dello Stato o di altro ente pubblico (art. 640, comma 2, n. 1, c.p.) e truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.);
12. frode nelle pubbliche forniture (art. 356 c.p.), anche mediante consegna di beni, sistemi, software o prestazioni difformi per qualità, quantità, caratteristiche o funzionalità rispetto a quanto offerto e contrattualmente dovuto;
13. frode informatica in danno della Pubblica Amministrazione.

A.1 CORRUZIONE TRA PRIVATI (ART. 25-TER D.LGS. 231/2001)

Corruzione tra privati e istigazione alla corruzione tra privati (artt. 2635 e 2635-bis c.c.), con riferimento alle procedure competitive private, ai rapporti con partner, fornitori, subappaltatori, consulenti e soggetti appartenenti ad altri operatori economici.

B. REATI INFORMATICI (ART. 24-BIS)

Considerata la natura altamente tecnologica delle attività svolte da BitControl e l'utilizzo di piattaforme telematiche di e-procurement.

RIENTRANO, TRA GLI ALTRI:

1. accesso abusivo ai sistemi informatici;
2. alterazione di dati informatici;
3. danneggiamento di sistemi informatici;
4. utilizzo illecito di credenziali;
5. alterazione delle piattaforme telematiche di gara;
6. manipolazione di documentazione digitale.

C. DELITTI DI CRIMINALITÀ ORGANIZZATA (ART. 24-TER)

Con riferimento ai rapporti con RTI, consorzi, reti di imprese, subappaltatori, partner commerciali, consulenti e intermediari.

D. REATI SOCIETARI (ART. 25-TER)

Con riguardo, in particolare, alle false comunicazioni sociali (artt. 2621 e 2622 c.c.), alla corruzione tra privati (art. 2635 c.c.) e all'istigazione alla corruzione tra privati (art. 2635-bis c.c.), quando dati societari, economici o finanziari non veritieri siano utilizzati per dimostrare requisiti, capacità o affidabilità nelle procedure di gara.

E. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (ART. 25-BIS.1)

Con riferimento all'utilizzo di certificazioni tecniche, software proprietari, soluzioni tecnologiche, brevetti, marchi, elaborati progettuali e documentazione tecnica.

F. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25-NOVIES)

Con riguardo all'utilizzo di software, banche dati, documentazione tecnica, elaborati progettuali, codice sorgente e contenuti generati mediante strumenti di Intelligenza Artificiale.

G. REATI DI RICICLAGGIO, AUTORICICLAGGIO E RICETTAZIONE (ART. 25-OCTIES)

Con riferimento ai flussi economici relativi all'esecuzione dell'appalto, ai pagamenti, ai subappalti e agli affidamenti a consulenti.

H. REATI TRIBUTARI (ART. 25-QUINQUIESDECIES)

Limitatamente alle condotte realizzabili nella fatturazione, contabilizzazione e rendicontazione della commessa, quali l'utilizzo o l'emissione di fatture o altri documenti per operazioni inesistenti, la dichiarazione fraudolenta mediante artifici, l'occultamento o distruzione di documenti contabili e la sottrazione fraudolenta al

pagamento delle imposte, nei casi previsti dall'art. 25-quinquiesdecies del D.Lgs. 231/2001.

I. OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME SULLA SALUTE E SICUREZZA SUL LAVORO (ART. 25-SEPTIES)

Rilevano nella fase esecutiva, nei sopralluoghi, nelle installazioni, nei collaudi, nelle attività presso cantieri o siti del committente e nella gestione di dipendenti, fornitori e subappaltatori.

J. REATI AMBIENTALI (ART. 25-UNDECIES)

Rilevano, ove applicabili alla singola commessa, nella gestione di rifiuti, RAEE, batterie, componenti elettronici, imballaggi, sostanze pericolose e nelle attività eseguite presso siti o impianti del committente.

K. INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 25-DECIES)

Rileva qualora, in relazione a indagini, contenziosi o procedimenti concernenti gare e appalti, siano esercitate pressioni su dipendenti, partner o terzi affinché non collaborino con l'Autorità o rendano dichiarazioni non veritiere.

7. AREE SENSIBILI

Nell'ambito del processo di gestione delle gare, BitControl individua le seguenti attività sensibili.

7.1 ANALISI DELLE OPPORTUNITÀ DI GARA

1. monitoraggio dei bandi;
2. valutazione della convenienza;
3. decisione di partecipazione.

7.2 PREDISPOSIZIONE DELLA DOCUMENTAZIONE AMMINISTRATIVA

1. DGUE;
2. dichiarazioni sostitutive;
3. requisiti generali;
4. requisiti speciali;
5. documentazione ANAC;
6. PASSOE/FVOE;
7. garanzie;

8. verifica delle cause di esclusione, degli illeciti professionali e delle misure di self-cleaning;
9. aggiornamento e comunicazione tempestiva delle variazioni dei requisiti durante la procedura.

7.3 PREDISPOSIZIONE DELL'OFFERTA TECNICA

COMPRENDE:

1. relazioni tecniche;
2. progetti;
3. architetture hardware e software;
4. sistemi di telecontrollo;
5. sistemi SCADA;
6. cybersecurity;
7. elaborati grafici;
8. cronoprogrammi.

7.4 PREDISPOSIZIONE DELL'OFFERTA ECONOMICA

1. prezzi;
2. costi;
3. ribassi;
4. costi della sicurezza;
5. costo della manodopera.

7.5 UTILIZZO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

COMPRENDE:

1. supporto alla redazione dell'offerta;
2. elaborazione di testi;
3. traduzioni;
4. analisi documentale;
5. generazione di codice;
6. produzione di elaborati tecnici.

7.6 RAPPORTI CON LA STAZIONE APPALTANTE

1. richieste di chiarimenti;
2. soccorso istruttorio;
3. sopralluoghi;

4. incontri;
5. verifiche;
6. commissioni di gara.

7.7 GESTIONE DEI PARTNER

1. RTI;
2. consorzi;
3. reti;
4. avvalimenti;
5. subappalti;
6. consulenti.

7.8 GESTIONE DELL'AGGIUDICAZIONE E DELL'ESECUZIONE

1. stipula;
2. SAL;
3. varianti;
4. collaudi;
5. penali;
6. revisione prezzi;
7. riserve.

7.9 GESTIONE DELLA DOCUMENTAZIONE

1. fascicolo digitale;
2. conservazione documentale;
3. tracciabilità;
4. archiviazione dei log;
5. documentazione IA.

7.10 GESTIONE DELLE PIATTAFORME DIGITALI E DELLE CREDENZIALI

Comprende l'accesso alle piattaforme certificate, la profilazione degli utenti, l'uso delle firme digitali, il caricamento e la trasmissione dei file, la conservazione delle ricevute, la gestione degli incidenti e la protezione delle credenziali.

7.11 SALUTE, SICUREZZA E AMBIENTE NELL'ESECUZIONE

Comprende sopralluoghi, accessi a cantieri e impianti, installazioni, collaudi, coordinamento con il committente e i subappaltatori, gestione dei rischi interferenziali, rifiuti e componenti elettronici.

8 CONDOTTE VIETATE

Nell'ambito del processo di gara è fatto espresso divieto di:

1. Rapporti con la Pubblica Amministrazione
2. promettere, offrire o corrispondere denaro, omaggi, utilità o altre forme di vantaggio a pubblici ufficiali o incaricati di pubblico servizio;
3. utilizzare consulenti, intermediari o partner per finalità corruttive;
4. intrattenere rapporti non autorizzati con commissari di gara o funzionari della Stazione Appaltante;
5. alterare il regolare svolgimento della procedura di gara;

CONCORRENZA E REGOLARITÀ DELLA GARA

1. concordare con concorrenti prezzi, ribassi, offerte di comodo, astensioni, rotazioni, ripartizioni di mercato, subappalti o altre condizioni dell'offerta;
2. promettere lavori, subappalti, forniture, compensi o altri vantaggi a un concorrente affinché non partecipi, ritiri o modifichi l'offerta;
3. influenzare, mediante doni, promesse, collusioni, minacce o altri mezzi fraudolenti, la predisposizione del bando, i requisiti, i criteri di valutazione o l'esito della procedura;
4. acquisire, utilizzare o divulgare informazioni riservate o non pubbliche relative alla gara, alle offerte concorrenti o alle valutazioni della commissione;
5. presentare offerte riconducibili a un unico centro decisionale o coordinare il contenuto dell'offerta con altri operatori economici.

DOCUMENTAZIONE DI GARA

È VIETATO:

1. produrre documentazione falsa o incompleta;
2. attestare requisiti non posseduti;
3. utilizzare certificazioni non veritiere;
4. alterare offerte o documenti dopo la loro presentazione;

5. omettere informazioni rilevanti ai fini della partecipazione;
6. rendere dichiarazioni omissive, reticenti o non aggiornate in merito a cause di esclusione, illeciti professionali, procedimenti, sanzioni, conflitti di interesse o perdita dei requisiti;
7. alterare, retrodatare, sostituire o creare certificati, referenze, contratti, fatture, curricula, attestazioni, firme digitali o ricevute di trasmissione;
8. utilizzare impropriamente il soccorso istruttorio per modificare l'offerta tecnica o economica o sanare carenze non consentite;
9. omettere la comunicazione delle misure correttive o di self-cleaning ovvero rappresentarle in modo non veritiero.

OFFERTA TECNICA ED ECONOMICA

È VIETATO:

1. presentare elaborati copiati o violativi di diritti di proprietà intellettuale;
2. utilizzare software privi di licenza;
3. alterare i dati economici dell'offerta;
4. formulare offerte prive dei necessari presupposti tecnici o economici;
5. indicare costi della manodopera, oneri di sicurezza, tempi, risorse o prestazioni consapevolmente non sostenibili o non coerenti con l'offerta;
6. utilizzare elaborati, referenze, certificazioni o esperienze di terzi senza titolo, autorizzazione o corretta attribuzione;
7. proporre apparecchiature, componenti, software o funzionalità differenti da quelle dichiarate, non conformi o prive delle necessarie licenze e autorizzazioni.

UTILIZZO DELL'INTELLIGENZA ARTIFICIALE

È VIETATO:

1. utilizzare strumenti di IA non autorizzati dalla Società;
2. impiegare sistemi di IA in violazione della Policy aziendale;
3. omettere la dichiarazione dell'utilizzo dell'IA quando richiesta dalla lex specialis di gara;
4. inserire nei prompt dati riservati della Stazione Appaltante, dati personali non anonimizzati o informazioni coperte da obblighi di riservatezza;

5. utilizzare output generati dall'IA senza preventiva revisione critica e validazione da parte del responsabile tecnico competente;
6. presentare come integralmente originale un'offerta predisposta, in tutto o in parte, mediante strumenti di IA senza il rispetto degli obblighi di trasparenza previsti dalla normativa di gara;
7. utilizzare output contenenti dati, fonti, riferimenti normativi, certificazioni, prestazioni o caratteristiche tecniche non verificati o inventati;
8. eliminare, alterare o omettere i log e le registrazioni richieste dalla Policy IA e dalla presente procedura;
9. delegare al sistema di IA decisioni, validazioni o attestazioni riservate alle funzioni aziendali competenti.

PARTNER E SUBAPPALTATORI

È VIETATO:

1. selezionare partner privi dei requisiti richiesti;
2. ricorrere a subappalti simulati o non autorizzati;
3. utilizzare prestanome o soggetti interposti;
4. costituire RTI, reti, consorzi o avvalimenti meramente cartolari o privi di effettive risorse, mezzi e capacità;
5. modificare senza autorizzazione quote, prestazioni, soggetti esecutori o assetti dichiarati in gara;
6. affidare attività a soggetti non dichiarati, non autorizzati o privi dei requisiti, anche mediante subcontratti o consulenze dissimulate.

GESTIONE ECONOMICA DELL'APPALTO

È VIETATO:

1. emettere fatture per prestazioni inesistenti;
2. alterare i SAL;
3. richiedere pagamenti non dovuti;
4. contabilizzare costi fittizi;
5. effettuare pagamenti non autorizzati o privi di adeguata tracciabilità.

ESECUZIONE, SICUREZZA E AMBIENTE

1. attestare o contabilizzare prestazioni, forniture, ore, materiali, collaudi o SAL non effettivamente eseguiti, consegnati o verificati;
2. consegnare beni, software o servizi difformi per qualità, quantità, caratteristiche, provenienza o funzionalità rispetto all'offerta e al contratto
3. introdurre varianti, proroghe, prestazioni extra, compensazioni o accordi informali privi delle necessarie autorizzazioni;
4. omettere misure di salute e sicurezza, obblighi di coordinamento, formazione, idoneità o gestione dei rischi interferenziali;
5. gestire rifiuti, RAEE, batterie, componenti elettronici o sostanze pericolose in violazione delle prescrizioni ambientali applicabili.

CONTROLLI, SEGNALAZIONI E CONSERVAZIONE

1. occultare, distruggere, alterare o non conservare documenti, comunicazioni, log, ricevute, verbali, giustificativi e registrazioni della gara o della commessa;
2. ostacolare i controlli del RICA, dell'OdV, della stazione appaltante, dell'ANAC o di altre Autorità;
3. omettere o ritardare la segnalazione di richieste indebite, anomalie, conflitti di interesse, perdita dei requisiti, incidenti informatici o violazioni della presente procedura;
4. indurre dipendenti, partner o terzi a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria o agli organi di controllo.

9 PRINCIPI GENERALI E DIVIETI

- ogni decisione deve essere documentata, verificabile e assunta da soggetti muniti di adeguati poteri;
- le dichiarazioni rese alla stazione appaltante devono essere complete, veritiere, aggiornate e coerenti con i dati aziendali;
- è vietato occultare cause di esclusione, illeciti professionali, conflitti di interesse, irregolarità fiscali o contributive e ogni altro fatto rilevante;
- è vietato acquisire o utilizzare informazioni riservate, anticipazioni o documenti non pubblici relativi alla gara;

- sono vietati accordi, intese, scambi di informazioni, offerte di comodo, promesse di subappalto o altre condotte idonee a restringere la concorrenza o alterare la procedura;
- sono vietati omaggi, utilità, ospitalità o vantaggi non conformi alla PMOG 05, specialmente durante gare, verifiche, ispezioni, autorizzazioni o contenziosi;
- i contatti con la P.A. devono avvenire esclusivamente per finalità lecite e istituzionali, tramite soggetti autorizzati e con tracciabilità degli interlocutori, della data, dell'oggetto e dell'esito;
- nessun output prodotto con sistemi di IA può essere trasmesso senza revisione critica integrale, validazione umana e verifica delle fonti.

10 VALUTAZIONE PREVENTIVA DELLA GARA E DECISIONE DI PARTECIPAZIONE

Il RSUG apre una scheda di valutazione contenente almeno: stazione appaltante, oggetto, CIG/CUP se disponibili, importo, durata, scadenze, criteri di aggiudicazione, requisiti, garanzie, sopralluogo, contributo ANAC, modalità di presentazione, principali rischi e funzioni coinvolte.

Il RTEC verifica la fattibilità tecnica e la disponibilità delle risorse; il RCOM/APVG e il REC verificano la sostenibilità economica e finanziaria; il RAM/RRU verifica l'impatto organizzativo e i costi del personale; il RICA esamina eventuali indicatori di rischio anticorruzione o conflitto di interesse.

La decisione di partecipare è formalizzata dal CDA/PRES o dal soggetto delegato e riporta le motivazioni, l'assetto di partecipazione, i responsabili, il budget, le eventuali riserve e le verifiche da completare.

11 VERIFICA DEI REQUISITI E SCELTA DEI PARTNER DI GARA

Prima della presentazione dell'offerta il RSUG acquisisce dalle funzioni competenti una conferma scritta sulla sussistenza e permanenza dei requisiti generali, speciali, economico-finanziari, tecnico-professionali, contributivi, fiscali, antimafia, di idoneità professionale e di qualificazione richiesti dalla lex specialis.

I partner, ausiliari, consorziati esecutori, retisti, progettisti indicati e subappaltatori sono selezionati secondo la PMOG 05, previa due diligence

proporzionata al rischio e acquisizione di dichiarazioni su titolarità effettiva, conflitti di interesse, cause di esclusione, sanzioni, contenziosi rilevanti, rispetto del Modello 231 e tracciabilità.

È vietato costituire raggruppamenti meramente strumentali, concordare preventivamente ribassi o ripartizioni di mercato, presentare offerte riconducibili a un unico centro decisionale o utilizzare partner al solo fine di eludere requisiti o divieti.

12 PREDISPOSIZIONE E PRESENTAZIONE DELL'OFFERTA

1. Il RSUG predispone un cronoprogramma interno con scadenze anticipate rispetto al termine di gara.
2. Ogni funzione redige e sottoscrive i documenti di propria competenza, assumendone la responsabilità.
3. Il RTEC valida l'offerta tecnica e attesta la revisione critica integrale dei contenuti, compresi quelli eventualmente supportati da IA.
4. Il REC e il RCOM/APVG validano l'offerta economica, i costi della manodopera, gli oneri della sicurezza e la sostenibilità del prezzo.
5. Il RSUG verifica DGUE, domanda, dichiarazioni integrative, garanzie, contributo ANAC, PASSOE/FVOE ove previsto, firme digitali, formati, dimensioni dei file e corretta compilazione del portale.
6. Prima dell'invio è eseguito un riesame finale a doppio controllo; l'esito è attestato nella Checklist di cui all'Allegato A.
7. La ricevuta di presentazione e l'intero pacchetto trasmesso sono immediatamente salvati nel fascicolo digitale.

13 UTILIZZO DELL'INTELLIGENZA ARTIFICIALE E DICHIARAZIONI ANAC

In conformità alla Delibera ANAC n. 148 del 1° aprile 2026, alla Legge n. 132/2025, al Regolamento (UE) 2024/1689 e alla documentazione della singola gara, BITCONTROL deve dichiarare se ha utilizzato sistemi di Intelligenza Artificiale nella predisposizione dell'offerta e/o se intende utilizzarli in fase esecutiva.

Il RSUG, prima della sottoscrizione della domanda, acquisisce l'Allegato B compilato dal responsabile tecnico e verificato dal RIA. La dichiarazione deve

specificare almeno: strumento e versione, parti dell'offerta interessate, finalità dell'uso, dati impiegati, misure di anonimizzazione, modalità di supervisione umana e prevista utilizzazione in fase esecutiva.

- usare esclusivamente strumenti autorizzati dalla Società;
- non inserire nei prompt dati personali non anonimizzati, segreti tecnici, informazioni riservate della stazione appaltante, criteri non pubblici, prezzi o strategie economiche non protette;
- conservare i log dei prompt e degli output rilevanti secondo la Policy IA e il fascicolo di gara;
- assicurare la prevalenza del lavoro intellettuale umano, il controllo e la verifica dei risultati, la correttezza delle fonti e il rispetto dei diritti di proprietà intellettuale;
- non dichiarare l'assenza di uso dell'IA quando lo strumento sia stato effettivamente utilizzato in modo rilevante nella predisposizione dell'offerta;
- aggiornare la dichiarazione qualora l'uso dell'IA intervenga o muti durante la fase esecutiva, se richiesto dalla lex specialis o dalla stazione appaltante.

Il limite economico o organizzativo previsto da altre procedure non attribuisce di per sé liceità all'uso dello strumento: ogni impiego deve essere valutato nel concreto rispetto ai principi di trasparenza, proporzionalità, sicurezza, riservatezza, responsabilità e controllo umano.

14 CHIARIMENTI, SOPRALLUOGHI E RAPPORTI CON LA STAZIONE APPALTANTE

Le richieste di chiarimenti sono formulate dal RSUG, previa validazione tecnica o legale quando necessaria, esclusivamente tramite i canali ufficiali e nei termini previsti. È vietato cercare risposte informali o riservate attraverso rapporti personali con funzionari o consulenti della stazione appaltante.

I sopralluoghi sono effettuati da soggetti formalmente delegati. Verbali, deleghe, attestazioni, comunicazioni e ogni contatto con la P.A. sono registrati nel fascicolo digitale secondo la PMOG 03.

15 SOCCORSO ISTRUTTORIO, ACCESSO AGLI ATTI E CONTENZIOSO

Le richieste di soccorso istruttorio, chiarimenti o giustificazioni sono immediatamente trasmesse al RSUG, al PRES, al RTEC e, secondo competenza, al RICA e al legale della Società. Le risposte devono essere veritiere, coerenti con la documentazione originaria e non possono modificare l'offerta in violazione della normativa.

Le istanze di accesso agli atti e le opposizioni all'ostensione sono gestite con il supporto legale, tutelando segreti tecnici e commerciali effettivi e specificamente motivati, senza utilizzare la riservatezza per occultare carenze o irregolarità.

Ogni precontenzioso ANAC, ricorso, segnalazione, esclusione, annotazione nel casellario o contestazione rilevante è comunicato tempestivamente al PRES, al RICA e all'OdV.

16 AGGIUDICAZIONE, STIPULA E AVVIO DELLA COMMESSA

A seguito dell'aggiudicazione, il RSUG verifica gli adempimenti richiesti per la stipula, la permanenza dei requisiti, le garanzie, le polizze, la tracciabilità finanziaria, la documentazione antimafia, gli eventuali obblighi di assunzione e le dichiarazioni aggiornate.

Il contratto è sottoscritto esclusivamente da soggetto munito di poteri. Il RSCM apre la commessa, predispone il budget, il piano delle risorse, il programma degli approvvigionamenti e il quadro dei subappalti, assicurando il passaggio documentato dall'Ufficio Gare alla funzione esecutiva.

17 ESECUZIONE DEL CONTRATTO, SAL, VARIANTI E REVISIONE PREZZI

- eseguire le prestazioni a regola d'arte, secondo contratto, capitolato, offerta e ordini di servizio;
- documentare avanzamento, prove, collaudi, consegne, non conformità, contestazioni, riserve e azioni correttive;
- emettere SAL, certificati, rapportini e fatture solo sulla base di prestazioni effettivamente eseguite e verificabili;
- sospendere la fatturazione in caso di discrasia tra prestazione prevista e prestazione eseguita sino alla regolarizzazione documentata;

- gestire varianti, proroghe, rinnovi, opzioni, quinto d'obbligo, modifiche e revisione prezzi esclusivamente nei casi e con le autorizzazioni previste dal contratto e dall'art. 120 del Codice;
- non introdurre prestazioni extra, compensazioni o accordi informali con funzionari o direttori dell'esecuzione.

18 SUBAPPALTO, AVVALIMENTO, RTI, CONSORZI E CONTRATTI DI RETE

La scelta e la gestione dei soggetti terzi devono essere coerenti con quanto dichiarato in gara, con le autorizzazioni della stazione appaltante e con la PMOG 05. Devono essere formalizzati oggetto, quote, attività, corrispettivi, responsabilità, obblighi 231, anticorruzione, sicurezza, tracciabilità e flussi informativi.

È vietato il subappalto non autorizzato, la cessione occulta del contratto, la fatturazione per prestazioni non rese, la modifica informale delle quote o l'utilizzo di imprese prive dei requisiti. Le prestazioni dei partner devono essere verificate dal RSCM prima del pagamento.

19 FATTURAZIONE, INCASSI E TRACCIABILITÀ FINANZIARIA

Il REC e il RSCM verificano la corrispondenza tra contratto, SAL, certificati, fatture, note di credito e pagamenti. Ogni movimento finanziario deve utilizzare conti e strumenti tracciabili e riportare CIG e CUP quando richiesti. Sono vietati pagamenti a soggetti diversi dal contraente, conti non comunicati, compensazioni non documentate e creazione di fondi extracontabili.

20 ARCHIVIAZIONE E FASCICOLO DIGITALE DI GARA/COMMESSA

Per ogni procedura il RGAD assicura un fascicolo digitale contenente almeno: bando e allegati, scheda di valutazione, autorizzazione a partecipare, checklist, documenti amministrativi, offerta tecnica ed economica, dichiarazione IA, log rilevanti, verifiche sui requisiti e sui partner, comunicazioni, ricevute del portale, chiarimenti, soccorso istruttorio, aggiudicazione, contratto, garanzie, subappalti, SAL, fatture, varianti, contestazioni, collaudi e chiusura della commessa.

I documenti devono essere datati, firmati ove previsto, protetti da modifiche non tracciate e conservati per il periodo stabilito dalla normativa, dal contratto e dalle policy aziendali.

21 CONTROLLI, REPORTISTICA E FLUSSI VERSO RICA E ODV

Il RICA effettua controlli a campione e, comunque, sulle gare a rischio elevato, sulle procedure con partner, sulle offerte predisposte con il supporto dell'IA, sui contatti anomali con la P.A., sulle esclusioni, sui soccorsi istruttori e sulle contestazioni esecutive. Gli esiti sono formalizzati e trasmessi al PRES e all'OdV.

Entro il 31 gennaio di ogni anno il RSUG, con il supporto del RTEC, del RCOM/APVG, del REC, del RIA, del RICA e del RGAD, predispone il Report annuale gare e appalti relativo all'anno precedente e lo trasmette all'OdV, previa validazione del PRES.

Il Report annuale indica almeno: gare valutate e gare presentate; esiti; importi; forme di partecipazione; partner; affidamenti diretti; uso dell'IA dichiarato; soccorsi istruttori; esclusioni; accessi agli atti; contenziosi; subappalti; varianti; penali; contestazioni; anomalie; segnalazioni; azioni correttive e stato di attuazione. In assenza di gare deve essere trasmessa una dichiarazione negativa.

Restano fermi i flussi immediati all'OdV per: sospetti di corruzione o turbativa; richieste indebite; dichiarazioni false o inesatte; perdita dei requisiti; iscrizioni o procedimenti ANAC; esclusioni; illeciti professionali; gravi inadempimenti; violazioni della Policy IA; utilizzo non dichiarato dell'IA; data breach o incidenti informatici; contenziosi e anomalie rilevanti.

22 SEGNALAZIONI E SISTEMA DISCIPLINARE

Chiunque rilevi violazioni, tentativi di condizionamento, collusioni, falsità, omissioni, indebite utilità, uso non autorizzato dell'IA o altre anomalie deve informare tempestivamente il superiore, il RICA e/o l'OdV, utilizzando anche il canale Whistleblowing quando ne ricorrono i presupposti. È vietata ogni forma di ritorsione.

La violazione della presente procedura e degli obblighi informativi costituisce violazione del Modello 231 e può determinare l'applicazione delle sanzioni previste

dal sistema disciplinare, ferme le ulteriori responsabilità civili, amministrative e penali.

ALLEGATO A CHECKLIST DI PARTECIPAZIONE ALLA GARA

N.	ATTIVITÀ DI CONTROLLO	RESPONSABILE	ESITO/DATA
1	Analisi bando, disciplinare, capitolato, scadenze e portale	RSUG	
2	Decisione motivata di partecipazione e nomina responsabili	CDA/PRES	
3	Verifica requisiti generali e speciali, FVOE/PASSOE, DURC e fiscalità	RSUG/RAM/REC	
4	Verifica fattibilità tecnica, risorse, tempi e costi	RTEC/RPROG/RCOM	
5	Due diligence su RTI, rete, consorzio, ausiliari e subappaltatori	RCOM/APVG/RICA	
6	Dichiarazioni conflitto di interesse e contatti con la P.A.	RICA/RSUG	
7	Verifica utilizzo IA, strumenti autorizzati, log e dichiarazione ANAC	RIA/RSUG/RTEC	
8	Validazione integrale offerta tecnica	RTEC	
9	Validazione offerta economica, manodopera e sicurezza	REC/RCOM/APVG/RAM	
10	Controllo firme, garanzie, contributo ANAC, formati e caricamento	RSUG	
11	Doppio controllo finale e autorizzazione all'invio	RSUG/PRES	
12	Archiviazione pacchetto e ricevuta di presentazione	RGAD/RSUG	

ALLEGATO B DICHIARAZIONE INTERNA SULL'UTILIZZO DELL'IA

CAMPO	CONTENUTO
Procedura / CIG / stazione appaltante	
Sistema IA utilizzato e versione	
Funzione autorizzata / utilizzatore	
Parti dell'offerta interessate	
Finalità dell'uso	
Dati inseriti e misure di anonimizzazione	
Log archiviati – percorso	
Modalità di controllo e validazione umana	
Uso previsto in fase esecutiva	
Dichiarazione ANAC applicabile	
Firma Responsabile tecnico	
Verifica RIA	
Visto RSUG/PRES	

ALLEGATO C REPORT ANNUALE GARE E APPALTI ALL'OdV

CONTENUTO MINIMO	DATI/RIFERIMENTI
Anno di riferimento	
Numero gare esaminate / presentate / aggiudicate	
Valore complessivo offerte e contratti	
Elenco gare con stazione appaltante, CIG, importo ed esito	
RTI, reti, consorzi, avvalimenti e subappalti	
Gare con utilizzo IA dichiarato e modalità di utilizzo	
Soccorsi istruttori, chiarimenti e giustificazioni	
Esclusioni, annotazioni ANAC, accessi e contenziosi	
Varianti, penali, contestazioni e gravi inadempimenti	
Anomalie, segnalazioni e azioni correttive	
Verifica RICA	
Validazione PRES	
Data di trasmissione all'OdV	

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'LLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

La presente procedura definisce i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento adottati dalla BITCONTROL S.r.l. nei casi in cui la società debba effettuare delle comunicazioni ai terzi.

La società si adopera affinchè non vengano assunte condotte finalizzate a 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), nonché a vietare che soggetti interni o esteri alla medesima società – che agiscono in nome o per conto di BitControl - comunichino e/o divulghino informazioni relative alla Società se riservate e/o coperte da segreto industriale.

È vietata la comunicazione all'esterno di dati personali, dati particolari, dati sensibili, informazioni riservate, confidenziali o strategiche, nonché di documenti, codici, prezzi, contratti, bilanci, informazioni tecniche, segreti industriali o altre informazioni non pubbliche, salvo che ciò sia consentito da legge, contratto o specifica autorizzazione e avvenga nel rispetto delle procedure aziendali applicabili.

In ogni caso, il contenuto delle comunicazioni esterne deve essere veritiero, completo, non fuorviante, coerente con la documentazione aziendale disponibile e formulato in modo da non esporre la Società a rischi di non conformità normativa o contrattuale.

Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Modello e nel Codice Etico.

Tutti coloro che per ragioni del proprio incarico o della propria funzione sono coinvolti nella gestione del processo in oggetto, devono garantire la tracciabilità dell'*iter* decisionale, autorizzativo e delle attività di controllo svolte.

Dunque, la presente procedura si applica altresì a tutti coloro che intrattengono con la Società un rapporto di lavoro subordinato (dipendenti), ivi compresi coloro che sono distaccati, in Italia e all'estero, per lo svolgimento dell'attività.

La presente Procedura si coordina con il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001, con il Codice Etico, con il Codice di Condotta, con la Policy sull'Intelligenza Artificiale, con la Procedura Whistleblowing vigente e con le ulteriori procedure aziendali approvate o aggiornate nel corso del 2026.

La presente Procedura si applica anche alle comunicazioni esterne, istituzionali, commerciali, tecniche, regolatorie, verso autorità, pubbliche amministrazioni, clienti, fornitori, partner, organismi di controllo, enti certificatori, organismi di gara e altri terzi, comprese quelle predisposte con il supporto di strumenti digitali o di Intelligenza Artificiale.

2 ABBREVIAZIONI

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
RGAD	Responsabili Gestione Archivi e Documenti
RSCM	Responsabile singola commessa

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

3 RIFERIMENTI NORMATIVI DEL MODELLO

- DECRETO LEGISLATIVO 231/2001 E S.S. MM.II (DI SEGUITO ANCHE D.LGS 231/01);
- CODICE ETICO DI BITCONTROL S.R.L.;
- CODICE DISCIPLINARE DI BITCONTROL S.R.L.
- MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO DI BITCONTROL S.R.L..

4 CAMPO DI APPLICAZIONE

Rientrano nel campo di applicazione della procedura l'Organo Amministrativo, il responsabile della medesima procedura (ed il professionista iscritto nell'apposito albo) autorizzato a rendere, per conto della Società, una comunicazione all'esterno.

5 RESPONSABILE DELLA PROCEDURA

Il principale responsabile della seguente procedura è il PRES.

Il Responsabile della procedura assicura il coordinamento della presente Procedura con il Codice Etico, il Codice di Condotta, la Policy IA, la Procedura Whistleblowing e con i flussi informativi verso

l'Organismo di Vigilanza, verificando che le comunicazioni esterne rilevanti siano autorizzate, tracciate, documentate e coerenti con i presidi del Modello 231.
Resta ferma la responsabilità giuridica, tecnica e professionale del soggetto autorizzato che approva o trasmette la comunicazione esterna, anche nel caso in cui la stessa sia stata predisposta, in tutto o in parte, con il supporto di strumenti di Intelligenza Artificiale.

6 INDICAZIONI COMPORTAMENTALI

È vietato a chiunque lavori o collabori con la Società 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.
Invero, i rapporti con soggetti interni ed esterni alla Società che, a qualsiasi titolo, abbiano accesso a Informazioni Privilegiate o ad Informazioni Rilevanti sono disciplinati da apposite clausole contrattuali aventi impegni di riservatezza.
Dunque, tutti i dipendenti, i collaboratori, i consulenti e chiunque agisca in nome e per conto della Società, sono tenuti, nell'ambito delle mansioni assegnate, alla corretta gestione delle informazioni privilegiate nonché alla conoscenza e al rispetto delle procedure aziendali in materia.
In particolare, la presente procedura prevede principi di comportamento per la gestione interna e la comunicazione all'esterno delle informazioni aziendali in generale e disciplinano: **(i)** i divieti di abuso di informazioni privilegiate e comunicazione illecita di informazioni privilegiate; **(ii)** la gestione interna e la comunicazione all'esterno delle informazioni privilegiate di BitControl S.r.l.;
Attraverso la presente procedura sono stati ulteriormente rafforzati i presidi a tutela della riservatezza delle informazioni aziendali in generale, e, in particolare delle informazioni privilegiate. Pertanto, eventuali eccezioni a questi protocolli devono essere autorizzate dal PRES o da altra funzione all'uopo preposta.
Qualora, nella predisposizione di comunicazioni esterne, documenti, offerte, risposte a richieste di chiarimento, relazioni, note tecniche, contenuti promozionali o altra documentazione destinata a soggetti esterni, siano utilizzati strumenti di Intelligenza Artificiale, è consentito esclusivamente l'uso degli strumenti approvati dalla Società secondo la Policy IA vigente.
È vietato l'utilizzo di strumenti di IA non approvati o di account personali per finalità aziendali.
È vietato inserire in strumenti di IA dati sensibili, dati particolari, dati personali non necessari, dati riservati o confidenziali, strategie, bilanci, contratti, prezzi non pubblici, segreti industriali o altre informazioni riservate della Società o di terzi.
Ogni contenuto generato con il supporto dell'IA deve essere sottoposto a supervisione, controllo e validazione umana da parte di un soggetto autorizzato prima della sua trasmissione all'esterno; l'IA non può sostituire il giudizio umano né essere utilizzata per generare in autonomia documenti

ufficiali, dichiarazioni vincolanti, offerte commerciali o comunicazioni istituzionali prive di revisione umana.

Devono essere assicurati controlli preventivi e successivi sugli output generati, nonché tracciabilità dei prompt e degli output rilevanti, in coerenza con quanto richiesto dall'Organismo di Vigilanza.

6.1 GESTIONE DELLE INFORMAZIONI SOCIETARIE E OBBLIGHI COMPORTAMENTALI

Da un punto di vista generale, la gestione interna delle Informazioni Rilevanti e delle Informazioni Privilegiate è rimessa alla responsabilità del Consiglio di Amministrazione.

Tuttavia, si precisa che per una migliore efficienza, il titolare del trattamento dei dati ai sensi del GDPR 2016/679 e della normativa nazionale in vigore, con comunicazione dell'11.01.2024, nominava l'ODV, quale Responsabile Esterno del Trattamento dei dati personali.

Ad ogni modo, al fine di garantire la riservatezza di tali informazioni, tutti i membri degli organi sociali, nonché gli amministratori ed i dipendenti, sono tenuti ad un generale obbligo di riservatezza ed è fatto divieto agli stessi di comunicare all'esterno informazioni e documenti acquisiti nello svolgimento dei propri compiti.

Solo i soggetti espressamente autorizzati possono relazionarsi in nome e per conto di BitControl S.r.l. con Autorità, Pubbliche Amministrazioni, enti pubblici, organismi di vigilanza, enti certificatori, stazioni appaltanti, organi ispettivi, clienti e terzi, nel rispetto delle deleghe, dei poteri interni e delle presenti regole procedurali.

Ogni contatto rilevante con soggetti pubblici o con terzi che possa generare effetti giuridici, economici, reputazionali o di compliance per la Società deve essere preventivamente autorizzato, documentato e conservato.

Nei rapporti con Pubblici Ufficiali, incaricati di pubblico servizio, Autorità e organismi di controllo, i destinatari autorizzati devono attenersi a massimi livelli di correttezza, integrità, veridicità e trasparenza, astenendosi da qualsiasi forma di pressione, induzione, promessa, utilità o comportamento finalizzato a conseguire vantaggi indebiti.

IN PARTICOLARE, TUTTI I PREDETTI SOGGETTI SONO TENUTI A:

(i) mantenere la massima riservatezza sulle informazioni acquisite nello svolgimento dell'attività lavorativa e, in particolare, sulle Informazioni Privilegiate e Rilevanti;

(ii) conservare e archiviare con la massima diligenza la documentazione riservata acquisita nello svolgimento delle proprie mansioni, in modo da garantirne l'accesso esclusivamente alle persone autorizzate;

(iii) adottare ogni necessaria cautela affinché la circolazione interna delle informazioni avvenga senza pregiudicare il carattere privilegiato o rilevante delle stesse e nel rispetto, tra l'altro, della normativa dettata in materia di tutela dei dati personali;

(iv) assicurare che ogni comunicazione delle informazioni avvenga in conformità alla presente Procedura e comunque nel rispetto dei principi di correttezza, trasparenza, veridicità e tutela dell'integrità delle stesse.

Si precisa, altresì, che le comunicazioni verso Autorità, Pubbliche Amministrazioni, organismi di controllo, enti regolatori, enti certificatori e stazioni appaltanti devono essere formulate in modo veritiero, completo, accurato e non fuorviante, nel rispetto dei poteri autorizzativi interni e della documentazione di supporto.

Qualora la comunicazione riguardi procedimenti di gara, affidamenti pubblici o documentazione destinata a stazioni appaltanti, devono essere rese, ove applicabili, le dichiarazioni richieste dalla normativa vigente in materia di utilizzo di sistemi di Intelligenza Artificiale.

Nei casi in cui le comunicazioni esterne coinvolgano profili attinenti a misure restrittive dell'Unione europea o obblighi informativi verso le autorità competenti, i destinatari autorizzati devono attenersi ai presidi del Modello 231 aggiornato e assicurare completezza, tempestività e correttezza dell'informazione trasmessa.

7 ARCHIVIAZIONE

Tutta la documentazione – comprese le autorizzazioni – relativa alla gestione della comunicazione a terzi, deve essere consegnata al PRES e al RGAD e opportunamente archiviata da quest'ultimo, o dalla Funzione a ciò incaricata.

Ogni contatto rilevante con soggetti pubblici, ogni comunicazione esterna formalmente autorizzata e ogni trasmissione avente rilievo giuridico, contrattuale, tecnico, regolatorio, reputazionale o 231 deve essere documentata e conservata in modo da consentire la ricostruzione del processo decisionale, del soggetto autorizzante, del soggetto mittente, del contenuto trasmesso, della data e del destinatario.

Qualora nella predisposizione della comunicazione sia stato utilizzato uno strumento di IA, devono essere conservate anche le evidenze rilevanti relative all'impiego dello strumento, ai controlli effettuati, alla validazione umana e, ove applicabile, alla tracciabilità dei prompt e degli output.

8 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Ciascun soggetto coinvolto nella procedura informa tempestivamente l'Organismo di Vigilanza di situazioni anomale e/o poste in essere in deroga alla presente procedura, nonché in ordine a comportamenti non conformi a quanto previsto nel Modello e nel Codice Etico.

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.

Tutti i destinatari della presente Procedura sono tenuti al rispetto dei principi di legalità, correttezza, integrità, riservatezza, tracciabilità, trasparenza e compliance 231 richiamati dal Codice Etico e dal Codice di Condotta.

I destinatari non possono intrattenere rapporti, rilasciare dichiarazioni, trasmettere documenti, dati, informazioni o chiarimenti all'esterno in nome e per conto della Società, salvo espressa autorizzazione e nei limiti dei poteri loro attribuiti.

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.

Devono altresì essere oggetto di flusso informativo verso l'Organismo di Vigilanza: l'utilizzo di strumenti di IA per comunicazioni esterne rilevanti; le dichiarazioni sull'uso dell'IA rese in documentazione di gara; le anomalie nei controlli sugli output; le violazioni della Policy IA; gli incidenti o le criticità che abbiano interessato dati, contenuti o sistemi utilizzati per la comunicazione esterna.

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.
COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev.6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev.8	CDA DEL 27.06.2026	AGGIORNAMENTO

1 SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

La Legge 48/2008 recante la "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*" ha introdotto nel Decreto l'art. 24 bis che ha inserito i reati informatici fra i reati presupposto del Decreto stesso. La tematica è rilevante, considerata l'ormai enorme diffusione degli strumenti informatici e la circostanza che le aziende siano spesso esposte ad attacchi/violazioni dei propri sistemi informativi.

Peraltro, con il recente aumento dell'utilizzo dello smart working, le aziende sono ancora più esposte al rischio di violazione delle misure tecniche adottate: l'uso di dispositivi e/o di connessioni di rete personali può, infatti, creare l'occasione per la commissione dei reati c.d. di criminalità informatica, che, come noto, ai sensi Decreto, possono comportare la responsabilità della Società ove gli stessi siano commessi nell'interesse o a vantaggio dell'ente.

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, la materia è stata significativamente riformata dalla Legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, che ha modificato e inasprito diverse fattispecie di criminalità informatica e i correlati presidi di prevenzione rilevanti ai sensi del D.Lgs. 231/2001.

La Direttiva (UE) 2022/2555 (c.d. NIS2) è stata recepita nell'ordinamento italiano con il D.Lgs. 4 settembre 2024, n. 138, in vigore dal 16 ottobre 2024. Il decreto impone ai soggetti rientranti nel relativo ambito applicativo l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate per la gestione dei rischi di sicurezza informatica, la continuità operativa, la sicurezza della catena di approvvigionamento e la gestione e notifica degli incidenti.

BITCONTROL, in considerazione dei servizi di progettazione, sviluppo, integrazione, assistenza e manutenzione di sistemi di telecontrollo, automazione industriale, SCADA, PLC, RTU, DCS, telemetria e IoT, verifica periodicamente la propria qualificazione ai sensi della disciplina NIS2 e, in ogni caso, applica i relativi principi di gestione del rischio anche nei rapporti con clienti, fornitori e partner operanti in settori essenziali o importanti.

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 BITCONTROL, 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.

Dunque, la presente procedura definisce i ruoli, le responsabilità operative, le attività di controllo e i principi di comportamento adottati dalla BITCONTROL 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. 24 bis, 25 quinquies, 25 novies e 25 quinquiesdecies del D.lgs. 231/2001, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione nonché di tracciabilità delle attività.

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 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 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 dalla BITCONTROL 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.

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*.

In relazione all'intelligenza artificiale, la presente procedura recepisce il Regolamento (UE) 2024/1689 (AI Act), applicabile secondo il calendario previsto dall'art. 113, nonché la Legge 23 settembre 2025, n. 132, e si coordina con la Politica IA e con il Codice Etico adottati dalla Società.

La Società ha pertanto integrato i propri presidi di controllo prevedendo l'utilizzo esclusivo degli strumenti di IA autorizzati, la classificazione preventiva dei dati, la supervisione umana, la tracciabilità degli utilizzi, la gestione degli incidenti e il divieto di inserire nei sistemi di IA dati personali non anonimizzati, informazioni riservate, credenziali, configurazioni di rete, codice sorgente o contenuti protetti da segreto industriale o da obblighi di riservatezza.

L'utilizzo dell'IA deve avvenire in modo antropocentrico, trasparente, proporzionato, sicuro e rispettoso dei diritti fondamentali, della protezione dei dati personali, della proprietà intellettuale e delle regole aziendali, restando sempre ferma la responsabilità della persona che valida e utilizza l'output.

La presente procedura costituisce, pertanto, presidio integrativo della Politica IA e del Codice Etico e disciplina, per quanto rilevante ai fini del D.Lgs. 231/2001, i rischi informatici connessi anche all'impiego di sistemi di IA generativa, strumenti cloud e componenti software di terze parti.

2 ACRONOMI 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
RGAD	Responsabile Gestione Archivi e Documenti
RSCM	Responsabile singola commessa
CDL	Consulente del Lavoro
REC	Responsabile Esterno Contabilità
RIT/RIA	Responsabile IT/Responsabile intelligenza artificiale

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

3 RIFERIMENTI NORMATIVI DEL MODELLO

- DECRETO LEGISLATIVO 231/2001 E S.S. MM.II (DI SEGUITO ANCHE D.LGS 231/01);
- CODICE ETICO DI BITCONTROL S.R.L.;
- CODICE DISCIPLINARE DI BITCONTROL S.R.L.
- MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO DI BITCONTROL S.R.L..
- REGOLAMENTO (UE) 2016/679 (GDPR) E D.LGS. 196/2003, COME MODIFICATO;
- DIRETTIVA (UE) 2022/2555 (NIS2) E D.LGS. 4 SETTEMBRE 2024, N. 138;
- LEGGE 28 GIUGNO 2024, N. 90, IN MATERIA DI CYBERSICUREZZA E REATI INFORMATICI;
- REGOLAMENTO (UE) 2024/1689 (AI ACT), COME MODIFICATO E INTEGRATO;
- LEGGE 23 SETTEMBRE 2025, N. 132, IN MATERIA DI INTELLIGENZA ARTIFICIALE;

- POLITICA IA, POLITICHE ICT E DI SICUREZZA DELLE INFORMAZIONI ADOTTATE DA BITCONTROL S.R.L.;

- PROCEDURE AZIENDALI DI GESTIONE DEGLI INCIDENTI, BUSINESS CONTINUITY, DISASTER RECOVERY E WHISTLEBLOWING.

4 CAMPO DI APPLICAZIONE

La presente procedura si applica a tutti i *Destinatari* coinvolti nelle attività di gestione e utilizzo dei Sistemi Informatici aziendali della Società.

Dunque, la presente procedura si applica altresì a tutti coloro che intrattengono con la Società un rapporto di lavoro subordinato (dipendenti), ivi compresi coloro che sono distaccati, in Italia e all'estero, per lo svolgimento dell'attività.

La presente procedura si applica a tutti i Destinatari coinvolti nelle attività di gestione e utilizzo dei Sistemi Informatici aziendali della Società. Essa si applica anche all'utilizzo di servizi cloud, piattaforme di intelligenza artificiale, strumenti di collaborazione, ambienti di sviluppo, sistemi di automazione e telecontrollo e componenti software o hardware impiegati nelle commesse aziendali.

5 RESPONSABILE DELLA PROCEDURA

Sono responsabili della procedura, ciascuno per quanto di competenza, il PRES, il RSPP, il RSGQ, il RTEC, il RPROG, il RFAM, il RAM/RRU, il Responsabile Sicurezza Informatica, il DPO/Responsabile Privacy e il Responsabile IA, ove nominati. Le responsabilità sono esercitate nel rispetto della segregazione dei compiti e delle deleghe aziendali vigenti.

6 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).

Sono state pertanto 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 BITCONTROL le aree aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati e le misure finalizzate a prevenire la commissione dei seguenti reati.

6.1 ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-TER C.P.)

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."

In particolare, l'art. 16, co. 1, lett. b), legge n. 90 del 2024 ha modificato siffatta disposizione legislativa nei seguenti termini: "*all'articolo 615-ter: 1) al secondo comma: 1.1) all'alinea, le parole: «da uno a cinque anni» sono sostituite dalle seguenti: «da due a dieci anni»; 1.2) al numero 2), dopo la parola: «usa» sono inserite le seguenti: «minaccia o»; 1.3) al numero 3), dopo le parole: «ovvero la distruzione o il danneggiamento» sono inserite le seguenti: «ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare»; 2) al terzo comma, le parole: «da uno a*

cinque anni e da tre a otto anni» sono sostituite dalle seguenti: «da tre a dieci anni e da quattro a dodici anni»;".

Dunque, il reato in esame si realizza quando un soggetto si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza. In merito si evidenzia come il legislatore abbia inteso punire il mero accesso abusivo ad un sistema informatico o telematico cui non deve necessariamente seguire il danneggiamento di dati. Tale fattispecie delittuosa si realizza anche nell'ipotesi in cui il soggetto agente, pur essendo entrato legittimamente in un sistema, utilizzi il sistema stesso per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato. Il delitto potrebbe pertanto essere astrattamente configurabile nell'ipotesi in cui un soggetto acceda abusivamente ai sistemi aziendali della società per acquisire informazioni alle quali non avrebbe legittimo accesso, in vista del compimento di atti ulteriori nell'interesse o a vantaggio della società stessa.

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)".

6.2 DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615-QUATER C.P.)

L'art. 615 quater c.p. che prevedeva "*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a € 5.164,00.*

La pena è della reclusione da uno a due anni e della multa da € 5.164,00 a € 10.329,00 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.", è stato modificato dall'art. 16, co. 1, lett. c), legge n. 90 del 2024, nel seguente modo: "*all'articolo 615-quater: 1) al primo comma, la parola: «profitto» è sostituita dalla seguente: «vantaggio»; 2) il secondo comma è sostituito dal seguente: «La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1)»; 3) dopo il secondo comma è aggiunto il seguente: «La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma»".*

Alla luce di tali cambiamenti: 1) viene ampliato il dolo specifico previsto per la configurabilità della fattispecie; 2) è prevista "l'ipotesi aggravata punita con la pena della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui al precedente articolo 615-ter, secondo comma, numero 1); 3) si inserisce "un ulteriore comma all'articolo, introducendo un'ulteriore ipotesi aggravata punita con la pena della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma.

Ciò posto, si rileva come il reato in esame si realizza nel caso in cui un soggetto abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, dispostivi di protezione (quali password, badge, ecc.) o altri mezzi idonei all'accesso a un sistema informatico o telematico protetto da misure di sicurezza, o comunque fornisca indicazioni idonee a raggiungere tale scopo a terzi. L'art. 615-quater c.p., pertanto, punisce le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico. Tale fattispecie può configurarsi sia nel caso in cui il soggetto, in possesso legittimamente dei dispositivi di protezione di cui sopra, li comunichi senza autorizzazione a terzi, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi.

L'art. 615-quater c.p. punisce altresì chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza: ad esempio, il dipendente che comunichi ad un terzo soggetto la password di accesso alla posta elettronica di un proprio collega, allo scopo di garantire al terzo la possibilità di controllare le attività svolte dal collega, quando da ciò possa derivare un determinato vantaggio o interesse per la società.

6.3 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.)

L'art. 16, co. 1, lett. d), legge n. 90 del 2024 ha abrogato l'art. 615-quinquies c.p. che, come è risaputo, nel prevedere il delitto di detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico, statuiva: "*Chiunque, allo scopo di danneggiare illecitamente 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a € 10.329,00.*"

Invero, i riferimenti normativi di cui all'articolo 615-quinquies sono stati rimossi e sostituiti con l'articolo 635-quater.1, i cui contenuti sono comunque sovrapponibili, seppur inaspriti dalla previsione di due nuove circostanze aggravanti.

Infatti, l'art. 16, co. 1, lett. q), legge n. 90 del 2024 introduce una ulteriore fattispecie criminosa, vale a dire il delitto di detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

Orbene, l'art. 635-quater.1 (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) dispone testualmente: "*Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici e' punito con la reclusione fino a due anni e con la multa fino a euro 10.329. La pena e' della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1). La pena e' della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma*".

Quindi, se il primo comma di questo nuovo articolo "riproduce il vigente art. 615-quinquies c.p.9 che, appunto, viene contestualmente abrogato dalla lett. d), punendo "con la reclusione fino a 2 anni e con la multa fino a euro 10.329 chiunque, allo scopo di danneggiare illecitamente 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici", a loro volta, il "*secondo e il terzo comma prevedono quali circostanze aggravanti: - la commissione del fatto da parte di un pubblico ufficiale o incaricato di pubblico servizio*

con abuso dei poteri o con violazione dei doveri, da un investigatore privato anche abusivo, o con abuso della qualità di operatore di sistema (reclusione da 2 a 6 anni), previsione operata tramite il rinvio alle circostanze di cui all'art. 615-ter, secondo comma, n. 1; - la commissione del fatto su 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 (reclusione da 3 a 8 anni), previsione operata tramite il rinvio all'articolo 615-ter, terzo comma, primo periodo".

6.4 DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635-BIS C.P.)

"*Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre 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 della reclusione da uno a quattro anni.*"

Il reato in esame si realizza qualora un soggetto distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui. Il danneggiamento potrebbe essere commesso a vantaggio della società nel caso in cui, ad esempio, l'alterazione o l'eliminazione di alcuni file o del programma informatico, siano volte a nascondere dati aziendali ritenuti compromettenti per la società o a celare la prova del credito da parte di un fornitore della società (es. fee) o a contestare il corretto adempimento delle obbligazioni da parte di quest'ultimo.

6.5 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.)

"*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 utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.*

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto 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."

Tale delitto si distingue dal precedente (art. 635-bis c.p.) poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne consegue,

dunque, che il delitto si realizza anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati al soddisfacimento di un interesse di natura pubblica.

6.6 DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635-QUATER C.P.)

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".

Invero, il reato in esame si realizza quando un soggetto mediante le condotte di cui all'art. 635-bis c.p., distrugga, danneggi, renda (in tutto o in parte) inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento. Ne deriva che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-bis c.p..

Dunque, 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).

6.7 DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (ART. 635-QUINQUIES.C.P.)

"*Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità ad ostacolarne gravemente*

il funzionamento, la pena è della reclusione da uno a quattro anni.
Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto 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."

Il reato in esame si configura quando la condotta di cui al precedente art. 635-quater c.p. sia diretta a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. Rileva in questo reato che il sistema sia utilizzato per il perseguimento di pubblica utilità, indipendentemente dalla proprietà privata o pubblica dello stesso

6.8 INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUATER C.P.)

"*Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.*
Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.
I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.
Tuttavia, si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:
***1.** in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;*
***2.** 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, ovvero con abuso della qualità di operatore del sistema;*
***3.** da chi esercita anche abusivamente la professione di investigatore privato*"

Tale ipotesi di reato può configurarsi quando un soggetto fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisca o interrompa tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione. Lo scopo è quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

6.9 INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUINQUIES C.P.)

"*Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.*"

6.10 FALSITÀ IN UN DOCUMENTO INFORMATICO PUBBLICO O AVENTE EFFICACIA PROBATORIA (ART. 491-BIS C.P.)

"*Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici.*"

La norma in esame dispone che tutti i delitti relativi alla "falsità in atti" disciplinati dal codice penale di cui al Capo III, Titolo VII, Libro II, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo, bensì un documento informatico, pubblico o privato, avente efficacia probatoria.

6.11 FRODE INFORMATICA DEL CERTIFICATORE DI FIRMA ELETTRONICA (ART. 640-QUINQUIES C.P.)

"*Il 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, è punito con la reclusione fino a tre anni e con la multa da € 51,00 a € 1.032,00.*"

Il reato in esame si realizza quando un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero di arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato di firma. Il reato è, dunque, qualificabile come reato "proprio" in quanto può essere commesso solo da parte dei certificatori qualificati, vale a dire i soggetti che prestano servizi di certificazione di firma elettronica qualificata.

6.12 UTILIZZO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

I sistemi di intelligenza artificiale possono essere utilizzati esclusivamente nei limiti, con gli strumenti e tramite gli account aziendali autorizzati dalla Politica IA. Ogni utilizzo deve essere

pertinente alle mansioni assegnate, proporzionato alla finalità perseguita e sottoposto a supervisione umana effettiva e documentabile.

Prima dell'inserimento di dati o documenti in un sistema di IA, l'utilizzatore deve verificarne la classificazione. È consentito trattare soltanto dati pubblici o interni e dataset adeguatamente anonimizzati o pseudonimizzati. È vietato inserire dati personali non anonimizzati, categorie particolari di dati, informazioni riservate o confidenziali, credenziali, password, token, API key, configurazioni di rete, architetture IT, codice sorgente, documenti coperti da NDA, segreti commerciali, informazioni tecniche dei clienti o dati relativi a infrastrutture critiche.

Gli output generati dall'IA non possono essere utilizzati automaticamente né sostituire il giudizio professionale. Il soggetto autorizzato deve verificarne accuratezza, completezza, liceità, assenza di contenuti discriminatori, rispetto della proprietà intellettuale e coerenza con le specifiche tecniche e contrattuali. Le decisioni con effetti giuridici, economici, tecnici o significativi devono restare imputabili a una persona fisica individuata.

È vietato utilizzare strumenti di IA per aggirare controlli di sicurezza, generare o perfezionare malware, phishing, exploit, credenziali o codice destinato ad accessi abusivi, intercettazioni, danneggiamenti, frodi informatiche o manipolazione di sistemi di pagamento. È altresì vietato utilizzare output IA non verificati nella programmazione di PLC, RTU, DCS, SCADA, sistemi IoT o infrastrutture di telecontrollo.

Per gli utilizzi rilevanti devono essere conservate, secondo le regole aziendali, le evidenze dell'autorizzazione, della finalità, della piattaforma utilizzata, dei prompt e degli output significativi, delle verifiche svolte e del validatore umano, nel rispetto dei principi di minimizzazione e conservazione limitata dei dati.

Qualsiasi uso improprio, anomalia, perdita di riservatezza, esposizione di dati, output potenzialmente dannoso o incidente connesso a sistemi di IA deve essere immediatamente segnalato al Responsabile Sicurezza Informatica, al Responsabile IA e, ove siano coinvolti dati personali, al DPO/Responsabile Privacy, nonché all'Organismo di Vigilanza quando l'evento possa integrare una violazione del Modello o della presente procedura.

7 INDICAZIONI COMPORTAMENTALI PER LA PREVENZIONE DEI REATI INFORMATICI

I Destinatari del Modello, competenti per le attività oggetto di regolamentazione della presente Parte Speciale, sono tenuti ad osservare i seguenti principi di comportamento:

1. rispettare le norme in tema di trasparenza per tutte le operazioni poste in essere;

2. garantire l'attuazione del principio di segregazione dei compiti e delle funzioni anche attraverso la predisposizione di specifiche procedure;
3. garantire la tracciabilità e la documentabilità di tutte le operazioni effettuate, prevedendo specifici obblighi di archiviazione;
4. garantire che le attività a rischio prevedano i necessari controlli gerarchici, che devono essere tracciati/documentati;
5. garantire la corretta applicazione del Sistema disciplinare, in caso di mancato rispetto dei principi e dei protocolli contenuti nel Modello;
6. prestare una fattiva collaborazione e rendere dichiarazioni veritiere ed esaustivamente rappresentative dei fatti nei rapporti con l'Autorità Giudiziaria;
7. attenersi alle istruzioni impartite ai sensi del Regolamento UE/2016/679 e D. Lgs. 196/03 in tema di trattamento dei dati personali;
8. effettuare verifiche periodiche delle credenziali utente al fine di prevenire eventuali erronee abilitazioni ai sistemi applicativi;
9. applicare, nell'utilizzo dei sistemi informatici aziendali, regole atte ad assicurare l'aggiornamento delle password dei singoli utenti;
10. attenersi a quanto disposto dalle procedure aziendali e linee guida in materia di:
    - utilizzo del personal computer;
    - utilizzo della rete aziendale;
    - gestione delle password;
    - utilizzo dei supporti magnetici e dei PC portatili;
    - utilizzo della posta elettronica;
    - utilizzo della rete internet e dei relativi servizi;
    - protezione dei dati personali e riservatezza del know-how della Società, dei Clienti e delle Pubbliche Amministrazioni con cui la Società si trova ad operare; ogni altra attività svolta mediante strumentazioni, piattaforme o sistemi informatici;
    - utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta dalla Società e per le specifiche finalità assegnate;
    - non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile della funzione competente alla gestione dei relativi sistemi informatici;
    - in caso di smarrimento o furto di qualsiasi apparecchiatura informatica della Società o delle Pubbliche Amministrazioni coinvolte, informare tempestivamente il responsabile della funzione competente alla gestione dei relativi sistemi/dispositivi informatici e

attenersi alla Procedura gestione delle violazioni dei dati personali (data breach notification);

- utilizzare la connessione internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che rendono necessario il collegamento;
- rispettare le procedure e gli standard previsti in materia di utilizzazione delle risorse informatiche, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali di queste ultime;
- impiegare sulle apparecchiature di BitControl soltanto prodotti ufficialmente acquisiti dalla Società;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni di BITCONTROL;
- in ogni caso osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

NELL'AMBITO DEI SUDDETTI COMPORTAMENTI È FATTO DIVIETO IN PARTICOLARE DI:

 alterare documenti informatici, pubblici, aventi efficacia probatoria;

 aggirare e/o tentare di aggirare i meccanismi di sicurezza aziendali (antivirus, firewall, proxy server, etc.);

 accedere abusivamente al sistema informatico o telematico di soggetti pubblici e privati con cui BITCONTROL intrattiene rapporti nell'ambito della propria attività, al fine di alterare e /o cancellare dati e/o informazioni;

 detenere e/o utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico di soggetti pubblici o privati con i quali la Società intrattiene rapporti nell'ambito della propria attività, al fine di acquisire informazioni riservate;

 detenere e/o utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al sistema informatico o telematico di BITCONTROL o delle Pubbliche Amministrazioni al fine di acquisire informazioni riservate;

 svolgere attività di approvvigionamento, e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di (a) danneggiare (i) un sistema informatico o telematico di soggetti pubblici o privati con i quali la Società intrattiene rapporti nell'ambito della propria attività, nonché (ii) le informazioni, i dati o i programmi in esso contenuti; ovvero allo scopo di (b) favorire l'interruzione, totale o parziale, o l'alterazione del loro funzionamento;

 svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, con i quali la Società intrattiene rapporti nell'ambito della propria attività, al fine di acquisire informazioni riservate;

 installare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;
 svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o di soggetti pubblici o comunque di pubblica utilità;
 svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;
 distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità;
 introdurre e/o conservare applicazioni/software che non siano state preventivamente sottoposte al vaglio del responsabile della funzione competente alla gestione del relativo sistema informatico o la cui provenienza sia dubbia o sconosciuta;
 trasferire all'esterno di BITCONTROL e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà di Consip, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio superiore gerarchico;
 lasciare accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (parenti, amici, ecc.);
 utilizzare password di altri utenti aziendali, neppure per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del responsabile della funzione competente;
 utilizzare strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
 accedere a pagine web con contenuti pedopornografici.

Tuttavia, a seguito dell'introduzione della Legge 90/2024, che mira ad aumentate la sicurezza informatica per difendersi dai cyber-attacchi, aumentando le sanzioni previste per i c.d. "computer crimes", la Bitcontrol ha aggiunto ulteriori prescrizioni e norme di comportamento a quelle già e sopra dettagliatamente indicate.

7.1 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).

7.2 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 (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.

7.3 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.

7.4 L'UTILIZZO DI INTERNET E PROGRAMMI INFORMATICI

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.

7.5 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 RGAD, sotto la supervisione del PRES, o della Funzione eventualmente incaricata dal

primo, dovrà tenere un registro aggiornato, anche digitale, da caricare, con cadenza semestrale, e tenere nell'apposito archivio informatico – all'uopo predisposto nella piattaforma digitale di condivisione -, di tutte le utenze attive e di quelle disabilitate, provvedendo alla relativa archiviazione.

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.

7.6 LA GESTIONE DELLA POSTA ELETTRONICA

Per ciò che concerne la gestione della posta elettronica certificata, 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; in entrambi i casi, deve essere apposto il relativo numero di protocollo.

L'invio di P.E.C. in uscita deve unicamente avvenire a cura dei componenti del CDA, nonché, previa autorizzazione, da parte del RPROG.

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.

7.7 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.

7.8 IL LICENZIAMENTO O LE DIMISSIONI DI UN DIPENDENTE

Qualora un dipendente interrompa il rapporto di lavoro con l'azienda, per qualsivoglia ragione, è opportuno procedere alla variazione delle password di cui lo stesso era a conoscenza e/o disabilitare le utenze.

BITCONTROL 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.

7.9 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.

7.10 INSTALLAZIONE DI SOFTWARE DI TERZE PARTI PER LA FATTURAZIONE

È fatto divieto ad ogni operatore autorizzato 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.

7.11 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.

7.12 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.

7.13 SOSPETTO O CERTEZZA DI DATA BREACH

La commissione di un reato informatico coincide, il più delle volte, con il verificarsi di una Violazione dei dati personali (c.d. " data breach "), prevista dall'art. 33 del Regolamento (UE) 2016/679 in materia di protezione dei dati personali (" GDPR ").

Infatti, la violazione dei dati personali è una "violazione di sicurezza che comporta - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Nel caso in cui si verifichi una violazione dei dati personali, 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.

Nel dettaglio, sarà fondamentale:

- 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 BITCONTROL 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.

7.14 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.

7.15 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.

9.10 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 BITCONTROL 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 BITCONTROL s.r.l., 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).

7.16 I CONTROLLI

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.

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, che apporrà 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.

La presente Procedura ad integrazione e completamento del Regolamento informatico adottato dalla Società.

8 CYBERSICUREZZA

La gestione della cybersicurezza è attuata secondo un approccio basato sul rischio, coerente con il D.Lgs. 138/2024 e con il sistema di gestione per la sicurezza delle informazioni della Società. Sono oggetto di valutazione almeno i rischi relativi a sistemi IT e OT, reti industriali, ambienti SCADA, accessi remoti, dispositivi mobili, servizi cloud, supply chain, vulnerabilità dei componenti, continuità operativa e dipendenze da fornitori esterni.

La Società adotta misure adeguate e proporzionate comprendenti, ove applicabili: analisi e trattamento del rischio; gestione degli incidenti; business continuity, backup e disaster recovery; gestione delle crisi; sicurezza della catena di approvvigionamento; sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi; gestione e divulgazione coordinata delle vulnerabilità; verifica

dell'efficacia dei controlli; igiene informatica e formazione; crittografia; controllo degli accessi e degli asset; autenticazione a più fattori e comunicazioni protette.

Gli incidenti significativi o potenzialmente significativi sono gestiti secondo la procedura aziendale e, qualora BITCONTROL sia soggetto agli obblighi NIS o operi contrattualmente per soggetti NIS, sono rispettati i termini e i contenuti delle comunicazioni previsti dalla normativa e dagli accordi con clienti e committenti. Ogni comunicazione esterna è previamente coordinata con le funzioni autorizzate.

I fornitori di servizi ICT, cloud, software, manutenzione e assistenza remota sono selezionati e monitorati anche sotto il profilo della sicurezza, con clausole su riservatezza, gestione degli accessi, notifica degli incidenti, vulnerabilità, continuità operativa, restituzione o cancellazione dei dati e diritto di audit, in misura proporzionata al rischio.

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.

9 REATI PRESUPPOSTO STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

L'art. 3 del d.lgs.184/2021 ha esteso la responsabilità amministrativa degli enti ai delitti in materia di strumenti di pagamento diversi dai contanti, introducendo nel Decreto l'art. 25-octies 1, la cui numerazione vuole sottolineare lo stretto collegamento con i reati di riciclaggio previsti all'art. 25 octies. Il predetto decreto costituisce infatti l'atto di recepimento della Direttiva 2019/713/UE del Parlamento europeo e del Consiglio del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, che rappresentano una minaccia alla sicurezza in quanto possono essere fonti di entrate per la criminalità organizzata e quindi rendono possibili altre attività criminali come il terrorismo, il traffico di droga e la tratta di esseri umani.

La definizione di strumenti di pagamento diversi dal contante è rinvenibile nell'art. 1 del d.lgs. 184/2021, il quale definisce come tale «*un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali*», chiarendo ulteriormente che:

i) per «dispositivo, oggetto o record protetto» si intende un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta (per esempio mediante disegno, codice o firma);
ii) la locuzione «mezzo di scambio digitale» indica «qualsiasi moneta elettronica definita all'art. 1, comma 2, lett. h ter), d.lgs. 385/1993, e la valuta virtuale», intendendosi quest'ultima come una «*rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente*».
Tali definizioni riprendono sostanzialmente quelle proposte nella Direttiva (UE) 2019/71.
In virtù del primo comma del art. 25-octies.1, la condanna dell'ente può discendere, oltre che dai delitti ex artt. 493-ter c.p. (indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti) e 493-quater c.p. (detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti), anche dalla commissione di frode informatica (art. 640-ter c.p.), nella nuova ipotesi aggravata quando il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale.
Il comma 2 dell'art. 25-octies.1 prevede, inoltre, un'ipotesi residuale di responsabilità dell'ente, in quanto la norma dispone la sanzionabilità di ogni altro delitto contro la fede pubblica (Titolo VII c.p.), contro il patrimonio o che comunque offende il patrimonio (Titolo XIII c.p.) previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, salvo che il fatto integri altro illecito amministrativo sanzionato più gravemente. Tale disposto intende evidentemente responsabilizzare l'ente per tutti gli altri reati riguardanti gli «*strumenti di pagamento diversi dai contanti*» *previsti dalla direttiva europea che a sua volta fa espresso riferimento al «furto o altra illecita appropriazione»* degli strumenti materiali e all'«ottenimento illecito» di quelli immateriali; ipotesi queste che vanno sanzionate in quanto «*preparano il terreno all'effettiva utilizzazione fraudolenta dei mezzi di pagamento diversi dal contante*».
Sono state pertanto 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 BITCONTROL le aree aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati e le misure finalizzate a prevenire la commissione dei seguenti reati.

9.1 INDEBITO UTILIZZO E FALSIFICAZIONE DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART. 493-TER C.P.)

"*Chiunque 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 è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace 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.

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta".

L'ARTICOLO INDIVIDUA TRE DIVERSE TIPOLOGIE DI CONDOTTE:

1. la prima consiste nella indebita utilizzazione, cioè nel concreto uso illegittimo delle carte di credito o delle carte di pagamento – lecita o illecita che sia la loro provenienza – da parte del non titolare al fine di realizzare un profitto per sé o per altri;

2. la seconda categoria di condotte include quelle di falsificazione e alterazione dei medesimi strumenti di pagamento;

3. infine, viene punito chi possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. Si tratta in questi ultimi casi di un'azione che sotto il profilo logico e temporale è distinta dalla prima perché la precede e ne costituisce il presupposto fattuale.

Presupposto di queste tipologie di condotta è, infatti, la illecita provenienza della carta o degli altri documenti indicati dalla norma; ciò perché da sole tali condotte non sono caratterizzate da alcuna illiceità a differenza dell'utilizzo indebito o della falsificazione. Nel caso in cui le carte siano contraffatte o alterate l'illecita provenienza deriva direttamente dalla contraffazione o dalla alterazione. Per quanto riguarda le persone giuridiche, tale reato potrebbe astrattamente configurarsi nel caso in cui il dipendente della società cui è affidata la gestione della carta di credito aziendale, ma non ne è il titolare qualificato, la utilizzi indebitamente per un profitto personale arrecando un danno all'ente; laddove invece l'uso indebito fosse ascrivibile al titolare della carta di credito, si potrà configurare il reato di appropriazione indebita ex art. 646 c.p. e non quello di indebito utilizzo di carta di credito.

Diverso invece è il caso in cui l'uso indebito – o addirittura la falsificazione – vengano effettuati nell'interesse e a vantaggio dell'ente di appartenenza, ipotesi che, sebbene in linea teorica non si possa escludere del tutto, appare effettivamente remota.

9.2 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, chiunque, alfine 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 sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnicocostruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo, è punito con la reclusione sino a due anni e la multa sino a 1000 euro.*

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è sempre ordinata la confisca delle apparecchiature, dei dispositivi o dei programmi informatici predetti, nonché la confisca del profitto o del prodotto del reato ovvero, quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto".

Tale fattispecie richiama in parte alcuni reati informatici che sono già inclusi nel catalogo dei reati presupposto: si pensi ai delitti di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici e di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (artt. 615 quater e 615 quinquies c.p., richiamati nell'art. 24 bis, d.lgs. 231/2001). Tuttavia, considerando il dettato della norma in esame, sebbene in linea teorica non si possa escludere del tutto, appare effettivamente remota la possibilità che tale tipologia di reato possa essere commesso nell'interesse e a vantaggio dell'ente di appartenenza.

9.3 FRODE INFORMATICA (ART. 640-TER C.P.)

"*Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, 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. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 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.

La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o taluna delle circostanze previste dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età, e numero 7."

Come sopra accennato, con il d.lgs. 184/2021 viene inserita tra i reati presupposto anche la frode informatica aggravata dal fatto che dalla condotta derivi un trasferimento di denaro, di valore monetario o di valuta virtuale.

10 INDICAZIONI COMPORTAMENTALI PER LA PREVENZIONE DEI REATI DI INDEBITO UTILIZZO DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

I Destinatari del Modello, competenti per le attività oggetto di regolamentazione della presente Parte speciale, sono dunque tenuti ad osservare i seguenti ulteriori principi:

1. rispettare le norme in tema di trasparenza per tutte le operazioni poste in essere;
2. garantire l'attuazione del principio di segregazione dei compiti e delle funzioni anche attraverso la predisposizione di specifiche procedure;
3. garantire la tracciabilità e la documentabilità di tutte le operazioni effettuate, prevedendo specifici obblighi di archiviazione;
4. garantire che le attività a rischio prevedano i necessari controlli gerarchici, che devono essere tracciati/documentati;
5. garantire la corretta applicazione del Sistema disciplinare, in caso di mancato rispetto dei principi e dei protocolli contenuti nel Modello con particolare riguardo alle attività di gestione dei pagamenti;
6. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione dell'anagrafica fornitori, anche stranieri (attraverso l'amministrazione, l'aggiornamento e il monitoraggio del relativo elenco storico);
7. non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi di denaro di rilevante entità;
8. assicurare, in caso di pagamenti a favore di soggetti terzi tramite bonifico bancario, il rispetto di tutti i passaggi autorizzativi relativi alla predisposizione, validazione ed emissione del mandato di pagamento, nonché della registrazione a sistema della relativa distinta;

9. in caso di pagamento a carico della Società a mezzo di carta di credito, impiegare esclusivamente la carta di credito aziendale o altro strumento comunque intestato alla Società o a persona fisica in sua rappresentanza;
10. assicurare che tutti i pagamenti riferiti ad acquisti realizzati dalla Società vengano effettuati a fronte dell'inserimento a sistema della fattura corrispondente dal personale amministrativo all'uopo preposto;
11. assicurare un adeguato sistema di segregazione dei poteri autorizzativi, di controllo ed esecutivi in relazione alla gestione dei pagamenti delle fatture e alle modalità di predisposizione ed approvazione delle relative distinte di pagamento;
12. operare nel rispetto degli obblighi di legge e ad assicurare la corretta attuazione delle politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo;
13. segnalare tempestivamente ai soggetti competenti ogni circostanza per la quale si conosca, si sospetti, o si abbiano ragionevoli motivi per sospettare che siano state compiute, tentate o siano in corso operazioni di frode e/o falsificazione di mezzi di pagamento diversi dai contanti, riciclaggio, di finanziamento del terrorismo o che i fondi, indipendentemente dalla loro entità, provengano da un'attività criminosa;
14. non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità (i.e. a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura);con riguardo all'utilizzo delle apparecchiature informatiche/software;
15. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta dalla Società e per le specifiche finalità assegnate;
16. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile della funzione competente alla gestione dei relativi sistemi informatici;
17. utilizzare la connessione internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che rendono necessario il collegamento;
18. rispettare le procedure e gli standard previsti in materia di utilizzazione delle risorse informatiche, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali di queste ultime;
19. impiegare sulle apparecchiature di BITCONTROL soltanto prodotti ufficialmente acquisiti dalla Società;
20. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

21. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni di BITCONTROL;
22. in ogni caso osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

In generale, è fatto dunque divieto ai Destinatari del Modello di porre in essere comportamenti che possano rientrare, anche potenzialmente, nelle fattispecie di reato richiamate dagli articoli 25 octies 1 del D.Lgs. 231/2001, ovvero di collaborare o dare causa alla relativa realizzazione.

NELL'AMBITO DEI CITATI COMPORTAMENTI È DUNQUE FATTO DIVIETO, IN PARTICOLARE, DI:

- usare in modo illegittimo carte di credito o carte di pagamento – lecita o illecita che sia la loro provenienza –al fine di realizzare un profitto;
- possedere, cedere o acquisire tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi;
- 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.

L'osservanza dei principi di comportamento e dei presidi indicati nella presente Procedura è essenziale per evitare che soggetti terzi, dall'esterno, entrino nel sistema aziendale e che qualcuno, dall'interno, violi sistemi aziendali altrui pubblici o privati, rendendoli inagibili, ovvero effettui attività di spionaggio industriale.

11 ARCHIVIAZIONE

Tutta la documentazione prodotta nell'ambito della presente procedura, inclusi log, autorizzazioni, report di sicurezza, evidenze di backup e ripristino, registri degli incidenti, valutazioni del rischio, verifiche sui fornitori e documentazione relativa agli utilizzi rilevanti dell'IA, deve essere trasmessa al RGAD o resa disponibile nella piattaforma informatica aziendale autorizzata, nel rispetto dei tempi di conservazione, dei profili di accesso e delle misure di sicurezza applicabili.

12 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

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;
- report su violazioni da cui si evincono accessi non autorizzati ai sistemi interni o di terzi;
- Anomalie, criticità riscontrate, etc.
- incidenti di sicurezza informatica, data breach, indisponibilità significativa dei sistemi, attacchi ransomware, compromissioni di credenziali o vulnerabilità critiche;
- comunicazioni, notifiche o richieste provenienti da ACN, CSIRT Italia, Garante per la protezione dei dati personali, Autorità giudiziaria o clienti soggetti alla disciplina NIS2;
- utilizzi non autorizzati o anomalie di sistemi di IA, inserimento improprio di dati, mancata supervisione umana o output che abbiano prodotto o possano produrre effetti dannosi;
- esiti delle verifiche periodiche sulla sicurezza, test di ripristino, audit sui fornitori ICT e aggiornamenti rilevanti della Politica IA o delle politiche di sicurezza.
- qualsiasi violazione del Modello di Organizzazione e del Codice Etico, con l' indicazione delle ragioni delle difformità e dando atto del processo autorizzativo seguito.

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 e concernenti i reati disciplinati dalla presente procedura e riguardanti gli illeciti penali privacy e reati informatici.

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.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

SOMMARIO

1. OBIETTIVI DELLA PROCEDURA

La presente procedura individua e regola i criteri cui BITCONTROL s.r.l. deve attenersi nell'attività di selezione, assunzione e gestione del personale e dei relativi adempimenti.

I principi e le regole di condotta definite dalla presente procedura dovranno essere osservate anche dai soggetti terzi, eventualmente coinvolti, dalla funzione aziendale all'uopo preposta, ad operare in nome e per conto della società, nelle attività relative alla selezione, assunzione e gestione del personale.

I *Destinatari* che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella selezione, assunzione e gestione del personale (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.

È FATTO ESPLICITO DIVIETO DI:

- 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.

Il processo di selezione ed assunzione del personale, 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".
Infatti, una gestione non trasparente del processo di selezione ed assunzione del personale, potrebbe 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 BITCONTROL.
Nell'ipotesi di assunzione di soggetti facenti parti di Paesi Terzi, BITCONTROL 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".
Dunque, il presente protocollo è finalizzato ad assicurare il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

2. ACRONOMI 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	Responsabile Progettazione
RSCM	Responsabile singola commessa
RATTR	Responsabile Attrezzature e Mezzi

PROG	Programmatori
RGAD	Responsabile Gestione Archivi e Documenti
CDL	Consulente del lavoro
REC	Responsabile Esterno Contabilità

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

3. RIFERIMENTI NORMATIVI DEL MODELLO

- DECRETO LEGISLATIVO 231/2001 E S.S. MM.II (DI SEGUITO ANCHE D.LGS 231/01);
- CODICE ETICO DI BITCONTROL S.R.L.;
- CODICE DISCIPLINARE DI BITCONTROL S.R.L.
- MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO DI BITCONTROL S.R.L..

4. CAMPO DI APPLICAZIONE

La presente procedura si applica a tutti i *Destinatari* che siano coinvolti nella selezione, assunzione e gestione del personale, i quali dovranno verificare le competenze professionali richieste dalla Società.

Il presente Protocollo si applica alle seguenti attività, svolte dalle Funzioni Aziendali delle Risorse Umane di BITCONTROL:

a) selezione del personale (anche tramite l'ausilio di una società esterna);

b) assunzione del personale;

c) gestione dei rapporti continuativi di collaborazione;

d) gestione distacchi

Nel caso in cui le Funzioni Aziendali Responsabili della gestione del processo si avvalgano di eventuali soggetti terzi, che operano in nome e per conto della società, per l'esecuzione delle attività di cui ai precedenti punti, questi dovranno assicurare, attraverso la propria struttura organizzativa, il recepimento dei principi contenuti nel presente Protocollo.

5. RESPONSABILI DELLA PROCEDURA

Rientrano nel campo di applicazione della procedura di selezione del personale dipendente il RAM/RRU e il PRES.

6. REATI ASTRATTAMENTE IPOTIZZABILI

RECLUTAMENTO DEL PERSONALE

I principali reati e illeciti amministrativi potenzialmente rilevanti nell'ambito del processo in oggetto sono:

- i reati societari (richiamati dall'art. 25-ter del D. Lgs. n. 231/2001), tra cui: False comunicazioni sociali (art. 2621 c.c.); Fatti di lieve entità (art. 2621-bis c.c.); Corruzione tra privati (art. 2635 c.c.); Istigazione alla corruzione tra privati (art. 2635-bis c.c.);
- i reati contro la pubblica amministrazione (richiamati dall'art. 25 del D. Lgs. n. 231/2001), tra cui: Concussione (art. 317 c.p.); Corruzione per l'esercizio della funzione (art. 318 c.p.); Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.); Corruzione in atti giudiziari (art. 319-ter c.p.); Induzione indebita a dare o promettere utilità (art. 319-quater c.p.); Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.); Pene per il corruttore (art. 321 c.p.); Istigazione alla corruzione (art. 322 c.p.); Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.); Traffico di influenze illecite (art. 346 bis c.p.);
- i delitti contro la personalità individuale (richiamati dall'art. 25-quinquies del D. Lgs. n. 231/2001), tra cui: Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.);
- i delitti contro l'eguaglianza (richiamati dall'art. 25-terdecies del D.Lgs. n. 231/2001 rubricato "Razzismo e xenofobia"), tra cui: Propaganda e istigazione a delinquere per motivi di discriminazione razziale etica e religiosa (art. 604 bis c.p.)
- il reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (richiamato dall'art. 25-duodecies del D. Lgs. n. 231/2001);

AMMINISTRAZIONE DEL PERSONALE

I principali reati e illeciti amministrativi potenzialmente rilevanti nell'ambito del processo in oggetto sono:

- i reati contro il patrimonio mediante frode (richiamati dall'art. 24 del D. Lgs. n. 231/2001), tra cui: Truffa a danno dello Stato o di altro Ente Pubblico (art. 640, comma 2, n.1 c.p.); Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.); Frode informatica (art. 640 ter c.p.);
- i reati contro la pubblica amministrazione (richiamati dall'art. 25 del D. Lgs. n. 231/2001), tra cui: Concussione (art. 317 c.p.); Corruzione per l'esercizio della funzione (art. 318 c.p.); Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.); Corruzione in atti giudiziari (art. 319-ter c.p.); Induzione indebita a dare o promettere utilità (art. 319-quater c.p.); Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.); Pene per il corruttore (art. 321 c.p.);Istigazione alla corruzione (art. 322 c.p.); Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.); Traffico di influenze illecite (art. 346 bis c.p.);

- i reati societari (richiamati dall'art. 25-ter del D. Lgs. n. 231/2001), tra cui: Corruzione tra privati (art. 2635 c.c.); Istigazione alla corruzione tra privati (art. 2635-bis c.c.); i delitti contro il patrimonio mediante frode richiamati dall'art. 24 del D. Lgs. n. 231/2001), tra cui: Frode Informatica (art. 640-ter c.p.);
- i delitti informatici e trattamento illecito dei dati (richiamati dall'art. 24-bis del D. Lgs. n. 231/2001), tra cui: Documenti informatici (il riferimento è ai delitti di falso richiamati dall'art.491-bis c.p.); Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);

GESTIONE, FORMAZIONE E SVILUPPO DEL PERSONALE

I principali reati e illeciti amministrativi potenzialmente rilevanti nell'ambito del processo in oggetto sono:

- i reati contro la pubblica amministrazione (richiamati dall'art. 25 del D. Lgs. n. 231/2001), tra cui: Concussione (art. 317 c.p.); Corruzione per l'esercizio della funzione (art. 318 c.p.); Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c.p.); Corruzione in atti giudiziari (art. 319-ter c.p.); Induzione indebita a dare o promettere utilità (art. 319-quater c.p.); Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.); Pene per il corruttore (art. 321 c.p.); Istigazione alla corruzione (art. 322 c.p.); Peculato, concussione, induzione indebita dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.); Traffico di influenze illecite (art. 346 bis c.p.);
- i reati societari (richiamati dall'art. 25-ter del D. Lgs. n. 231/2001), tra cui: Corruzione tra privati (art. 2635 c.c.); Istigazione alla corruzione tra privati (art. 2635-bis c.c.);
- omicidio colposo e lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (articoli 589, comma secondo e 590, comma terzo del c.p., così richiamati dall'art. 25-septies del D. Lgs. n. 231/2001), avuto stretto riguardo ai corsi di formazione sulla materia;
- i reati ambientali (richiamati dall'art. 25-undecies del D. Lgs. n. 231/2001) avuto stretto riguardo ai corsi di formazione sulla materia.

7. INDICAZIONI COMPORTAMENTALI

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;
- adottare specifiche procedure di gestione dei rischi alla salute, igiene e sicurezza dei dipendenti distaccati presso i luoghi di lavoro estranei alla disponibilità giuridica della Società.

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 BITCONTROL;

- 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 BITCONTROL, 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.

7.1 LA VALUTAZIONE DEL CANDIDATO

Il processo di selezione del personale dovrà essere condiviso dal RAM/RRU e dal PRES.

La presente procedura deve essere applicata anche in caso di soggetti segnalati da referenti. In ogni caso, è fatto divieto di accettare segnalazioni che possano far incorrere la società nei reati di cui al D.lgs. 231/2001. In particolare, sono proibite le segnalazioni di soggetti dalla cui assunzione possano derivare vantaggi, per sé o per altri, ai dipendenti della Pubblica Amministrazione o ai loro parenti o affini.

Il RAM/RRU, ove necessario con il supporto del PRES, effettua colloqui con i candidati, finalizzati a valutarne le competenze tecniche e attitudinali;

Il RAM/RRU conserva tutta la documentazione prodotta nell'ambito del processo di selezione. Nel caso venga attivata una figura di intermediario, questi provvederà ad effettuare dei colloqui esplorativi ed a presentare alla Società una rosa ristretta di candidati. L'accesso e l'intervento sui dati dei candidati è consentito, esclusivamente, alle persone autorizzate ed è garantita la riservatezza nella trasmissione delle informazioni. Tale attività dovrà essere svolta nel pieno rispetto della vigente normativa in tema di *privacy*.

7.2 L'ASSUNZIONE

Se le valutazioni sui candidati, secondo le prescrizioni sopra indicate, 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.

7.3 IL PAGAMENTO DEL SALARIO MENSILE E LA GESTIONE DI RIMBORSI SPESE

Il CDL, per ciascun mese, elabora un elenco con i pagamenti da effettuare in favore dei dipendenti, che sottopone al PRES per un visto.

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.

7.4 L'ADOZIONE DEL MODELLO E IL SISTEMA SANZIONATORIO

Ai nuovi assunti verrà consegnata copia cartacea (o digitale) del Modello e del Codice Etico, a seguito della quale la risorsa sottoscriverà un documento per presa visione ed accettazione, con il quale si impegna al rispetto dei principi e delle regole negli stessi contenuti (tale documento verrà allegato al contratto e conservato).

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.

7.5 L'ASSUNZIONE DI PERSONALE STRANIERO

Oltre a quanto stabilito nel paragrafo precedente il RAM/RRU, in collaborazione con l'eventuale Funzione richiedente e/o eventuali soggetti terzi, si impegna a rispettare i seguenti ulteriori presidi di controllo nella selezione ed impiego di cittadini stranieri non comunitari, garantendo la tracciabilità della documentazione prodotta in ogni fase del processo.

In caso di assenza del permesso di soggiorno, il RAM/RRU e/o eventuali soggetti terzi all'uopo incaricati:

- richiedono alle Autorità competenti il nulla osta e verificano l'effettivo ricevimento dello stesso da parte dello Sportello Unico Immigrazione;
- raccolgono copia del visto d'ingresso, rilasciato dall'ambasciata e/o consolato italiano presso lo stato straniero, per motivi di lavoro subordinato del lavoratore;
- mantengono copia del permesso di soggiorno o della ricevuta rilasciata dall'ufficio postale.

La documentazione di cui ai punti precedenti deve pervenire alla Società e/o ad eventuali soggetti terzi all'uopo incaricati, in data antecedente l'entrata in Italia del cittadino straniero non comunitario.

In caso di possesso di un valido documento di soggiorno, il RAM/RRU e/o eventuali soggetti terzi all'uopo incaricati:

- verificano che il cittadino straniero non comunitario, già soggiornante in Italia, sia munito di regolare documento in corso di validità che abiliti a prestare lavoro (permesso di soggiorno europeo per soggiornanti di lungo periodo; permesso per lavoro subordinato o autonomo, per attesa di occupazione, per famiglia, per assistenza ai minori, per asilo politico, per protezione sociale, per motivi umanitari);
- se pendente domanda di rinnovo del permesso di soggiorno, controllano la relativa ricevuta postale rilasciata dall'autorità preposta;
- comunicano l'assunzione al Centro per l'impiego, competente per la sede di lavoro, il giorno precedente all'inizio dell'attività, inviando lo specifico modello.

I cittadini stranieri assunti presso la Società devono essere specificamente evidenziati all'interno dell'anagrafica dipendenti; tali posizioni vengono monitorate e, per quelle prossime alla scadenza, il RAM/RRU provvede a richiedere la documentazione necessaria entro la data di scadenza.

Resta, comunque, inteso che la responsabilità di rinnovo del permesso di soggiorno è in capo ai singoli dipendenti; il RAM/RRU ne monitora esclusivamente le scadenze. Tale onere di monitoraggio può essere espressamente affidato, tramite apposita delega, al responsabile di Funzione eventualmente incaricato.

In ogni caso, BITCONTROL s.r.l. e/o eventuali soggetti terzi all'uopo incaricati, ognuno per le parti di rispettiva competenza, si impegnano a garantire al lavoratore straniero non comunitario il trattamento retributivo ed assicurativo previsto dalle leggi vigenti e dai contratti collettivi nazionali di lavoro applicabili e ad effettuare, entro i termini di legge, le comunicazioni obbligatorie relative al rapporto di lavoro;

Nel caso in cui il lavoratore non adempia alle richieste di cui sopra o, comunque, non fornisca la relativa documentazione, il datore di lavoro– qualora il lavoratore fosse già stato assunto – potrà sospendere il rapporto di lavoro, in attesa dell'esito della procedura di rinnovo. In caso di esito negativo, il datore di lavoro potrà procedere con il licenziamento legittimo del lavoratore. Il

RAM/RRU comunicherà al CDA di procedere al licenziamento dei soggetti che non hanno ottenuto o richiesto il rinnovo.

7.6 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.

7.7 GESTIONE DEL PERSONALE DISTACCATO

Con l'istituto del distacco un datore di lavoro (distaccante) pone temporaneamente uno o più lavoratori(distaccati) a disposizione di un altro soggetto (distaccatario), per l'esecuzione di una determinata attività lavorativa. La fattispecie è disciplinata, nel settore privato, dal D. Lgs. 276/2003, attuazione della legge 14/2003, attuazione della legge 14/2003 (cosiddetta "Legge Biagi"). La normativa vigente (D. Lgs. 81/08 e ss.mm.), e le svariate sentenze della Cassazione hanno definito quali sono gli obblighi in materia di salute e sicurezza sul lavoro gravanti in capo al distaccante e al distaccatario. Nel presente articolo tratteremo gli adempimenti in carico al Datore di Lavoro che "ospita" i lavoratori di altre aziende, ovvero il distaccatario.

Orbene, nell'ipotesi di un eventuale distacco del proprio personale dipendente, BITCONTROL presta molta attenzione alla pratica del distacco, predisponendo idonei presidi di tutela per le persone giuridiche coinvolte, in quanto l'articolo 25-septies del D.Lgs. 231/01 include i delitti di cui agli articoli 589 e 590 del Codice penale nell'elenco dei reati presupposto.

Pertanto, i predetti presidi sono necessari poichè se, in astratto, tanto in caso di omicidio colposo quanto in caso di lesioni colpose gravi o gravissime con violazione delle norme antinfortunistiche, è configurabile una responsabilità penale sia per l'impresa distaccante che per l'impresa distaccataria, è bene valutare se sussista uno dei requisiti fondamentali richiesti dal D.Lgs. 231/01, ovvero l'interesse o vantaggio dell'ente.

Prima di tutto, è imprescindibile la stipula di un contratto scritto (in verità non richiesto dal D.Lgs. 276/2003) nel quale indicare le parti coinvolte e le loro attività, la mansione del dipendente nell'impresa cedente e quelle che ricoprirà nell'impresa distaccataria, un'esaustiva esposizione dell'interesse al distacco, una descrizione analitica delle lavorazioni nelle quali verranno coinvolti i distaccati, la formazione già erogata dal concedente e quella che verrà somministrata dall'utilizzatore, i DPI distribuiti dal distaccante e quelli che verranno forniti dal distaccatario, la data di inizio e la data di ultimazione, l'identificazione del luogo in cui i distaccati lavoreranno, il consenso dei distaccati espresso in calce o su atto separato (solo se l'unità produttiva di destinazione è ubicata a più di 50 km dalla sede in cui il lavoratore è attualmente adibito o se mutano le mansioni rispetto a quelle ordinariamente svolte).

Ciò posto, è bene che il distaccatario chieda copia del giudizio di idoneità alla mansione ex articolo 41 comma 6 del D.Lgs. 81/2008 e dei registri attestanti la formazione generale e specifica, a seconda dei casi, ai sensi dell'Accordo Stato-Regioni, nonché il modulo Unificato Lav relativo al distacco16.

Successivamente, sarà necessario che il distaccatario formi il lavoratore in relazione alle specificità delle lavorazioni da effettuare e ai rischi presenti sul luogo di distacco, distribuisca eventuali dispostivi di protezione individuali, fornisca copia delle procedure operative e del codice etico. Semplificando, deve quindi gestire il distaccato alla stregua di un proprio assunto.

Il distaccante dovrebbe tuttavia preoccuparsi di inserire clausole contrattuali che obblighino l'altra parte a comportarsi secondo le disposizioni del codice etico aziendale, anche attraverso la rescissione dell'accordo di distacco in caso di violazioni. Inoltre, è consigliabile prevedere con chiarezza le lavorazioni per verificare che queste corrispondano alla mansione richiesta e che non siano necessari ulteriori presidi di tutela.

Sul punto, è vantaggioso improntare i rapporti sulla trasparenza, poiché solo un'apposita dichiarazione inerente le lavorazioni può consentire la collaborazione in tema di sicurezza pretesa dall'attuale orientamento della Corte di Cassazione.

Dunque, BITCONTROL S.R.L., prima di distaccare un lavoratore:

- verifica la presenza di adeguate condizioni di sicurezza per l'attività che sarà svolta;
- informa e forma il lavoratore sui rischi tipici generalmente connessi allo svolgimento delle mansioni per le quali egli viene distaccato.

Nel caso in cui BITCONTROL S.r.l. distacchi il proprio personale dipendente presso altra società, tali dipendenti sono soggetti -nell'espletamento delle proprie mansioni lavorative - alle direttive impartite dai responsabili della società distaccataria. Essi sono, quindi, tenuti al rispetto:

a) dei principi di comportamento previsti dal presente Modello 231;

b) del Modello Anticorruzione e Trasparenza di Gruppo;

c) di quanto previsto dal Modello predisposto dalla società distaccataria.

7.8 FORMAZIONE DEL PERSONALE SUL MODELLO EX D.LGS. 231/2001

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.

La partecipazione ai corsi di formazione ha carattere obbligatorio.

8. 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*.

9. LA GESTIONE DEGLI OMAGGI

Il Codice Etico stabilisce la politica di BITCONTROL s.r.l. 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, 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.

10. ARCHIVIAZIONE

Tutti i documenti relativi all'assunzione del personale sono archiviati dal RAM/RRU, con il supporto del RGAD, in luoghi non accessibili a soggetti esterni all'azienda; quelli conservati elettronicamente su un *pc* devono essere protetti da *password*.

11. FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutti i *Destinatari* coinvolti 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, 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.

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.
COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2001	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

La presente procedura, uniformemente e ad integrazione del sistema di gestione della salute e sicurezza sul lavoro adottato da BITCONTROL S.r.l., individua i principi, i protocolli e i controlli organizzativi conformi all'art. 30 del D.Lgs. 9 aprile 2008, n. 81 e s.m.i., al D.Lgs. 8 giugno 2001, n. 231, al Decreto del Ministero del Lavoro 13 febbraio 2014, all'Accordo Stato-Regioni del 17 aprile 2025 e alle ulteriori disposizioni vigenti, al fine di verificare e controllare la corretta applicazione degli obblighi di tutela della salute e della sicurezza nei luoghi di lavoro.

Le prescrizioni della presente procedura integrano i principi di comportamento contenuti nel Modello di Organizzazione, Gestione e Controllo, nel Codice Etico, nel Codice Disciplinare, nelle politiche, nei regolamenti e nelle procedure aziendali vigenti, che tutti i Destinatari sono tenuti a conoscere e rispettare.Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Modello e nel Codice Etico.

È fondamentale che l'Organismo di Vigilanza venga posto nella condizione di conoscere tutta la documentazione aziendale, relativamente agli adempimenti posti in essere dalla società, in conformità a quanto previsto dalla vigente legislazione nazionale in materia di tutela della salute e della sicurezza negli ambienti di lavoro.

In particolare, la presente procedura ha lo scopo di fornire all'OdV e ai responsabili delle altre 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.

I Destinatari 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) - 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 e addestramento dei lavoratori, ai sensi del D.Lgs. 81/2008 e dell'Accordo Stato-Regioni del 17 aprile 2025, con particolare riferimento al posto di lavoro, alle mansioni, ai rischi specifici e alle misure di prevenzione. La formazione e, ove prevista, l'addestramento devono essere effettuati in occasione dell'assunzione e, comunque, prima dell'adibizione alla mansione, nonché in caso di trasferimento o cambiamento di mansioni, introduzione di nuove attrezzature, tecnologie, sostanze o preparati pericolosi e ogniqualvolta l'evoluzione dei rischi o della normativa lo richieda;
- 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 ACRONOMI 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
RGAD	Responsabile Gestione Archivi e Documenti

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE RELATIVO AL SERVIZIO PREVENZIONE E PROTEZIONE DI BITCONTROL S.R.L..

3 RIFERIMENTI NORMATIVI DEL MODELLO

- DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 E S.M.I.;

- DECRETO LEGISLATIVO 9 APRILE 2008, N. 81 E S.M.I.;

- ACCORDO STATO-REGIONI DEL 17 APRILE 2025 IN MATERIA DI FORMAZIONE SULLA SALUTE E SICUREZZA SUL LAVORO;

- DECRETO-LEGGE 31 OTTOBRE 2025, N. 159, CONVERTITO CON MODIFICAZIONI DALLA LEGGE 29 DICEMBRE 2025, N. 198;

- DECRETO DEL MINISTERO DEL LAVORO E DELLE POLITICHE SOCIALI 13 FEBBRAIO 2014;

- NORMA UNI EN ISO 45001:2018 E SISTEMA DI GESTIONE AZIENDALE PER LA SALUTE E SICUREZZA SUL LAVORO;

- CODICE ETICO, CODICE DISCIPLINARE E MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI BITCONTROL S.R.L.;

- POLITICHE, REGOLAMENTI, ISTRUZIONI E PROCEDURE AZIENDALI VIGENTI, IVI COMPRESA LA POLICY AZIENDALE SULL'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE, PER QUANTO APPLICABILE.

4 CAMPO DI APPLICAZIONE

La presente procedura si applica a tutti i destinatari che operano in BITCONTROL s.r.l., ognuno nell'ambito delle proprie attribuzioni e competenze. L'applicazione deve essere estesa anche ai terzi *Destinatari* ovvero a 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.

5 RESPONSABILI DELLA PROCEDURA

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 BITCONTROL 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*.

6 AREA SENSIBILE CONCERNENTE I REATI IN TEMA DI SALUTE E SICUREZZA SUL LAVORO

La presente procedura, riguarda i reati previsti dall'art. 25 septies del D.Lgs. n. 231/2001 (ovvero i "***Reati in materia di salute e sicurezza sul lavoro***"), introdotti dall'art. 9 della Legge 3 agosto2007, n. 123, in forza del quale la responsabilità amministrativa per gli Enti deriva a seguito della commissione dei reati di omicidio colposo e lesioni colpose gravi o gravissime derivanti da violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

In questa sede è opportuno ricordare che il decreto legislativo n. 81 del2008, integrato e/o modificato dal D.Lgs 81/2015 in materia di disciplina organica dei contratti e revisione della normativa in tema di mansioni, a norma dell'articolo 1 comma 7 della legge 10dicembre, n. 183 e a cui nel contesto della presente parte speciale si farà anche sempre implicito riferimento (Testo Unico in materia di Sicurezza ed igiene del lavoro, di seguito, per brevità "TUS") ha stabilito un contenuto minimo essenziale del modello organizzativo in questa materia. L'art. 30 del TUS dispone che:

"*il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi: a) al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;*

b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;

c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;

d) alle attività di sorveglianza sanitaria;

e) alle attività di informazione e formazione dei lavoratori;

f) alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.

Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico."

La norma, pertanto, comporta che, per espressa volontà del Legislatore, debbano essere considerate "a rischio" e debbano essere presidiate, a prescindere da ogni valutazione di merito sulla concreta possibilità di realizzazione di reati, le aree e le attività indicate ed interessate dall'articolo stesso.

In tema di reati in materia di salute e sicurezza sul lavoro, l'art. 25-septies del Decreto, prevede e regolamenta i casi di "*Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*".

Ai sensi dell'art. 25-septies del Decreto:

"*In relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione dell'articolo*

55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura pari a 1.000 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno.

Salvo quanto previsto dal comma 1, in relazione al delitto di cui all'articolo 589 del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non inferiore a tre mesi e non superiore ad un anno. In relazione al delitto di cui all'articolo 590, terzo comma, del codice penale, commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applica una sanzione pecuniaria in misura non superiore a 250 quote. Nel caso di condanna per il delitto di cui al precedente periodo si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, per una durata non superiore a sei mesi."

Ai sensi dell'art. 55, comma 1 e 2, d.lgs. 81/2008 (come per ultimo anche integrato e/o modificato dal D. Lgs. 81/2015 di cui si è detto, TUS):

"*1. È punito con l'arresto da quattro a otto mesi o con l'ammenda da 2.500 a 6.400 Euro il datore di lavoro:*

a) per la violazione dell'art. 29, comma 1;

b) che non provvede alla nomina del responsabile del servizio prevenzione e protezione ai sensi dell'articolo 17, comma 1, lettera b, o per la violazione dell'articolo 34, comma 2.

2. Nei casi previsti al comma 1, lettera a), si applica la pena dell'arresto da quattro a otto mesi se la violazione è commessa:

a) nelle aziende di cui all'articolo 31, comma 6, lettere a), b), c) ,d), f).

b) in aziende che svolgono attività che espongono i lavoratori a rischi biologici di cui all'art. 268, comma 1, lettere c) e d), da atmosfere esplosive, cancerogeni, mutageni e da attività di manutenzione, rimozione, smaltimento e bonifica di amianto;

c) per le attività disciplinate dal titolo IV caratterizzate dalla compresenza di più imprese e la cui entità presunta di lavoro non sia inferiore a 200, uomini giorno."

Le sanzioni a carico dell'Ente, che operi alle condizioni previste dall'art. 55, comma 2, TUS, sono perciò più severe laddove siano mancate:

- la valutazione dei rischi;
- l'adozione del Documento di valutazione dei Rischi.

Il reato di omicidio colposo (art. 589 c.p.), lesioni personali colpose gravi e gravissime (art. 590 c.p.) si configura con il fatto di aver cagionato, per colpa, la morte di un uomo oppure di aver cagionato, per colpa, una lesione personale dalla quale è derivata una malattia grave1 o gravissima.

Il reato costituisce presupposto della responsabilità amministrativa degli enti soltanto se commesso con violazione delle norme sulla prevenzione degli infortuni sul lavoro.

In genere, i reati considerati dal Decreto sono dolosi, ossia posti in essere volontariamente dal soggetto con quello scopo specifico, e il Modello organizzativo ha una funzione di esimente della responsabilità di BITCONTROL S.R.L. se le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il Modello.

I reati considerati in questa Sezione della Parte Speciale sono invece di natura colposa, ossia conseguenza di negligenza, imprudenza, imperizia o inosservanza di leggi e regolamenti da parte dell'autore del reato, e pertanto la funzione di esimente del Modello organizzativo, è rappresentata dall'introduzione di previsioni volte a far si che i Destinatari pongano in essere una condotta (non accompagnata dalla volontà dell'evento morte/lesioni personali) rispettosa delle procedure previste dal sistema di prevenzione e protezione ai sensi del TUS, congiuntamente agli adempimenti e agli obblighi di vigilanza previsti dal Modello organizzativo.

Si tratta di uno dei pochi casi (unitamente agli illeciti ambientali) in cui il presupposto per la responsabilità dell'ente è ancorato ad un fatto colposo e non doloso; ciò comporta la necessità di valutare i rischi secondo parametri differenti rispetto a quelli utilizzati per la responsabilità dolosa.

Non mancano perplessità in ordine al requisito d'imputabilità oggettiva a carico dell'ente, vale a dire l'interesse o il vantaggio derivanti dal reato. Trattandosi di fatti colposi non è agevole individuare quale vantaggio o interesse possa derivare ad un ente dal fatto della morte o delle lesioni di un dipendente determinate da colpa.

A tal proposito, si tende ad individuare nella condotta, piuttosto che nel reato, i parametri di riferimento per far sorgere la responsabilità dell'ente. Il vantaggio o l'interesse deriverebbero, di conseguenza, non dal fatto della morte o delle lesioni, ma dall'utilità conseguita (ad esempio risparmio in termini di spesa) dalla condotta negligente causalmente correlata all'evento.

6.1 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.

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.

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.

7 Il DOCUMENTO VALUTAZIONE RISCHI

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 osservanza a quanto disposto dalla suddetta normativa, BITCONTROL S.R.L. ha adottato 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.

Invero, il DVR è il 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, e contiene:

a. una relazione sulla valutazione dei rischi per la sicurezza e la salute nei luoghi di lavoro, nella quale sono specificati i criteri adottati per tale valutazione, effettuata in relazione alla natura dell'attività dell'impresa;
b. l'individuazione delle misure di prevenzione, di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione di cui alla lettera a). 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;
c. il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza.

Il documento è custodito presso la Società.

Il DL può, se necessario, coinvolgere, in tale processo o in alcune sue fasi, altri soggetti aziendali.

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.

IL DVR, AI SENSI DELL'ART. 28 DEL D.LGS. N. 81/08, CONTIENE:

• una relazione circa la valutazione di tutti i rischi per la sicurezza e la salute a cui sono esposti i lavoratori;

• l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuale adottati, a seguito della valutazione di cui all'articolo 17, comma 1, lettera a);

• il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli 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, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha 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.

Il DVR di BITCONTROL S.R.L. rispetta le indicazioni previste dalle specifiche norme sulla valutazione dei rischi contenute nel D.lgs. 81/08.

7.1 DESCRIZIONE DEL PROCESSO DI VALUTAZIONE DEI RISCHI

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.

7.2 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 riguarda, tra l'altro, la scelta delle attrezzature di lavoro, delle sostanze e dei preparati impiegati, la sistemazione dei luoghi di lavoro e i rischi cui sono esposti gruppi di lavoratori soggetti a rischi particolari, compresi lo stress lavoro-correlato, i rischi psicosociali e organizzativi, il lavoro al videoterminale, il lavoro agile o da remoto, le trasferte e le attività presso siti dei clienti, le lavoratrici in stato di gravidanza, i minori e i rischi connessi alle differenze di genere, età, provenienza e tipologia contrattuale. La valutazione tiene altresì conto dell'evoluzione tecnologica, dell'introduzione di sistemi digitali e di intelligenza artificiale e delle eventuali ricadute sulla salute e sicurezza dei lavoratori.

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:

- TASSATIVAMENTE OBBLIGATORIE;
- DA IMPIEGARE CORRETTAMENTE E CONTINUAMENTE;
- DA OSSERVARE PERSONALMENTE.

7.3 CERTIFICAZIONI DI SISTEMA ISO

BITCONTROL 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 45001:2018 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;

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.

8. SALUTE E SICUREZZA SUI LUOGHI DI LAVORO – RISCHIO BIOLOGICO ED EMERGENZE SANITARIE

Il Datore di Lavoro, con il supporto del RSPP e del Medico Competente, valuta il rischio biologico in relazione alle attività svolte, ai luoghi di lavoro, alle trasferte e agli accessi presso sedi o impianti di clienti e committenti, aggiornando il DVR e le misure di prevenzione quando intervengano nuove evidenze scientifiche, disposizioni delle Autorità competenti o situazioni emergenziali.

In presenza di emergenze sanitarie o di specifici rischi biologici, la Società adotta e diffonde tempestivamente protocolli e istruzioni operative coerenti con le indicazioni delle Autorità sanitarie e del Ministero del Lavoro, assicurando informazione, disponibilità dei presidi necessari, corretta gestione degli accessi, pulizia e igiene degli ambienti, organizzazione delle attività e protezione dei soggetti particolarmente vulnerabili.

I lavoratori sono tenuti a rispettare le misure organizzative e igienico-sanitarie comunicate dalla Società, a utilizzare correttamente i dispositivi di protezione eventualmente prescritti e a segnalare tempestivamente al proprio responsabile e al RSPP ogni situazione di rischio o sintomatologia rilevante, nel rispetto della riservatezza e della disciplina in materia di protezione dei dati personali.

Le misure emergenziali sono formalizzate, comunicate con strumenti idonei a garantirne la conoscibilità e sottoposte a periodico riesame. La relativa documentazione è conservata e resa disponibile all'Organismo di Vigilanza nell'ambito dei flussi informativi previsti dalla presente procedura.

8 BIS SALUTE E SICUREZZA SUI LUOGHI DI LAVORO – GESTIONE EMERGENZA COVID 19

Per quanto concerne il rischio biologico, in relazione all'emergenza Coronavirus in atto sul territorio Italiano ed in considerazione dei recenti sviluppi e del continuo aggiornamento delle disposizioni governative per il contenimento del virus COVID-19 ed in particolare ai DPCM emanati dal Consiglio dei Ministri si pone l'obbligo per tutto il personale di attenersi scrupolosamente alle misure emanate dalle autorità statali così come integrato nel "*Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro e nei cantieri temporanei e mobili*".
Allo stesso modo si pone l'obbligo del rispetto delle ordinanze regionali e delle procedure di sicurezza adottate dal datore di lavoro per rispondere all'emergenza sanitaria.
Attualmente data la possibile presenza generale dell'agente patogeno, non si può individuare una particolare lavorazione prevista dal capitolato per la quale possa ritenersi più elevata la possibilità di contagio; pertanto, la presenza dell'agente biologico non rappresenta uno specifico oggetto dell'attività stessa, ma esso può essere sempre presente.

Si può ragionevolmente affermare che i lavoratori, durante le loro attività, siano esposti al rischio di contagio da COVID19 a causa di molteplici fattori facendo sì che l'esposizione al rischio biologico subisca un notevole incremento.

Attualmente la società Bit Control S.r.l. e le aziende all'interno prevede procedure per in contenimento del rischio COVID 19 che possono essere sintetizzate in: distanziamento sociale, utilizzo di dispositivi di protezione individuale, presidi di pulizia per l'igiene delle mani, divieti di riunioni e formazione sfasamento temporale e quant'altro previsto dal protocollo di sicurezza sino al termine dell'emergenza.

Data la possibile presenza generale dell'agente patogeno, non si può individuare una particolare lavorazione prevista dal capitolato per la quale possa ritenersi più elevata la possibilità di contagio; pertanto la presenza dell'agente biologico non rappresenta uno specifico oggetto dell'attività stessa, ma esso può essere sempre presente. Si può ragionevolmente affermare che i lavoratori, durante le loro attività, siano esposti al rischio di contagio da COVID19 a causa di molteplici fattori facendo sì che l'esposizione al rischio biologico subisca un notevole incremento.

Durante l'esecuzione delle attività, è assolutamente necessario rispettare la distanza minima tra le persone di almeno 1 metro. Nel caso in cui, per casi "strettamente necessari" per le attività da eseguirsi, sia inevitabile la distanza ravvicinata tra due operatori, gli operatori dovranno indossare guanti e mascherina.

L'utilizzo costante dei DPI è comunque consigliabile a prescindere dalla distanza minima tra gli operatori.

Nel caso in cui un lavoratore manifesti sintomi quali febbre, tosse, difficoltà respiratorie, è necessario che non si presenti sul luogo di lavoro e che, in ogni caso, contatti il proprio medico curante o il numero 1500 o il numero 112 o quelli della USL di riferimento.

I lavoratori saranno muniti di soluzioni idroalcoliche per il lavaggio delle mani. I lavoratori devono lavarsi le mani con tale soluzione all'ingresso del campus, prima e dopo le pause pranzo e all'ingresso e all'uscita dai servizi igienici. Si consiglia di limitare uso promiscuo delle attrezzature e dei mezzi. Qualora non fosse possibile, questi dovranno essere igienizzati prime e dopo l'utilizzo con apposita soluzione idroalcolica e/o dovranno essere utilizzate con guanti.

Il "Protocollo condiviso di regolazione delle misure per il contrasto ed il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro" in costante aggiornamento sono parte integrante del presente

documento e gestito in maniera puntuale dal Datore di lavoro e dal Servizio di Prevenzione e Protezione con comunicazioni certificate che possano arrivare a tutti i lavoratori in maniera più semplice e diretta possibile.

IN LINEA GENERALE ED A TITOLO NON ESAUSTIVO, PER RIDURRE AL MINIMO IL RISCHIO BIOLOGICO DERIVANTE DA CONTAGIO COVID-19 È NECESSARIO CHE SIANO ADOTTATE:

- tenersi costantemente informati sui provvedimenti adottati dalle istituzioni (organi di governo nazionale, regionale e comunale);
- garantire il rispetto della distanza di almeno 1 metro tra i lavoratori durante l'attività lavorativa ed evitare l'accesso promiscuo ad ambienti ristretti;
- qualora non fosse possibile mantenere tale distanza di sicurezza, esaminare, ove possibile, un'eventuale diversa organizzazione del lavoro (es. turnazione personale) e/o un nuovo cronoprogramma dei lavori;
- qualora il lavoro imponga di lavorare a distanza interpersonale minore di un metro e non siano possibili altre soluzioni organizzative è comunque necessario l'uso delle mascherine, e altri dispositivi di protezione (guanti, occhiali, tute, cuffie, camici, ecc…) conformi alle disposizioni delle autorità scientifiche e sanitarie;
- Favorire i luoghi aperti ai locali chiusi, mantenere sempre la distanza interpersonale di almeno 1 metro;

limitare il numero dei partecipanti negli incontri fissati, trattenersi il tempo strettamente necessario ed utilizzare locali di spazi adeguati;

- mettere a disposizione presso il singolo sito di intervento appositi presidi igienizzanti;
- mantenere obbligatoriamente lo sfasamento temporale laddove le attività risultino naturalmente consecutive o ove sia applicabile;
- laddove non sia possibile garantire lo sfasamento temporale tra le lavorazioni, per motivi tecnicooperativi, si dovrà mantenere obbligatoriamente lo sfasamento spaziale. In tal caso le aree di lavoro dovranno essere separate e delimitate al fine di ridurre le interferenze tra le due organizzazioni e tali da garantire che ogni soggetto possa rispettare la distanza interpersonale di almeno 1 m;
- in tutti quei casi di lavorazioni contemporanee, in cui lo sfasamento spaziale non possa garantire la distanza interpersonale di almeno 1 m, si valuterà di attuare misure compensative (es. la dotazione al personale di DPI aggiuntivi rispetto a quelli previsti per la specifica lavorazione come guanti, tute monouso tyvek, mascherine facciali filtranti);
- limitare l'uso del medesimo mezzo e delle medesime attrezzature a più operatori, e in ogni caso garantire le misure interpersonali previste dai Decreti ministeriali indicati;
- l'eventuale passaggio o uso da parte di più persone di mezzi, attrezzature e di materiale vario o di documentazione dovrà avvenire osservando idonee misure igieniche (utilizzo di guanti, sterilizzazione delle superfici, ecc);

Per tutto quanto non elencato si fa riferimento ai DPCM e alle specifiche ordinanze regionali per l'organizzazione delle attività lavorative di cantiere.

9 Il PIANO DI MIGLIORAMENTO

La Società elabora un piano di miglioramento sulla base della politica aziendale, degli obiettivi con evidenza di azioni, indicatori, priorità di intervento, costi, tempi e responsabilità.

10 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.

10.1 L'ACQUISTO DI BENI STRUMENTALI E LA VERIFICA DELLO STATO MANUTENTIVO

Nel caso di acquisto di impianti, oltre a quanto previsto dalla PMOG 05 sulla scelta dei *partner* commerciali, che si richiama per formarne parte integrante della presente procedura, si devono adottare i seguenti presidi:

1. per ogni acquisto il RATTR dovrà verificare la corrispondenza di quanto eventualmente fornito con le specifiche di acquisto e le migliori tecniche presenti sul Mercato;
2. 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.

Sul punto, si rinvia a quanto previsto dal sistema di gestione della sicurezza sul lavoro.

L'Azienda, con periodicità semestrale, dovrà garantire la regolare manutenzione dei mezzi e apparecchiature utilizzati dagli amministratori, dai dirigenti e dai lavoratori, con particolare riferimento a quelli utilizzati nell'ambito delle attività di installazione e manutenzione svolte dall'Azienda presso i Committenti.

La verifica dovrà essere effettuata dal RATTR, e l'eventuale manutenzione dovrà essere autorizzata dal RAM/APVG.

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).

10.2 I CONTRATTI DI APPALTO

Gli appaltatori, i subappaltatori, i lavoratori autonomi e gli altri soggetti esterni, per poter operare all'interno delle sedi aziendali o in collaborazione con la Società, devono fornire evidenza del possesso dei requisiti di idoneità tecnico-professionale e del rispetto della normativa applicabile, inclusi gli eventuali requisiti relativi alla patente a crediti nei cantieri temporanei o mobili, nonché dei parametri e delle regole definiti dalla Società nelle 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.

11 ATTIVITÀ DI NATURA ORGANIZZATIVA, QUALI GESTIONE DELLE EMERGENZE E PRIMO SOCCORSO

Il Datore di Lavoro è tenuto ad analizzare le possibili emergenze e le relative modalità di gestione, individuando le possibili situazioni di emergenza, nonché il numero di persone che possono essere presenti nei luoghi di lavoro.

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.

12 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.*).

13 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).

14 ATTIVITÀ DI SORVEGLIANZA SANITARIA

Il DL nomina il Medico Competente per l'effettuazione della sorveglianza sanitaria. Il DL vigila sul corretto svolgimento dei compiti da parte del MC e provvede ad individuare i lavoratori che dovranno effettuare la visita medica entro le scadenze previste dal protocollo di sorveglianza sanitaria e di rischio. Prima d'adibire il lavoratore alla mansione prevista, il DL verifica il rilascio del giudizio d'idoneità alla mansione stessa, sia in caso di prima assegnazione che a seguito di un cambio di mansione.

15 ATTIVITÀ DI INFORMAZIONE E FORMAZIONE DEI LAVORATORI

Il Datore di Lavoro assicura mezzi e risorse adeguati per lo svolgimento delle attività di informazione, formazione e addestramento, avvalendosi delle competenze interne o esterne necessarie. Approva il Programma di formazione, informazione e addestramento proposto dal RSPP, con il coinvolgimento del RLS e del Medico Competente per quanto di competenza. Il programma è aggiornato in occasione della revisione o rielaborazione della valutazione dei rischi, di modifiche normative, nuove assunzioni, trasferimenti o cambiamenti di mansione, introduzione di nuove macchine, attrezzature, impianti, sostanze, tecnologie o modalità operative e in ogni caso in cui emergano nuovi rischi.

Il RSPP, in coordinamento con la funzione Amministrazione/Risorse Umane, assicura la registrazione della formazione, informazione e dell'addestramento di ciascun lavoratore, compresi i neoassunti, e la conservazione della documentazione comprovante le attività svolte, le verifiche di apprendimento, l'efficacia della formazione e le qualifiche conseguite. Le competenze acquisite sono annotate nei sistemi e nei fascicoli previsti dalla normativa vigente, incluso, quando operativo e applicabile, il fascicolo elettronico del lavoratore.

Al termine degli interventi formativi deve essere verificato l'apprendimento e, secondo i casi, l'efficacia della formazione durante lo svolgimento della prestazione lavorativa, nel rispetto delle modalità stabilite dall'Accordo Stato-Regioni del 17 aprile 2025 e dalle successive indicazioni applicative.

Nell'ambito del programma formativo, i lavoratori ricevono specifica informazione sui principi del Modello 231, sul Codice Etico, sul sistema disciplinare, sui canali di segnalazione e whistleblowing, nonché sui ruoli, compiti e responsabilità delle figure coinvolte nel sistema di prevenzione e protezione.

Al momento dell'assunzione, e comunque prima dell'effettivo inserimento nella mansione, la funzione Amministrazione/Risorse Umane consegna o rende disponibili al dipendente, con modalità idonee a garantirne l'accessibilità e la tracciabilità, il Codice Etico, il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001, il Codice Disciplinare, la presente procedura, le politiche, i regolamenti, le informative e le istruzioni aziendali vigenti applicabili al rapporto e alla mansione. Tra tali documenti rientrano anche le policy relative all'utilizzo degli strumenti informatici e dell'intelligenza artificiale, alla protezione dei dati, alla riservatezza e alle modalità organizzative del lavoro, ove applicabili.

La consegna o messa a disposizione della documentazione aziendale è accompagnata da un'informativa sui contenuti essenziali e dalla raccolta di una dichiarazione di ricezione, presa visione e impegno al rispetto. Ogni successivo aggiornamento rilevante è comunicato tempestivamente ai lavoratori e, ove necessario, è seguito da specifica formazione o nuova presa visione. L'addestramento consiste nello svolgimento di prove pratiche per l'uso corretto e sicuro di attrezzature, macchine, impianti, sostanze e dispositivi, compresi i dispositivi di protezione individuale, ed è tracciato in apposito registro, anche informatizzato.

16 ACQUISIZIONE DI DOCUMENTAZIONI E CERTIFICAZIONI OBBLIGATORIE PER LEGGE

La definizione delle modalità di gestione di tale documentazione è effettuata stabilendo:

a. le modalità di comunicazione della documentazione;
b. il sistema di conservazione e controllo;
c. le modalità di revisione, necessarie specialmente in caso di cambiamenti organizzativi, tecnici, strutturali, dei processi, *etc.*;
d. la figura in azienda che ne ha la responsabilità.

17 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.

L'Organismo di Vigilanza deve vigilare sulla effettiva approvazione di tale stanziamento.

18 RIESAME

Con riferimento agli adempimenti inerenti la sicurezza sul lavoro, con cadenza annuale, il DL deve, anche con l'ausilio di consulenti esterni, riesaminare il Modello Organizzativo Gestionale per verificare che:

- sia attuato con efficacia;
- sia idoneo per il mantenimento ed il miglioramento, nel tempo, delle 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.

Gli argomenti che il DL dovrà attenzionare sono i seguenti:

i. i risultati del monitoraggio interno, con riferimento al grado di raggiungimento degli obiettivi;
ii. gli esiti delle azioni intraprese nel precedente riesame e la loro efficacia;
iii. i dati sugli infortuni e malattie professionali;
iv. le analisi delle cause di eventuali infortuni, incidenti e situazioni di emergenza;
v. le relazioni del Medico Competente, se nominato;
vi. 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;
vii. rapporti sulle prove di emergenza;
viii. risultati delle azioni correttive e preventive intraprese sul modello;
ix. risultati della consultazione e del coinvolgimento;
x. dati sulla formazione e addestramento effettuati;
xi. report o segnalazioni da parte dell'OdV;
xii. 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 ed i temi trattati devono rispettare anche quanto previsto dalla legislazione.

19 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

I soggetti 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;
- la documentazione attestante la consegna ai neoassunti e gli aggiornamenti del Codice Etico, del Modello 231, del Codice Disciplinare, delle politiche e dei regolamenti aziendali applicabili, nonché le relative prese visione;
- 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" cui si rimanda.

L'Organismo di Vigilanza, alla luce delle risultanze di cui sopra, propone l'eventuale aggiornamento del Modello o delle procedure previste per la sua attuazione, previa condivisione con il Datore di Lavoro.

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.

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.
COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

SOMMARIO

1 OBIETTIVI DELLA PROCEDURA E VIOLAZIONE DEL DIRITTO D'AUTORE

Il presente protocollo definisce i ruoli, le responsabilità operative, le attività di controllo e i principi di comportamento adottati da BITCONTROL S.r.l. nell'ambito dei processi di acquisizione, creazione, sviluppo, modifica, licenza, utilizzo, pubblicazione, distribuzione e conservazione delle opere dell'ingegno, del software, delle banche dati, della documentazione tecnica e dei contenuti generati o rielaborati mediante sistemi di intelligenza artificiale, con riguardo alle attività a rischio connesse alle fattispecie previste dall'art. 25-novies del D.Lgs. 231/2001, nel rispetto dei principi di trasparenza, autorizzazione, segregazione dei compiti e tracciabilità.

La procedura è finalizzata a prevenire la pirateria, la duplicazione o diffusione abusiva di software e contenuti, l'estrazione e il reimpiego illecito di banche dati, il web scraping non autorizzato, l'utilizzo di codice o materiali protetti in violazione delle licenze, nonché la produzione e diffusione illecita di contenuti sintetici o manipolati mediante IA.

Le prescrizioni della presente procedura integrano i principi del Codice Etico, della Politica IA e del Modello 231 di BITCONTROL e si coordinano, in particolare, con la PMOG 08 in materia di reati informatici e sicurezza dei sistemi e con la PMOG 16 sulla gestione e l'utilizzo dei sistemi di intelligenza artificiale.

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.

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.

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.

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 n. 132/2025 ha introdotto l'art. 612-quater c.p., relativo all'illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale. È pertanto vietata la cessione, pubblicazione o diffusione, senza consenso, di immagini, video o voci falsificati o alterati mediante IA, idonei a indurre in inganno sulla loro genuinità e a cagionare un danno ingiusto.

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.

BITCONTROL 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".

2 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 E DI OPERE PROTETTE: È VIETATO INSERIRE NEI SISTEMI DI IA DATI PERSONALI NON ANONIMIZZATI, CODICE SORGENTE, CONFIGURAZIONI DI RETE O DI IMPIANTO, CREDENZIALI, API KEY, DOCUMENTAZIONE DI COMMESSA, SEGRETI TECNICI O COMMERCIALI, CONTENUTI COPERTI DA NDA, ELABORATI DEL CLIENTE O OPERE DI TERZI,

SALVO PREVENTIVA VERIFICA DELLA BASE GIURIDICA, DEI DIRITTI DI UTILIZZO E SPECIFICA AUTORIZZAZIONE SECONDO LA PMOG 16 E LA POLITICA IA.

Verifica preventiva degli input: prima di utilizzare testi, immagini, codice, dataset o documentazione di terzi come prompt, allegato o materiale di riferimento, l'utente deve verificare la legittima disponibilità del contenuto, l'ambito della licenza, le eventuali riserve di text and data mining e gli obblighi di attribuzione.

Verifica degli output: gli output dell'IA non si presumono liberi da diritti di terzi. Prima dell'utilizzo esterno o dell'integrazione nel software, devono essere controllati originalità, fonti, licenze, segni distintivi, eventuali dati personali e possibili somiglianze sostanziali con opere protette.

Codice generato con IA: il codice deve essere sottoposto a code review, test funzionali e di sicurezza, analisi delle dipendenze e verifica delle licenze. È vietata l'integrazione automatica in ambienti di produzione o in sistemi del cliente senza validazione e approvazione del responsabile tecnico.

Tracciabilità: per gli utilizzi rilevanti devono essere conservati, secondo la PMOG 16, l'identità dell'utente, lo strumento autorizzato, la finalità, la classificazione dei dati, i prompt e gli output pertinenti, l'esito delle verifiche e il nominativo del validatore umano, nel rispetto dei principi di minimizzazione e sicurezza.

Attribuzione e trasparenza: ove richiesto dalla legge, dal contratto, dalla licenza o dalla natura dell'elaborato, devono essere indicati l'autore, la fonte, la licenza e l'eventuale impiego significativo di sistemi di IA. È vietato attribuire a una persona fisica un contenuto che essa non abbia validato o approvato.

3 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 BITCONTROL partecipi a procedure di affidamento di contratti pubblici aventi ad oggetto sviluppo software, telecontrollo, automazione, integrazione di sistemi, assistenza o manutenzione, il RCOM/APVG e il RSCM devono coordinarsi con il Responsabile IA e con il responsabile tecnico per garantire la veridicità delle dichiarazioni sull'eventuale impiego di sistemi di IA, la prevalenza del lavoro intellettuale umano, la validazione degli output e la conservazione delle evidenze previste dalla PMOG 16.

In particolare:

IN SEDE DI PRESENTAZIONE DELL'OFFERTA LA SOCIETÀ DOVRÀ DICHIARARE:

"BITCONTROL 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, BITCONTROL 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."*

4 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:

1. 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 BITCONTROL 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;
2. 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.

BITCONTROL garantisce che i software, le librerie, i componenti, le banche dati e gli altri contenuti di terzi utilizzati per le attività aziendali siano identificati, autorizzati e corredati da licenze valide e compatibili con l'uso previsto; i relativi pagamenti, rinnovi e condizioni d'uso sono sottoposti a 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

Gestione delle anomalie: sospetti di plagio, violazioni di licenza, uso di strumenti non autorizzati, scraping anomalo, divulgazione di segreti, output ingannevoli o deepfake devono essere immediatamente sospesi, segregati e segnalati secondo la PMOG 16, la procedura incidenti e la procedura whistleblowing.

Controlli a campione: il Responsabile IA, il Responsabile IT e i responsabili tecnici possono effettuare controlli documentati su prompt, output, repository, dipendenze, licenze, fonti e materiali pubblicati, nel rispetto della normativa lavoristica e privacy.

Supplier due diligence: prima dell'acquisto o dell'adozione di piattaforme IA, software, dataset o contenuti di terzi sono verificati condizioni contrattuali, titolarità, sicurezza, trattamento dei dati, facoltà di riuso degli input/output e compatibilità con gli obblighi verso i clienti.

Registro delle licenze e dei componenti: il Responsabile IT/Responsabile IA, con il supporto dei responsabili tecnici, mantiene evidenza dei principali software, librerie, dataset, banche dati e strumenti IA autorizzati, delle relative licenze e delle scadenze.

5 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)

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.

6 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:

1. qualsiasi violazione ai principi di comportamento adottati;
2. qualsiasi situazione non conforme alla normativa;
3. qualsiasi utilizzo di opere, software, banche dati, codice o output IA in assenza di licenza, autorizzazione o validazione;
4. qualsiasi sospetto di plagio, scraping abusivo, violazione di licenze open source, diffusione di deepfake, perdita di riservatezza o contestazione da parte di titolari di diritti;
5. gli esiti rilevanti degli audit periodici, le revoche o sospensioni di strumenti IA e gli incidenti che abbiano determinato o possano determinare un rischio ai sensi del D.Lgs. 231/2001
6. 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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev.0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
REV.6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

SOMMARIO

Sommario

1 OBIETTIVI DELLA PROCEDURA

La presente procedura definisce i ruoli, le responsabilità operative, le attività di controllo e i principi di comportamento adottati dalla BITCONTROL S.r.l. nell'ambito del procedimento di richiesta di finanziamenti e di autorizzazioni, permessi e licenze ad Enti e Istituzioni Pubbliche, al fine di regolare il flusso e le responsabilità che si possono delineare all'interno di ciascuna Funzione coinvolta, nonché di garantire, relativamente ai finanziamenti e contributi assimilabili ad essi, la più facile individuazione di opportunità e il corretto utilizzo degli stessi in fase di gestione del finanziamento.

La procedura disciplina anche la fase di individuazione delle opportunità, la verifica preventiva dei requisiti di ammissibilità, la presentazione dell'istanza, la gestione del provvedimento, l'impiego delle risorse, la rendicontazione, il monitoraggio degli obblighi successivi e l'eventuale restituzione o revoca delle somme. Essa è coordinata con il Modello 231, il Codice Etico, il Codice di Condotta, la Politica Anticorruzione, la Policy IA, la Procedura Whistleblowing, le procedure di tesoreria, acquisti, gare, gestione delle commesse, sicurezza delle informazioni e archiviazione documentale di BITCONTROL.

Per BITCONTROL le attività rilevanti comprendono, in particolare, richieste di contributi e incentivi per investimenti, ricerca, innovazione, digitalizzazione, cybersecurity, formazione, internazionalizzazione ed efficientamento; autorizzazioni o nulla osta connessi a sedi, cantieri, installazioni, impianti, accessi a infrastrutture dei clienti, utilizzo di frequenze o connettività, trattamento e sicurezza dei dati, nonché licenze o autorizzazioni necessarie all'esecuzione di commesse di telecontrollo, automazione industriale, SCADA, PLC, RTU, DCS e IoT.

Per le operazioni relative alle attività inerenti la richiesta di autorizzazioni, licenze o altri provvedimenti amministrativi o l'esecuzione di adempimenti verso la Pubblica Amministrazione (es. richiesta di autorizzazione all'immissione in commercio), i protocolli prevedono:

• procedure per la gestione delle richieste di autorizzazioni, licenze o altri provvedimenti amministrativi o l'esecuzione di adempimenti verso la Pubblica Amministrazione;

• che i poteri autorizzativi e/o negoziali esercitati dai soggetti nei confronti della Pubblica Amministrazione devono essere individuati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal responsabile della struttura di riferimento, tramite delega interna; nel caso in cui i rapporti con la Pubblica Amministrazione vengano intrattenuti da soggetti terzi quest'ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali;

• segregazione di funzioni tra chi predispone la documentazione necessaria per la richiesta di un'autorizzazione/licenza, chi la controlla e chi sottoscrive la richiesta; all'uopo, i contratti con agenti o intermediari coinvolti in attività verso la Pubblica Amministrazione devono essere stipulati per iscritto, con indicazione di compensi proporzionati alla prestazione, e devono contenere clausole

anticorruzione; i pagamenti devono essere effettuati su conti correnti tracciabili, intestati al beneficiario effettivo. Dunque, nei rapporti con la Pubblica Amministrazione devono essere rispettati gli obblighi di verifica preventiva sull'identità e sulla regolarità della controparte, sul beneficiario effettivo e sulla coerenza tra documentazione presentata e flussi finanziari o operativi connessi all'autorizzazione richiesta.

• 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'

a di autorizzazione o forniti in esecuzione degli adempimenti prevedendo specifici controlli in contraddittorio; in particolare, prima della presentazione di qualsiasi istanza, richiesta di finanziamento, autorizzazione o licenza alla Pubblica Amministrazione, devono essere obbligatoriamente effettuati i seguenti controlli aggiuntivi rispetto a quelli già previsti dalla presente procedura:

i) Screening misure restrittive UE: verifica che la controparte, il beneficiario effettivo e il Paese destinatario non siano soggetti a misure restrittive dell'Unione Europea; in caso di dubbio, l'operazione deve essere sospesa e sottoposta a escalation al Responsabile amministrativo/legale e all'Organismo di Vigilanza;

ii) Verifica regolarità soggiorno e titolo di lavoro: nelle richieste che implicano l'impiego di personale straniero, verifica della regolarità del titolo di soggiorno e del permesso di lavoro, con conservazione delle evidenze documentali;

iii) Verifica compliance ambientale: nelle richieste con potenziale impatto ambientale (gestione rifiuti, immissioni, emissioni, attività soggette ad AIA o VIA), verifica del rispetto della normativa ambientale vigente e delle nuove fattispecie introdotte dal D.Lgs. n. 81/2026;

iv) Verifica compliance lavoro agile: nelle richieste che coinvolgono prestazioni in modalità agile, verifica del rispetto degli obblighi rafforzati del datore di lavoro previsti dalla Legge n. 34/2026, inclusi la consegna dell'informativa sui rischi, la sottoscrizione degli accordi individuali e del regolamento aziendale sul lavoro agile;

v) Verifica utilizzo IA: nelle richieste, offerte o documentazioni di gara predisposte con il supporto di strumenti di Intelligenza Artificiale, verifica del rispetto della Policy IA aziendale, effettuazione della dichiarazione sull'utilizzo di IA ove richiesta dalla Delibera ANAC n. 148/01.04.2026, validazione umana degli output generati e conservazione delle relative evidenze.

Tutti i controlli sopra indicati devono essere documentati e conservati agli atti unitamente alla documentazione relativa alla richiesta.

- Qualora nella predisposizione di istanze, richieste di autorizzazioni, licenze, finanziamenti,

offerte in procedure di gara o altra documentazione destinata alla Pubblica Amministrazione siano utilizzati strumenti di Intelligenza Artificiale, si applicano le seguenti regole:

a) è consentito esclusivamente l'utilizzo degli strumenti di IA approvati dalla Società secondo la Policy IA vigente; è vietato l'uso di strumenti non approvati o di account personali per finalità aziendali;
b) prima dell'utilizzo di qualsiasi strumento di IA nella predisposizione della documentazione, deve essere verificata e documentata l'autorizzazione scritta del Responsabile IT;
c) è vietato inserire in strumenti di IA dati personali non anonimizzati, dati appartenenti a categorie particolari ai sensi dell'art. 9 GDPR, informazioni riservate o confidenziali, codice sorgente, credenziali, dati economici non pubblici, documentazione contrattuale riservata o qualsiasi altra informazione classificata come riservata secondo la classificazione aziendale;
d) ogni output generato da un sistema di IA deve essere validato da una persona autorizzata prima di essere trasmesso alla Pubblica Amministrazione, sottoscritto o depositato; l'IA non può sostituire il giudizio umano né essere utilizzata per generare autonomamente documenti ufficiali, dichiarazioni vincolanti o comunicazioni istituzionali prive di revisione umana; la responsabilità giuridica, tecnica e professionale dei contenuti rimane integralmente in capo all'operatore economico;
e) nelle procedure di gara o affidamento, deve essere resa la dichiarazione sull'eventuale utilizzo di sistemi di IA nella predisposizione dell'offerta e della documentazione, in conformità alla Delibera ANAC n. 148/01.04.2026 e all'art. 13 della Legge 132/2025;
f) devono essere assicurati logging, tracciabilità dei prompt e degli output rilevanti, conservazione documentale, con indicazione del soggetto che ha utilizzato lo strumento, del tipo di strumento impiegato, degli input forniti, degli output ottenuti, della validazione umana effettuata e della data;
g) per i trattamenti ad alto rischio ai sensi del Regolamento UE 2024/1689 (AI Act) e del GDPR, deve essere effettuata una valutazione preventiva d'impatto (DPIA), in coordinamento con il DPO;
h) qualsiasi anomalia, uso improprio o incidente connesso all'utilizzo di strumenti di IA nella predisposizione di documentazione verso la Pubblica Amministrazione deve essere segnalato immediatamente al Responsabile Sicurezza Informatica e, ove coinvolti dati personali, al DPO;

- tracciabilità del processo sia a livello di sistema informatico sia in termini documentali e conservazione della documentazione prodotta da parte della struttura di competenza presso l'archivio della struttura medesima;
- 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;
- verifica attraverso appositi scadenzari delle autorizzazioni/licenze ottenute al fine di richiedere il rinnovo delle stesse nel rispetto dei termini di legge. Nell'ambito del monitoraggio delle autorizzazioni e delle licenze in essere, deve essere effettuata una verifica periodica della permanenza dei presupposti che hanno portato al rilascio del titolo abilitativo, con particolare attenzione a eventuali

modifiche delle misure restrittive UE applicabili, a variazioni nelle condizioni di regolarità del soggiorno del personale straniero coinvolto, a modifiche della normativa ambientale applicabile alle attività autorizzate e a eventuali nuovi obblighi imposti dall'AI Act o dalla normativa nazionale sull'IA.

La presente procedura è stata altresì aggiornata per recepire le seguenti novità normative e organizzative intervenute successivamente:

– il D.Lgs. n. 211/2025, entrato in vigore il 24.01.2026, che recepisce la Direttiva (UE) 2024/1226 e introduce nel catalogo dei reati presupposto del D.Lgs. 231/2001 fattispecie relative alla violazione delle misure restrittive dell'Unione Europea, rilevanti nei processi di richiesta di autorizzazioni, licenze, finanziamenti e nei rapporti con controparti estere o soggetti designati;

– il D.Lgs. n. 83/16.04.2026, che recepisce la Direttiva UE 2024/1233 e modifica l'art. 22 del T.U. Immigrazione (D.Lgs. 286/98), con riflessi sull'art. 25-duodecies D.Lgs. 231/2001 in materia di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, rilevante nelle autorizzazioni e licenze che implicano l'impiego di personale straniero;

– la Legge n. 34/11.03.2026, che rafforza gli obblighi del datore di lavoro in materia di salute e sicurezza anche nel lavoro agile, con implicazioni sull'art. 25-septies D.Lgs. 231/2001, rilevante nelle autorizzazioni che coinvolgono prestazioni in modalità agile;

– il D.Lgs. n. 81/21.04.2026, che attua la Direttiva UE 2024/1203 e amplia il catalogo dei reati ambientali presupposto di cui all'art. 25-undecies D.Lgs. 231/2001, rilevante nelle autorizzazioni e licenze con potenziale impatto ambientale;

– la Delibera ANAC n. 148/01.04.2026, che impone obblighi di trasparenza e dichiarazione sull'utilizzo di sistemi di Intelligenza Artificiale nelle procedure di gara e di affidamento;

– il Codice Etico, il Codice di Condotta, la Policy sull'Intelligenza Artificiale e la Procedura Whistleblowing, adottati o aggiornati con delibera dell'Organo Amministrativo del 27.07.2026, quali presidi integrativi del Modello 231 applicabili anche ai processi disciplinati dalla presente procedura.

2 ACRONOMI 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
RIA	Responsabile IA
RCA	Responsabile interno conformità anticorruzione

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

3 RIFERIMENTI NORMATIVI DEL MODELLO

- CODICE ETICO DI BITCONTROL S.R.L.;
- CODICE DISCIPLINARE DI BITCONTROL S.R.L.
- MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO DI BITCONTROL S.R.L..
- D.LGS. 30 DICEMBRE 2025, N. 211, IN MATERIA DI VIOLAZIONE DELLE MISURE RESTRITTIVE DELL'UNIONE EUROPEA;
- D.LGS. 21 APRILE 2026, N. 81, IN MATERIA DI TUTELA PENALE DELL'AMBIENTE;
- LEGGE N. 34/2026 AGGIORNAMENTO REATI IN MATERIA DI SICUREZZA SUL LAVORO.
- D.LGS. 16 APRILE 2026, N. 83, IN MATERIA DI PERMESSO UNICO DI SOGGIORNO E LAVORO PER CITTADINI DI PAESI TERZI;
- REGOLAMENTO (UE) 2024/1689 E LEGGE 23 SETTEMBRE 2025, N. 132, IN MATERIA DI INTELLIGENZA ARTIFICIALE;
- D.LGS. 10 MARZO 2023, N. 24, IN MATERIA DI WHISTLEBLOWING;
- D.P.R. 28 DICEMBRE 2000, N. 445, CODICE DELL'AMMINISTRAZIONE DIGITALE E NORMATIVA APPLICABILE IN MATERIA DI DOCUMENTI, DICHIARAZIONI E ISTANZE TELEMATICHE;
- NORMATIVA UE E NAZIONALE APPLICABILE AI FONDI PUBBLICI, AIUTI DI STATO, PNRR/PNC, DIVIETO DI DOPPIO FINANZIAMENTO, TRACCIABILITÀ E RENDICONTAZIONE, OVE APPLICABILE.

4 INDICAZIONI COMPORTAMENTALI

I *Destinatari* che, per ragione del proprio incarico o della propria Funzione, siano coinvolti nella richiesta e gestione di finanziamenti pubblici, autorizzazioni, permessi e licenze devono, in particolare:

- garantire la veridicità delle dichiarazioni rese a organismi pubblici nazionali o comunitari per ottenere erogazioni, contributi o finanziamenti e rilasciare apposito rendiconto nel caso in cui i medesimi vengano ottenuti;
- destinare le somme ricevute da organismi pubblici nazionali o stranieri a titolo di contributo, sovvenzione o finanziamento per le finalità per le quali sono stati erogate;

- garantire che la documentazione di rendicontazione delle somme spese sia puntualmente redatta e debitamente archiviata.

AI DESTINATARI È, INOLTRE, FATTO ESPRESSO DIVIETO DI:

- autorizzare, sollecitare, offrire, promettere di concedere, direttamente o indirettamente, pagamenti o oggetti di valore a funzionari pubblici con l'intento di persuadere e/o influenzare detti funzionari ad agire secondo modalità che consentirebbero alla Società di ottenere, promuovere e mantenere le proprie attività, nonché assicurarsi vantaggi illegittimi o indebiti nello svolgimento delle stesse. Parimenti, i *Destinatari* sono tenuti a segnalare qualsiasi tentativo di estorsione o concussione da parte di un pubblico ufficiale, e ciò sia nel caso in cui dovessero essere i destinatari, sia nel caso in cui dovessero venirne a conoscenza;
- offrire o corrispondere a soggetti operanti nella P.A. (o a soggetti loro congiunti, affini, conviventi o ad essi in qualche modo collegati), 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;
- rivolgersi a soggetti che sfruttano o vantano relazioni esistenti e/o asserite con pubblici ufficiali e incaricati di pubblico servizio, consegnando o promettendo loro denaro quale prezzo per la propria mediazione illecita nei confronti di detti soggetti operanti nella P.A. o per la remunerazione degli stessi in relazione alle loro funzioni e ai loro poteri;
- nella scelta dei *partners* di gara avviare rapporti con soggetti dei quali sia 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;
- 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 operatore economico, al fine di indurlo ad agire o ad astenersi dall'agire in violazione dei suoi doveri.

NEI RAPPORTI CON LA P.A. E GLI ORGANISMI DI CONTROLLO SONO, INOLTRE, VIETATI I SEGUENTI COMPORTAMENTI:

- la tenuta di condotte che possano indurre i rappresentanti della P.A. o delle Autorità di vigilanza a favorire l'indebito rilascio di agevolazioni, contributi, atti autorizzativi, certificazioni, visti, nulla osta, *etc.*;
- la presentazione di documentazione mendace, la rappresentazione non veritiera ovvero l'omissione di fatti e circostanze atti ad influenzare il processo decisionale;
- esaminare, proporre o paventare opportunità commerciali che possano, direttamente o indirettamente, avvantaggiare i dipendenti della P.A., delle Istituzioni e delle Autorità;
- tentare di influenzare le decisioni delle parti;
- offrire, promettere o accettare qualsiasi tipo di oggetto, servizio e/o prestazione;

- sollecitare o ottenere, fuori dai casi prescritti dalla legge, informazioni riservate;
- conferire incarichi a soggetti nei confronti dei quali si possa determinare un conflitto di interessi;
- esporre nelle comunicazioni, nelle segnalazioni e nelle risposte a richiesta, fatti non corrispondenti al vero, nonchè occultare quelli veritieri, con mezzi fraudolenti in tutto o in parte;
- adottare nella predisposizione delle comunicazioni, delle segnalazioni e delle risposte di cui al punto precedente i princìpi di completezza, integrità, oggettività e trasparenza.

Ancora, a seguito delle nuove disposizioni recepite dalla Società, si precisa che:

- i Destinatari devono conformarsi, oltre che alla normativa vigente e al Modello 231, ai principi di legalità, integrità, correttezza, veridicità, tracciabilità, trasparenza, riservatezza, diligenza professionale e prevenzione dei conflitti di interesse sanciti dal Codice Etico e dal Codice di Condotta aziendali.

- Solo i Destinatari espressamente autorizzati possono relazionarsi in nome e per conto di BitControl S.r.l. con le Autorità e la Pubblica Amministrazione. Ogni contatto rilevante con soggetti pubblici deve essere documentato e conservato secondo le procedure interne.

- È assolutamente vietato offrire, promettere o corrispondere, direttamente o attraverso intermediari, denaro, regali, utilità o altri vantaggi a pubblici ufficiali o incaricati di pubblico servizio, al fine di ottenere decisioni favorevoli, contratti, autorizzazioni, finanziamenti o trattamenti di privilegio.

- I Destinatari che ricevano proposte, sollecitazioni o pressioni corruttive da funzionari pubblici o da terzi sono tenuti a rifiutarle e a informare immediatamente il Consiglio di Amministrazione e l'Organismo di Vigilanza, mediante comunicazione scritta che descriva compiutamente i fatti. La mancata segnalazione costituisce autonoma violazione della presente procedura e del Codice di Condotta.

- È vietato falsificare, alterare o manipolare documenti, rendiconti, dichiarazioni, certificazioni o qualsiasi altra documentazione da presentare alla Pubblica Amministrazione o ad enti pubblici ai fini del rilascio di autorizzazioni, licenze, concessioni o finanziamenti.

- È vietato destinare contributi, sovvenzioni o finanziamenti pubblici a finalità diverse da quelle per le quali sono stati concessi, nonché alterare i rendiconti al fine di ottenere un indebito vantaggio.

- È vietato porre in essere condotte elusive delle misure restrittive dell'Unione Europea, inclusi il trasferimento a soggetti designati di fondi, beni o risorse, l'omissione di comunicazioni obbligatorie alle autorità competenti, lo svolgimento di attività non conforme alle prescrizioni delle autorizzazioni rilasciate e la falsificazione o alterazione di documenti doganali o di altra documentazione funzionale all'elusione dei controlli.

5 CAMPO DI APPLICAZIONE

La presente procedura si applica a tutti i Destinatari che si occupano della presentazione e della gestione di procedimenti relativi a richieste e/o autorizzazioni e/o concessioni nei confronti della P.A., e specificatamente:

1. richiesta e gestione di agevolazioni, contributi, finanziamenti pubblici, licenze, permessi e autorizzazioni;
2. avvio e gestione di procedimenti finalizzati ad accertare il valore catastale di immobili ai fini della determinazione delle relative imposte.
3. richieste e gestione di incentivi, crediti, contributi o finanziamenti per investimenti in hardware, software, cybersecurity, ricerca e sviluppo, innovazione, formazione, transizione digitale, energia e internazionalizzazione.
4. richieste di autorizzazioni, nulla osta, permessi, abilitazioni, iscrizioni, concessioni o adempimenti amministrativi necessari per sedi, cantieri, installazioni, infrastrutture tecnologiche, accessi a impianti, attività tecniche e commesse della Società;

Tenuto conto del core business della BITCONTROL S.r.l., i Destinatari sono obbligati ad attenersi ai principi ed alle procedure qui di seguito esposte, sia nell'ambito delle attività svolte nell'interesse della Società, sia con riferimento alle attività eseguite per conto e nell'interesse dei clienti della medesima Società.

6 RESPONSABILE DELLA PROCEDURA

Responsabile della presente procedura è l'Organo amministrativo.

7 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. i pagamenti verso Paesi terzi, giurisdizioni ad alto rischio o non cooperative, conti non riconducibili alla controparte o soggetti sottoposti a misure restrittive sono vietati, salvo preventiva verifica documentata della liceità, della ragione economica e dell'identità del beneficiario effettivo, nonché autorizzazione dell'Organo Amministrativo;
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.
10. deve essere utilizzato, ove previsto dal bando o ritenuto necessario, un conto dedicato o una codifica contabile analitica che consenta di separare e riconciliare entrate, anticipazioni, spese, rimborsi e restituzioni relative al progetto;
11. prima del pagamento devono essere verificati contratto o ordine, documento di spesa, prova della prestazione o consegna, ammissibilità della voce, corretta imputazione temporale, tracciabilità e assenza di conflitti di interesse;
12. anticipazioni, SAL, richieste di rimborso e rendiconti devono essere riconciliati con contabilità generale, estratti conto, registro cespiti, timesheet e fascicolo tecnico; eventuali scostamenti devono essere motivati e approvati;
13. eventuali economie, spese non ammissibili, revoche, decadenze o somme da restituire devono essere tempestivamente segnalate al PRES, al RAM/RRU e all'OdV e contabilizzate senza compensazioni non autorizzate.

Ancora, il D.L. 25 febbraio 2022 n. 13, pubblicato in GU n. 47 del 25 febbraio 2022, all'art 2 ha introdotto modifiche, di segno ampliativo, alla rubrica e al testo degli artt. 240-bis, 316-bis ("Malversazione di erogazioni pubbliche") e 316-ter ("Indebita percezione di erogazioni pubbliche") del codice penale, al fine di rafforzare il contrasto alle frodi in materia di erogazioni pubbliche, alla luce delle notizie di operazioni illecite che hanno riguardato le agevolazioni fiscali note come "superbonus".

IN PARTICOLARE:

- in ordine al reato di "Malversazione a danno dello Stato" (art. 316 bis c.p.), la novella legislativa, modificando la rubrica del reato in "Malversazione di erogazioni pubbliche", ha ampliato l'oggetto della condotta aggiungendo ai contributi, sovvenzioni e finanziamenti, i "mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate" e rendendo più generica la destinazione di tali erogazioni, non più necessariamente legata alla realizzazione di opere o allo svolgimento di attività di pubblico interesse.

Il delitto può essere commesso da chiunque, purché estraneo alla Pubblica Amministrazione.

Il soggetto attivo può essere solo chi, avendo ricevuto un finanziamento pubblico, non destina le somme percepite alle finalità indicate negli atti di erogazione dei finanziamenti. Soggetto passivo del delitto è l'Ente (Stato, altro ente pubblico, Unione Europea) che ha erogato il finanziamento.

Presupposto della condotta è costituito dall'avvenuto conseguimento di contributi, sovvenzioni o finanziamenti erogati dalla P.A. o dall'Unione Europea "destinati a favorire iniziative dirette alla realizzazione di opere od allo svolgimento di attività".

La nozione di finanziamento pubblico ricomprende tutti quei rapporti in cui la temporanea creazione di disponibilità finanziarie avviene per intervento diretto o indiretto dei pubblici poteri e per uno specifico fine, di volta in volta individuato.

I contributi sono costituiti dalla partecipazione alle spese per attività e iniziative finalizzate al raggiungimento di obiettivi promozionali e/o produttivi e possono essere in conto capitale e/o conto interessi.

Le sovvenzioni sono attribuzioni pecuniarie a fondo perduto (ossia senza obbligo di restituzione) e possono avere carattere periodico o una tantum, misura fissa o determinata in base a parametri variabili, natura vincolata all'an o al quantum o di pura discrezionalità.

I finanziamenti in senso stretto, infine, sono atti negoziali (operazioni di credito) con cui lo Stato o altro Ente finanzia, direttamente o per il tramite di un istituto di credito, un soggetto il quale, a sua volta, si obbliga a restituire la somma erogata a medio o lungo termine. I finanziamenti si caratterizzano per l'esistenza di un'obbligazione di destinazione delle somme ricevute al fine specifico preventivamente determinato, per l'esistenza di un'obbligazione di restituzione, nonché per l'esistenza di ulteriori e diversi altri oneri. Rientrano nel concetto di finanziamento anche tutti i c.d. crediti agevolati o finanziamenti a valere sul PNRR.

Il disvalore penale del comportamento vietato è il contegno di chi non destina le somme ricevute a titolo di contributi, sovvenzioni o finanziamenti alle finalità per cui sono state erogate, cioè alle opere da realizzare e/o alle attività da svolgere.

Pertanto, dall'analisi della fattispecie di reato emerge come è fatto espresso divieto a tutti i Destinatari di:

1. non porre in essere l'opera e/o il mancato svolgimento dell'attività oggetto del finanziamento;

2. omettere di destinare le somme erogate alle finalità sottostanti al finanziamento.

Nel caso in cui l'opera o l'attività sovvenzionata sia stata realizzata con un certo risparmio di spesa, la mancata restituzione delle somme risparmiate configura il reato in esame se il finanziamento è corredato

dall'obbligo del rendiconto finanziario. La sussistenza di tale obbligo, infatti, comporta che le somme erogate hanno un originario vincolo di destinazione anche quantitativo.

Si ritiene, in prevalenza, che non integri il reato in oggetto il fatto di chi, dopo aver avanzato una richiesta di finanziamento la cui approvazione tardi a venire, dia inizio alla realizzazione dell'opera od allo svolgimento dell'attività finanziandola con mezzi propri e, dopo aver ottenuto finalmente il finanziamento, lo utilizzi per reintegrare il proprio patrimonio.

Va da sé che, se l'opera è stata interamente realizzata ancor prima che sia stata avanzata la richiesta di finanziamento e l'agente abbia ingannevolmente prospettato all'ente erogatore di voler richiedere un finanziamento per un'opera o attività ancora da realizzare, si profilerà il delitto di truffa aggravata per il conseguimento di erogazioni pubbliche.

Il reato è punibile a titolo di dolo generico e consiste nella consapevolezza in chi agisce di essere estraneo alla P.A. e di utilizzare un contributo, una sovvenzione o un finanziamento proveniente dallo Stato, da un ente pubblico e dall'Unione Europea diretto a consentire la realizzazione di opere o attività, nonché di non destinare le somme ricevute allo scopo anzidetto.

Il reato in esame si consuma nel momento in cui l'agente, non avendo realizzato compiutamente l'opera o l'attività prevista nell'atto di erogazione, destina le somme ad altra finalità.

- in ordine al reato di "Indebita percezione di erogazioni pubbliche" (art 316 ter c.p.) del codice penale, al fine di rafforzare il contrasto alle frodi in materia di erogazioni pubbliche, alla luce delle notizie di operazioni illecite che hanno riguardato le agevolazioni fiscali note come "superbonus".

In forza della clausola di sussidiarietà espressa contenuta nell'inciso iniziale, l'art. 316-ter è applicabile solo se la fattispecie concreta non ricade già sotto la previsione normativa dell'art. 640-bis c.p. (Truffa a danno dello Stato o di un altro ente pubblico). L'art. 316 ter contempla un reato che può essere consumato non già da chiunque indistintamente ma solo da chi cerca di conseguire l'erogazione pubblica con la condotta descritta nella fattispecie in esame. Il soggetto passivo è lo Stato, gli altri enti pubblici e la Comunità europea. La condotta punibile può manifestarsi tanto nella forma commissiva che omissiva. La prima modalità comportamentale si esplica nell'utilizzo o nella presentazione di dichiarazioni o documenti falsi, cui consegua la percezione difondi provenienti dal bilancio dello Stato, di altri enti pubblici e dell'Unione Europea. La seconda, invece, riguarda il caso della mancata comunicazione di un dato o di una notizia in violazione di uno specifico obbligo di informazione, cui consegua lo stesso effetto dell'indebita percezione delle erogazioni. Come si desume dal testo della norma, la condotta menzognera è assimilabile a quella della mancata comunicazione di rilevanti elementi di fatto che, se conosciuti, avrebbero impedito l'erogazione dei contributi. L'oggetto materiale della frode è rappresentato da ogni

attribuzione economica agevolata erogata dallo Stato, da altri enti pubblici o dall'Unione Europea. Essa può avere carattere di liberalità (ad es. contributi a fondo perduto), può essere a titolo gratuito ossia comportare un mero obbligo di restituzione senza interessi e, infine, a titolo oneroso e cioè comportare l'obbligo di restituzione e corresponsione, da parte del beneficiario, di interessi ridotti.

Con il termine contributi si intende qualsiasi erogazione in conto capitale e/o interessi finalizzata al raggiungimento di obiettivi promozionali e/o produttivi. La nozione di finanziamenti evoca l'erogazione dei mezzi finanziari che occorrono allo svolgimento di una determinata attività. In particolare, sono atti negoziali (operazioni di credito) caratterizzati dall'obbligo di destinazione delle somme o di restituzione o da ulteriori e diversi oneri; essi hanno rilevanza qualunque sia la finalità che li ha ispirati. I mutui agevolati costituiscono l'erogazione di una somma di denaro a favore di un soggetto con l'obbligo per quest'ultimo di restituire il tantundem maggiorato di interessi in misura inferiore a quella di mercato. Infine, con l'espressione altre erogazioni dello stesso tipo il legislatore ha inteso ricorrere ad una formula di chiusura per poter ricomprendere qualsiasi possibile forma di attribuzione comunque agevolata di risorse Pubbliche o comunitarie. La fattispecie prevista dall'art. 316 ter è punibile solo a titolo di dolo: la presentazione di dichiarazioni non veritiere determinata solo da negligenza o leggerezza potrà assumere rilevanza come causa di decadenza del finanziamento agevolato ma non potrà mai assumere rilevanza penale. Il reato si realizza nel momento e nel luogo in cui l'agente effettivamente consegue l'indebita percezione.

Prima dell'utilizzo di risorse finanziarie legate a finanziamenti, contributi, sovvenzioni o incentivi pubblici, deve essere effettuato uno screening preventivo volto a verificare che la controparte, il beneficiario effettivo, il Paese di destinazione e le modalità operative non siano soggetti a misure restrittive dell'Unione Europea, conformemente alle fattispecie introdotte dagli artt. 275-bis e seguenti c.p. (D.Lgs. n. 211/2025).

Le verifiche effettuate, le autorizzazioni rilasciate e le eventuali sospensioni e decisioni assunte in applicazione della normativa sulle misure restrittive UE devono essere tracciate e conservate agli atti, in modo da consentire la ricostruzione del processo decisionale e dei soggetti intervenuti.

In caso di richiesta di autorizzazione allo svolgimento di attività in deroga a misure restrittive (ai sensi dell'art. 275-quater c.p.), l'operazione deve essere preliminarmente sottoposta all'approvazione dell'Organo Amministrativo e dell'Ufficio Legale, con tempestiva comunicazione all'Organismo di Vigilanza.

8. PRESIDI SPECIFICI

Al fine di prevenire i reati di cui agli artt. 24 e 25 del D.Lgs. 231/2001, BitControl adotta inoltre i seguenti presidi:

1. divieto assoluto di presentare dichiarazioni, attestazioni o documentazione non veritiera;
2. obbligo di doppia verifica di tutte le dichiarazioni sostitutive rese ai sensi del D.P.R. n. 445/2000;
3. verifica preventiva dei requisiti soggettivi e oggettivi richiesti dal bando;
4. controllo sull'assenza di situazioni di incompatibilità, conflitto di interessi o pantouflage;
5. tracciabilità integrale dei flussi finanziari e documentali;
6. divieto di utilizzo delle somme finanziate per finalità diverse da quelle autorizzate;
7. obbligo di immediata comunicazione all'Ente finanziatore di variazioni rilevanti, rinunce, revoche, 8.
8. sospensioni o eventi incidenti sull'esecuzione del progetto;
9. tempestiva segnalazione all'Organismo di Vigilanza, anche tramite il canale di whistleblowing, di qualsiasi anomalia, irregolarità o richiesta indebita proveniente da pubblici ufficiali o incaricati di pubblico servizio.

9 ARCHIVIAZIONE DELLA DOCUMENTAZIONE

Tutta la documentazione prodotta nell'ambito del procedimento, dovrà essere trasmessa dalla Funzione interessata al RGAD, che ne curerà l'archiviazione nella piattaforma digitale all'uopo predisposta nell'apposita piattaforma informatica, così da consentire in qualunque momento un controllo da parte dell'OdV.

Il sistema di archiviazione documentale deve garantire la conservazione, la completezza, l'integrità e la non alterabilità di tutta la documentazione relativa alle richieste, autorizzazioni e licenze, incluse le evidenze dei controlli preventivi effettuati, delle verifiche sulle misure restrittive UE, delle verifiche di compliance ambientale, lavoristica e in materia di regolarità del soggiorno, nonché dei log relativi all'utilizzo di strumenti di IA nella predisposizione delle istanze.

I documenti e le evidenze sopra indicati devono essere conservati per il periodo di tempo previsto dalla normativa applicabile e, in ogni caso, per un periodo non inferiore a 5 anni, in coerenza con gli obblighi di conservazione previsti dalla Procedura Whistleblowing.

In caso di trattamento di dati personali nell'ambito dei processi disciplinati dalla presente procedura, devono essere rispettati gli obblighi del Regolamento UE 2016/679 (GDPR), inclusi gli obblighi di minimizzazione dei dati, di limitazione della conservazione e di sicurezza dei trattamenti.

10 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutti i *Destinatari* coinvolti nelle attività oggetto della presente procedura informano tempestivamente l'Organismo di Vigilanza di situazioni anomale e/o in contrasto con quanto disposto nel Modello, nonché 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.

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.

Devono essere altresì tempestivamente comunicati all'Organismo di Vigilanza:

– operazioni sospese, bloccate o sottoposte a escalation per rischio di collegamento con soggetti sanzionati, misure restrittive dell'Unione Europea, anomalie documentali o possibile elusione della normativa applicabile;

– richieste di autorizzazioni, licenze o finanziamenti nelle quali siano stati riscontrati profili di rischio connessi alla regolarità del soggiorno del personale straniero coinvolto, alla compliance ambientale o alla sicurezza sul lavoro in modalità agile;

- utilizzo di strumenti di IA nella predisposizione di istanze, offerte in gara o documentazione verso la Pubblica Amministrazione, con indicazione delle finalità, degli strumenti autorizzati impiegati, delle dichiarazioni sull'uso dell'IA rese in documentazione di gara, dei controlli svolti sugli output e delle eventuali criticità riscontrate;

– anomalie o incidenti informatici che coinvolgano strumenti digitali o di IA impiegati nei processi disciplinati dalla presente procedura;

– segnalazioni whistleblowing ricevute aventi ad oggetto fatti rilevanti per i processi di richiesta di autorizzazioni, licenze e finanziamenti pubblici;

- variazioni dei soggetti autorizzati a presentare istanze alla Pubblica Amministrazione.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA del 14.11.2020	ADOZIONE
Rev. 1	CDA del 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA del 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA del 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA del 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA del 13.11.2023	AGGIORNAMENTO
Rev 6	CDA dell'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA del 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA del 27.07.2026	AGGIORNAMENTO

SOMMARIO

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 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.);
- 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);
– obblighi di tracciabilità dei rifiuti mediante il Registro elettronico nazionale per la tracciabilità dei rifiuti (RENTRI), registri cronologici e formulari di identificazione, secondo gli artt. 188-bis, 190, 193 e 258 del D.Lgs. 152/2006 e il D.M. 4 aprile 2023, n. 59;
– spedizioni illegali di rifiuti ai sensi della disciplina vigente, incluso il Regolamento (UE) 2024/1157, applicabile dal 21 maggio 2026, ferme le disposizioni transitorie;
– impedimento del controllo (art. 452-septies c.p.) e ulteriori fattispecie ambientali ricomprese nell'art. 25-undecies del D.Lgs. 231/2001 nella formulazione vigente;
– 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).

Si richiamano altresì le modifiche introdotte dal D.Lgs. n. 81 del 21 aprile 2026, attuativo della Direttiva UE 2024/1203, che ha modificato in modo significativo l'art. 25-undecies del D.Lgs. 231/2001, ampliando il catalogo dei reati presupposto ambientali e aumentando le sanzioni applicabili agli enti.

La presente Procedura si coordina inoltre con il Codice Etico, il Codice di Condotta, la Policy IA e la Procedura Whistleblowing vigente, quali presidi integrativi del Modello 231 rilevanti anche ai fini della prevenzione dei reati ambientali.

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 BITCONTROL 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.

Nello specifico, BitControl ha provveduto a fare:

– l'aggiornamento dei protocolli interni al fine di prevenire le nuove fattispecie di reato introdotte dal D.Lgs. n. 81/2026, incluse le condotte di commercio di prodotti inquinanti, le ipotesi di abusività estesa, le aggravanti da profitto rilevante o da uso di documentazione falsa e le ipotesi aggravate in materia di gestione dei rifiuti;

– il coordinamento della presente Procedura con la Policy IA aziendale, per disciplinare l'utilizzo di strumenti di Intelligenza Artificiale nei processi che possano incidere sul monitoraggio ambientale, sulla reportistica tecnica, sulla gestione documentale o sulla partecipazione a gare;

– il coordinamento con la Procedura Whistleblowing Rev. 8, quale canale interno di segnalazione delle violazioni ambientali, dei rischi ambientali, delle anomalie documentali e delle condotte idonee a integrare reati presupposto ai sensi del D.Lgs. 231/2001;

– l'aggiornamento della mappatura dei ruoli sensibili anche in relazione alle nuove assunzioni formalizzate dal 01.04.2026 e alla formazione aziendale svolta in materia di IA in data 23.03.2026;

– l'integrazione dei flussi informativi verso l'Organismo di Vigilanza e dei controlli documentali anche con riferimento ai presidi di tracciabilità, supervisione umana e conservazione degli output generati da strumenti di IA.

Dunque, in considerazione dell'analisi dei rischi effettuata, BITCONTROL 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) COME MODIFICATO DALL' ART.4 DEL D.LGS.N.116 DEL 3 SETTEMBRE 2020, DAL DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E DALLA LEGGE N.147 DEL 3 OTTOBRE 2025)

Tale ipotesi di reato, nella versione originaria, prevedeva di punire 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.

Orbene, con le modifiche normative apportate dal 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.

Inoltre, 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.

Ciò posto, per una migliore comprensione delle ipotesi di reato, si riporta il testo modificato dell'Art. 258 D. Lgs. n. 152/2006:

[I]. 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

[II]. 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.

[II-bis]. 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.

[III]. 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.

[IV]. 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.

[IV-bis]. 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.

[V]. 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.

[VI]. 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.

[VII]. 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.

[VIII]. 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.

[IX]. 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.

[IX-bis]. 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.

[X]. 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.

[XI]. 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.

[XII]. 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.

[XIII]. 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.

• ATTIVITÀ ORGANIZZATE PER IL TRAFFICO ILLECITO DI RIFIUTI (ART. 452-QUATERDECIES C.P.)

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.

TRAFFICO E ABBANDONO DI MATERIALE AD ALTA RADIOATTIVITÀ (ART. 452 SEXIES CODICE PENALE)

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)

Tale reato previsto dall'Art. 452- septies si realizza 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.

Sul punto, 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.

*

Per una completa comprensione della riforma normativa, si riportano i reati la cui commissione, tuttavia, si ritiene remota e/o non ipotizzabile, e precisamente:

a) UCCISIONE, DISTRUZIONE, CATTURA, PRELIEVO, DETENZIONE DI ESEMPLARI DI SPECIE ANIMALI O VEGETALI SELVATICHE PROTETTE (ART. 727-BIS C.P.)

"1. Salvo che il fatto costituisca più grave reato, chiunque, fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie animale selvatica protetta è punito con l'arresto da uno a sei mesi o con l'ammenda fino a 4.000 euro, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie. 2. Chiunque, fuori dai casi consentiti, distrugge, preleva o detiene esemplari appartenenti ad una specie vegetale selvatica protetta è punito con l'ammenda fino a 4.000 euro, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie."

b) 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 (ART. 137 D.LGS. 152/2006)

"*1. Chiunque apra o comunque effettui nuovi scarichi di acque reflue industriali, senza autorizzazione, oppure continui ad effettuare o mantenere detti scarichi dopo che l'autorizzazione sia stata sospesa o revocata, è punito con l'arresto da due mesi a due anni o con l'ammenda da millecinquecento euro a diecimila euro. 2. Quando le condotte descritte al comma 1 riguardano gli scarichi di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto, la pena è dell'arresto da tre mesi a tre anni. 3. Chiunque, al di fuori delle ipotesi di cui al comma 5, effettui uno scarico di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto senza osservare le prescrizioni dell'autorizzazione, o le altre prescrizioni dell'autorità competente a norma degli articoli 107, comma 1, e 108, comma 4, è punito con l'arresto fino a due anni. (omissis)5. Chiunque, in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza del presente decreto, nell'effettuazione di uno scarico di acque reflue industriali, superi i valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5 alla parte terza del presente decreto, oppure i limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente a norma dell'articolo 107, comma 1, è punito con l'arresto fino a due anni e con l'ammenda da tremila euro a trentamila euro. Se sono superati anche i valori limite fissati per le sostanze contenute nella tabella 3/A del medesimo Allegato 5, si applica l'arresto da sei mesi a tre anni e l'ammenda da seimila euro a centoventimila euro (430). 6. Le sanzioni di cui al comma 5 si applicano altresì al gestore di impianti di trattamento*

delle acque reflue urbane che nell'effettuazione dello scarico supera i valori-limite previsti dallo stesso comma. (omissis) 11. Chiunque non osservi i divieti di scarico previsti dagli articoli 103 e 104 è punito con l'arresto sino a tre anni. (omissis) 13. Si applica sempre la pena dell'arresto da due mesi a due anni se lo scarico nelle acque del mare da parte di navi od aeromobili contiene sostanze o materiali per i quali è imposto il divieto assoluto di sversamento ai sensi delle disposizioni contenute nelle convenzioni internazionali vigenti in materia e ratificate dall'Italia, salvo che siano in quantità tali da essere resi rapidamente innocui dai processi fisici, chimici e biologici, che si verificano naturalmente in mare e purché in presenza di preventiva autorizzazione da parte dell'autorità competente. (omissis)"

INQUINAMENTO DEL SUOLO, DEL SOTTOSUOLO, DELLE ACQUE SUPERFICIALI O DELLE ACQUE SOTTERRANEE (ART. 257 D.LGS. 152/2006)

"*1. Chiunque cagiona l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio è punito con la pena dell'arresto da sei mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro, se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti. In caso di mancata effettuazione della comunicazione di cui all'articolo 242, il trasgressore è punito con la pena dell'arresto da tre mesi a un anno o con l'ammenda da mille euro a ventiseimila euro. 2. Si applica la pena dell'arresto da un anno a due anni e la pena dell'ammenda da cinquemiladuecento euro a cinquantaduemila euro se l'inquinamento è provocato da sostanze pericolose. 3. Nella sentenza di condanna per la contravvenzione di cui ai commi 1 e 2, o nella sentenza*

emessa ai sensi dell'articolo 444 del codice di procedura penale, il beneficio della sospensione condizionale della pena può essere subordinato alla esecuzione degli interventi di emergenza, bonifica e ripristino ambientale. 4. L'osservanza dei progetti approvati ai sensi degli articoli 242 e seguenti costituisce condizione di non punibilità per i reati ambientali contemplati da altre leggi per il medesimo evento e per la stessa condotta di inquinamento di cui al comma 1."

TRAFFICO ILLECITO DI RIFIUTI (ART. 259 D.LGS. 152/2006)

"*1. Chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 26 del regolamento (CEE) 1° febbraio 1993, n. 259, o effettua una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'articolo 1, comma 3, lettere a), b), c) e d), del regolamento stesso è punito con la pena dell'ammenda da millecinquecentocinquanta euro a ventiseimila euro e con l'arresto fino a due anni. La pena è aumentata in caso di spedizione di rifiuti pericolosi. (omissis)*"

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 è stato introdotto 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. Nello specifico, l'articolo dispone testualmente:

" 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".

ATTIVITÀ ORGANIZZATE PER IL TRAFFICO ILLECITO DI RIFIUTI (452-QUATERDECIES C.P. MODIFICATO DA DECRETO LEGGE N. 116 DELL'8 AGOSTO 2025 E DALLA LEGGE N.147 DEL 3 OTTOBRE 2025)

Tale fattispecie di reato si configura 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'articolo prevede l'inasprimento di pene ed eventuale confisca delle cose utilizzate a commettere il reato.

"[I]. 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

[II]. 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

[III]. 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.

(IV). 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

(V). 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

(VI). 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."

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
RIA	Responsabile IA
RCA	Responsabile interno conformità anticorruzione

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E AI RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL 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 BITCONTROL S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di BITCONTROL S.r.l.
- Policy AI;
- D.Lgs. 3 aprile 2006, n. 152 (Codice dell'Ambiente) e successive modificazioni;

- Legge 22 maggio 2015, n. 68 (Ecoreati);
- D.L. n. 116/2020 (decreto "terra dei Fuochi")e Legge di conversione n. 147/2025;
- D.Lgs. n. 81/21.04.2026 (attuazione Direttiva UE 2024/1203 – tutela penale dell'ambiente): riforma organica dei reati ambientali, nuove fattispecie, aggravanti, abrogazione art. 733-bis c.p., aggiornamento art. 25-undecies D.Lgs. 231/2001

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 BITCONTROL, sono i seguenti:

- Gestione e caratterizzazione dei rifiuti
- Gestione delle acque reflue.

Si precisa che nella gestione dei rifiuti devono essere effettuati controlli documentali preventivi e successivi su autorizzazioni, iscrizioni, formulari, registrazioni, caratteristiche dei rifiuti, correttezza dei certificati analitici, iscrizione all'Albo dei gestori ambientali dei soggetti incaricati del trasporto e completezza dei flussi informativi rilevanti ai fini dell'art. 256 D.Lgs. 152/2006 e delle altre disposizioni applicabili.

Devono, altresì, essere previsti controlli rafforzati nei casi in cui i rifiuti siano pericolosi, le attività avvengano in siti contaminati o potenzialmente contaminati, vi sia rischio di compromissione o deterioramento di acque, aria, suolo, sottosuolo, ecosistema, biodiversità, flora o fauna, ovvero vi sia rischio per la vita o l'incolumità delle persone.

È vietata qualsiasi alterazione, falsificazione, incompletezza volontaria o manipolazione della documentazione ambientale, dei formulari, dei registri, dei certificati di analisi, delle informazioni inserite nei sistemi gestionali e dei dati trasmessi alle autorità o ai clienti.

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.

Ciò posto, al fine di assicurare uno standard di qualità e di corretta gestione del rischio ambientale, per il quale deve attuarsi un rafforzamento dell'efficacia esimente dello stesso Modello 231, la Bitcontrol Srl ha istituito una figura professionale che risulti in grado di garantire la puntuale osservanza delle

prescrizioni in materia di tutela dell'ambiente (D.Lgs. n. 152/2006 e ss.mm.), con la delega di assolvere a tutti i relativi compiti e le prescrizioni, così come normativamente previsti dal decreto legislativo n. 152 del 2006, dal codice penale e da ogni altra prescrizione in materia.

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. IDENTIFICAZIONE DELLE ATTIVITÀ SENSIBILI

Gli adempimenti relativi all'ambiente sono garantiti mediante il rigoroso rispetto di tutte le disposizioni previste in materia.

Le attività ritenute più specificamente a rischio per BitControl si ricollegano tutte all'inosservanza di norme poste a tutela dell'ambiente da cui discenda l'evento dannoso per la salute delle persone ovvero un danno rilevante per le componenti naturali dell'ambiente. L'area di tali attività coinvolge dunque tutta la componente produttiva dell'azienda.

L'area a rischio, in relazione alle peculiarità di business aziendale svolta da BITCONTROL e dall'organizzazione interna adottata, è di seguito riportata:

- PIANIFICAZIONE: si tratta dell'attività volta a fissare obiettivi coerenti con la politica aziendale, stabilire i processi necessari al raggiungimento degli obiettivi, definire e assegnare risorse;

- ATTUAZIONE E FUNZIONAMENTO: si tratta delle attività volte a definire strutture organizzative e responsabilità, modalità di formazione e comunicazione, modalità di gestione del sistema documentale, di controllo dei documenti e dei dati, le modalità di controllo operativo, la gestione delle emergenze, la selezione e il monitoraggio dei fornitori.

- CONTROLLO E AZIONI CORRETTIVE: si tratta delle attività volte ad implementare modalità di misura e monitoraggio delle prestazioni ambientali;

- RIESAME DELLA DIREZIONE: si tratta delle attività di riesame periodico del Vertice Aziendale al fine di valutare se il Sistema di Gestione Ambientale è stato completamente realizzato e se è sufficiente alla realizzazione della politica e degli obiettivi dell'azienda.

COSTITUISCONO INOLTRE AREE/PROCESSI SENSIBILI, OVE CONCRETAMENTE RICORRENTI NELL'OPERATIVITÀ AZIENDALE:

– l'utilizzo di strumenti di IA o software di supporto per monitoraggio ambientale, classificazione dati, predisposizione report tecnici, analisi di non conformità e gestione documentazione ambientale;

– progettazione, configurazione, sviluppo, collaudo, commissioning, assistenza e manutenzione di sistemi SCADA, PLC, RTU, DCS, IoT e telecontrollo destinati a impianti idrici, depuratori, potabilizzatori, reti energetiche, impianti industriali e sistemi di controllo ambientale;

– gestione di allarmi, soglie, log, storicizzazioni, report, misure e dati di processo aventi rilevanza ambientale, inclusa la prevenzione di alterazioni, omissioni, disattivazioni o manipolazioni che possano impedire la tempestiva rilevazione di anomalie, sversamenti, superamenti o malfunzionamenti;

– attività svolte presso sedi, cantieri e impianti dei clienti, con preventiva individuazione del produttore del rifiuto, delle responsabilità contrattuali e delle modalità di gestione di cavi, componenti elettrici ed elettronici, schede, batterie, accumulatori, imballaggi, toner, oli o altri residui eventualmente generati;

– gestione dei RAEE professionali e delle apparecchiature dismesse, assicurando classificazione, deposito temporaneo, consegna a soggetti autorizzati e conservazione della documentazione;

– qualifica e monitoraggio di trasportatori, intermediari, impianti destinatari, laboratori e appaltatori, mediante verifica iniziale e periodica di autorizzazioni, iscrizioni all'Albo nazionale gestori ambientali, scadenze, codici EER ammessi e coerenza delle attività autorizzate;

– acquisto, uso, stoccaggio e dismissione di prodotti chimici, batterie, sostanze e materiali potenzialmente pericolosi, con disponibilità delle schede di sicurezza e misure di prevenzione delle dispersioni;

– gestione delle emergenze ambientali e delle anomalie rilevate dai sistemi di supervisione, incluse escalation, registrazione dell'evento, comunicazione al cliente e alle funzioni aziendali competenti, conservazione dei log e divieto di cancellazione o modifica non autorizzata dei dati.

– la gestione dei dati ambientali, dei log, dei prompt e degli output generati da strumenti di IA impiegati in processi potenzialmente incidenti sulla compliance ambientale;

– la selezione, qualifica e controllo di fornitori, trasportatori, laboratori, consulenti e appaltatori che possano incidere sulla gestione rifiuti, sulle autorizzazioni, sulle analisi e sui controlli ambientali;

– le attività presso cantieri e siti dei clienti, con particolare riguardo a rifiuti, emissioni, reflui, documentazione ambientale e registrazioni di controllo;

– la partecipazione a gare o procedure negoziali nelle quali siano utilizzati sistemi di IA o siano rese dichiarazioni su processi che possano assumere rilievo ambientale

6 PRINCIPI GENERALI DI COMPORTAMENTO

I seguenti principi di carattere generale si applicano agli organi sociali, ai dirigenti ed a tutti i dipendenti di BITCONTROL anche se assunti con contratti di somministrazione per l'espletamento di specifiche commesse.

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; sono, altresì, proibite le violazioni ai principi comportamentali e divieti previsti nella presente Parte Speciale e nel Codice Etico di BITCONTROL.

Conformemente a quanto previsto nel Codice Etico, nelle procedure e nelle norme aziendali, i soggetti sopra individuati dovranno:

a) Tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge, dei limiti delle autorizzazioni ambientali ricevute e di eventuali prescrizioni, nonché delle procedure aziendali interne, in tutte le attività finalizzate:

− alla gestione degli scarichi di acque reflue;

− alla gestione, manutenzione e sanitizzazione degli ambienti di lavoro di proprietà o in usi a BITCONTROL.

b) Nella selezione dei fornitori cui è demandata la raccolta ed il trasporto dei rifiuti, porre particolare attenzione all'affidabilità ed accertarsi del possesso dei requisiti.

c) Rispettare la disciplina vigente sulla tracciabilità dei rifiuti e, ove applicabile, gli obblighi RENTRI, assicurando la corretta tenuta del registro cronologico di carico e scarico, la corretta emissione e gestione del FIR, la trasmissione dei dati, la conservazione documentale e la verifica della restituzione della copia completa. Fino al 15 settembre 2026 il FIR può essere emesso, nei casi previsti, in formato cartaceo o digitale; dal 16 settembre 2026 il FIR digitale è obbligatorio per gli iscritti al RENTRI, salvo successive modifiche normative.

In particolare, si precisa che ogni attività soggetta ad autorizzazione allo scarico deve essere svolta nel rigoroso rispetto delle prescrizioni contenute nel titolo autorizzativo. È vietato operare sulla base di autorizzazioni scadute, incomplete, ottenute mediante dichiarazioni non veritiere o conseguite con mezzi fraudolenti, anche alla luce della nozione estesa di condotta posta in essere "abusivamente".

INOLTRE, AI SOGGETTI SOPRA INDIVIDUATI È VIETATO, A MERO TITOLO ESEMPLIFICATIVO:

d) 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;

e) in sede di realizzazione di prescrizioni imposte dalla legge o da Enti pubblici in materia ambientale, perseguire l'obiettivo di risparmio costi e tempi a scapito della tutela dell'ambiente;

f) presentare o predisporre, anche in concorso con terzi, certificati falsi di analisi dei rifiuti;

g) superare i limiti consentiti, in termini di tempo e di quantità, per il temporaneo deposito di rifiuti sanitari o altri rifiuti.

h) in sede di ispezioni e verifiche, adottare comportamenti finalizzati ad influenzare indebitamente, nell'interesse della Società, il giudizio/parere degli Organismi di controllo.

Si rileva che i Destinatari sono tenuti a conformarsi, oltre che alla normativa ambientale e al Modello 231, ai principi di legalità, integrità, correttezza, diligenza professionale, tracciabilità e prevenzione sanciti dal Codice Etico e dal Codice di Condotta aziendali.

Nell'ambito delle attività con rilievo ambientale deve essere applicato il principio di precauzione e l'approccio preventivo alla gestione del rischio, anche nella progettazione, implementazione, manutenzione e monitoraggio di sistemi, servizi o strumenti tecnologici utilizzati dalla Società.

È fatto divieto di porre in essere condotte abusive anche quando formalmente coperte da autorizzazioni ottenute fraudolentemente o in violazione di disposizioni legislative, regolamentari o amministrative nazionali o dell'Unione europea in materia ambientale.

È fatto divieto di utilizzare o presentare dichiarazioni, analisi, certificati o altra documentazione falsa o non veritiera, anche ai fini autorizzativi, di trasporto, classificazione rifiuti, registrazione, comunicazione alle autorità, attestazione di conformità o gestione dei rapporti con clienti e fornitori.

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.

ALL'UOPO, LA SOCIETÀ SI IMPEGNA A:

• definire risorse, ruoli e responsabilità per l'attuazione delle disposizioni legislative e regolamentari in materia ambientale;
• fornire ai Destinatari un'adeguata informazione e formazione sui reati ambientali;
• fornire adeguata istruzione ed assistenza ai fornitori di servizi connessi con la gestione ambientale;
• comunicare ai responsabili delle funzioni di appartenenza ogni informazione relativa a situazioni a rischio di impatto ambientale o situazioni di emergenza dalle quali possa scaturire la commissione dei reati ambientali, da parte di soggetti interni od esterni all'organizzazione;
• avvisare le autorità competenti al verificarsi di eventi di inquinamento o del pericolo di inquinamento fornendo tutte le informazioni ad essi relative;
• segnalare ai soggetti competenti la mancata restituzione da parte del destinatario dei rifiuti, della copia del formulario di identificazione rifiuti debitamente firmata.

6.1 Utilizzo di sistemi di Intelligenza Artificiale in attività a rischio ambientale

L'utilizzo di strumenti di Intelligenza Artificiale in attività che possano incidere su profili ambientali è consentito esclusivamente nel rispetto della Policy IA aziendale, del Codice Etico, del Codice di Condotta, delle procedure interne e dei flussi informativi verso l'Organismo di Vigilanza.
Ogni decisione, azione o output generato dall'IA deve essere sempre validato da una persona autorizzata L'IA rappresenta uno strumento di supporto all'attività professionale e non un sostituto del giudizio umano.
Nei processi ambientali o con impatto ambientale:
– l'IA può avere esclusivamente funzione di supporto e non sostitutiva del giudizio umano;
– è ammesso il solo utilizzo di strumenti approvati dalla Società;
– devono essere garantiti logging, tracciabilità dei prompt e degli output rilevanti, conservazione documentale, verificabilità delle fonti dei dati e possibilità di audit;
– gli output IA non possono essere trasmessi all'esterno come documenti ufficiali, relazioni, dichiarazioni o comunicazioni aventi rilevanza ambientale senza preventiva revisione e validazione umana;
– in presenza di trattamenti ad elevato rischio devono essere attivati i presidi di valutazione preventiva richiamati dalla Policy IA.
È espressamente vietato inserire in strumenti di IA non autorizzati dati personali non anonimizzati, dati riservati o confidenziali, documentazione ambientale sensibile o altre informazioni aziendali protette

6.2. PRESIDI SPECIFICI DI BITCONTROL

In coerenza con il Modello 231, il Codice Etico e il Sistema di Gestione Ambientale certificato ISO 14001:2015, BitControl applica i seguenti protocolli specifici:

1. REGISTRO DEGLI ASPETTI AMBIENTALI E DEGLI OBBLIGHI DI CONFORMITÀ: aggiornamento periodico degli aspetti ambientali diretti e indiretti, delle prescrizioni legislative, contrattuali e autorizzative e valutazione della relativa significatività.

2. RESPONSABILITÀ E SEGREGAZIONE: identificazione del Responsabile del Sistema di Gestione Ambientale e dei responsabili operativi; separazione, per quanto possibile, tra chi classifica il rifiuto, chi autorizza il conferimento e chi verifica la documentazione.

3. RIFIUTI E RAEE: identificazione del codice EER da parte di personale competente; etichettatura; deposito temporaneo in aree idonee; divieto di miscelazione; controllo delle quantità e dei termini; gestione separata di batterie, accumulatori, apparecchiature elettroniche, cavi, toner e imballaggi.

4. FORNITORI AMBIENTALI: qualifica iniziale e riesame almeno annuale o in occasione di scadenze/modifiche; acquisizione e verifica delle autorizzazioni; controllo della targa dei mezzi e delle categorie/classi dell'Albo; sospensione del fornitore in caso di irregolarità.

5. TRACCIABILITÀ RENTRI/FIR: individuazione degli utenti abilitati; credenziali personali; divieto di condivisione; controllo a quattro occhi sui dati essenziali; conservazione delle ricevute e delle copie; procedura di continuità operativa in caso di indisponibilità dei servizi.

6. ATTIVITÀ PRESSO IMPIANTI DEI CLIENTI: definizione preventiva, nel contratto o nel piano operativo, delle responsabilità ambientali; osservanza delle procedure del sito; raccolta separata dei residui; divieto di abbandono; immediata segnalazione di sversamenti o anomalie.

7. SOFTWARE E SISTEMI DI TELECONTROLLO: gestione controllata delle modifiche; test e validazione delle soglie e degli allarmi; profilazione degli accessi; logging; backup; tracciabilità delle versioni; doppia verifica per modifiche che incidono su parametri ambientali; divieto di disabilitare allarmi senza autorizzazione e motivazione documentata.

8. DATI AMBIENTALI: protezione dell'integrità e disponibilità dei dati; conservazione dei log; divieto di alterazione o cancellazione; verifica della plausibilità delle misure e gestione documentata dei dati mancanti o anomali.

9. EMERGENZE AMBIENTALI: disponibilità di istruzioni, contatti ed eventuali kit di contenimento; prova periodica delle risposte; registrazione dell'evento, delle azioni adottate e delle comunicazioni effettuate.

10. AUDIT E MIGLIORAMENTO: audit interni ISO 14001 coordinati, per quanto rilevante, con i controlli 231; gestione di non conformità e azioni correttive; riesame della Direzione; trasmissione all'OdV degli esiti con rilievo 231.

11. FORMAZIONE: formazione iniziale e periodica, differenziata per ruolo, su classificazione e gestione dei rifiuti, RENTRI/FIR, emergenze, attività nei siti dei clienti, integrità dei dati e obblighi di segnalazione.

12. CONTROLLO DOCUMENTALE: utilizzo esclusivo di modelli aggiornati; approvazione delle dichiarazioni ambientali da parte di soggetti autorizzati; archiviazione nel sistema documentale aziendale e rispetto dei tempi di conservazione.

Utilizzo di sistemi di Intelligenza Artificiale in attività a rischio ambientale

L'utilizzo di strumenti di Intelligenza Artificiale in attività che possano incidere su profili ambientali è consentito esclusivamente nel rispetto della Policy IA aziendale, del Codice Etico, del Codice di Condotta, delle procedure interne e dei flussi informativi verso l'Organismo di Vigilanza.

Ogni decisione, azione o output generato dall'IA deve essere sempre validato da una persona autorizzata L'IA rappresenta uno strumento di supporto all'attività professionale e non un sostituto del giudizio umano.

NEI PROCESSI AMBIENTALI O CON IMPATTO AMBIENTALE:

– l'IA può avere esclusivamente funzione di supporto e non sostitutiva del giudizio umano;

– è ammesso il solo utilizzo di strumenti approvati dalla Società;

– devono essere garantiti logging, tracciabilità dei prompt e degli output rilevanti, conservazione documentale, verificabilità delle fonti dei dati e possibilità di audit;

– gli output IA non possono essere trasmessi all'esterno come documenti ufficiali, relazioni, dichiarazioni o comunicazioni aventi rilevanza ambientale senza preventiva revisione e validazione umana;

– in presenza di trattamenti ad elevato rischio devono essere attivati i presidi di valutazione preventiva richiamati dalla Policy IA.

È espressamente vietato inserire in strumenti di IA non autorizzati dati personali non anonimizzati, dati riservati o confidenziali, documentazione ambientale sensibile o altre informazioni aziendali protette

7 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.).

8 CERTIFICAZIONE ISO 14001:2015

Come previsto nella PMOG10, BITCONTROL 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 BITCONTROL 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.

La certificazione ISO 14001:2015 costituisce un presidio organizzativo integrato nel Modello 231, ma non sostituisce la valutazione dei rischi-reato né i protocolli previsti dalla presente Procedura.

Ai fini 231, sono resi disponibili all'OdV, secondo i flussi definiti, almeno: analisi del contesto; registro degli aspetti ambientali; registro degli obblighi di conformità; obiettivi e programmi ambientali; esiti degli audit; non conformità; azioni correttive; verbali di riesame; dati su rifiuti e consumi; emergenze, reclami, ispezioni e provvedimenti delle autorità; valutazioni dei fornitori ambientali.

Ogni modifica significativa delle attività, delle sedi, delle commesse, delle tecnologie, dei processi di telecontrollo o della normativa comporta il riesame degli aspetti ambientali, dei rischi 231 e dei controlli applicabili.

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.

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.

In particolare, devono formare oggetto di tempestivo flusso informativo verso l'Organismo di Vigilanza anche:

– eventi di inquinamento, dispersione, smaltimento irregolare, anomalie nella gestione rifiuti o reflui;

– ispezioni, prescrizioni, diffide, contestazioni o richieste documentali di autorità o enti di controllo in materia ambientale;

– mancata o tardiva restituzione o formalizzazione della documentazione di trasporto e tracciabilità dei rifiuti;

– anomalie o incidenti relativi a sistemi IA o digitali impiegati in processi con impatto ambientale;

– non conformità rilevate in audit interni o esterni aventi impatto sulla compliance ambientale;

– ingresso di nuovi soggetti in ruoli sensibili o variazione di deleghe e responsabilità rilevanti per i processi ambientali

Con specifico riguardo all'uso di IA, devono essere trasmessi all'OdV i flussi informativi relativi alla dichiarazione dell'utilizzo di sistemi di IA, alle modalità di impiego degli strumenti autorizzati, ai controlli sugli output generati, alla tracciabilità dei prompt e degli output rilevanti e all'individuazione delle responsabilità dei soggetti coinvolti.

L'OdV esercita i propri poteri di controllo anche con riferimento all'utilizzo di sistemi di IA nei processi con impatto ambientale, verificando il rispetto della Policy IA, degli obblighi di tracciabilità e supervisione umana, nonché la coerenza tra i presidi di compliance ambientale, il miglioramento del Rating ESG e il Rating di Legalità.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA del 14.11.2020	ADOZIONE
Rev. 1	CDA del 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA del 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA del 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA del 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA del 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DEL 11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.06.2026	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 14

SOMMARIO

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.

Si precisa altresì, che la presente Procedura si coordina con il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 aggiornato nel 2026, con il Codice Etico, con il Codice di Condotta, con la Policy sull'Intelligenza Artificiale, con la Procedura Whistleblowing e con le ulteriori procedure aziendali approvate o aggiornate.

La presente Procedura si applica anche ai processi aziendali nei quali il rischio di agevolazione o infiltrazione criminale possa manifestarsi mediante l'utilizzo di strumenti

digitali o di Intelligenza Artificiale, nonché ai rapporti con controparti, intermediari, consulenti, fornitori, appaltatori, operatori economici, clienti e soggetti esteri.

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
RIA	Responsabile IA
RCA	Responsabile interno conformità anticorruzione

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E AI RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL 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 BITCONTROL S.r.l.;
- Modello di Gestione, Organizzazione e Controllo di BITCONTROL S.r.l.
- D.Lgs. n. 211/2025 in materia di violazioni delle misure restrittive dell'Unione Europea.

- Codice penale: artt. 416, 416-bis, 416-ter e 630; art. 74 D.P.R. 9 ottobre 1990, n. 309; art. 407, comma 2, lett. a), n. 5, c.p.p.;
- Legge 16 marzo 2006, n. 146, in materia di criminalità organizzata transnazionale;
- D.Lgs. 6 settembre 2011, n. 159 e s.m.i. (Codice antimafia), con particolare riferimento alla documentazione antimafia, alle comunicazioni e informazioni antimafia e alle misure di prevenzione;
- Legge 13 agosto 2010, n. 136 e s.m.i., in materia di tracciabilità dei flussi finanziari relativi a commesse pubbliche;
- D.Lgs. 21 novembre 2007, n. 231 e s.m.i., come modificato dal D.Lgs. 31 dicembre 2025, n. 210, in materia di prevenzione dell'utilizzo del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo;
- D.Lgs. 31 marzo 2023, n. 36 e s.m.i. (Codice dei contratti pubblici), con particolare riferimento agli artt. 94, 95, 96 e 98;
- D.Lgs. 10 marzo 2023, n. 24 e Procedura Whistleblowing aziendale;
- Policy aziendali in materia di anticorruzione, selezione delle controparti, gestione degli approvvigionamenti, sicurezza delle informazioni e utilizzo dell'Intelligenza Artificiale.

4 CAMPO DI APPLICAZIONE E 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.

Per BitControl assumono particolare rilevanza, oltre alle funzioni indicate nell'organigramma, l'Ufficio Gare/Commerciale, l'Approvvigionamento, l'Amministrazione e Finanza, le Risorse Umane, i Responsabili Tecnici e di Commessa, il Facility Management e i soggetti che gestiscono accessi remoti, credenziali, infrastrutture SCADA, PLC, RTU, DCS, telecontrollo e manutenzione presso siti di clienti pubblici e privati. Ciascuna funzione opera nel rispetto della segregazione dei compiti, delle deleghe e dei poteri autorizzativi vigenti.

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 POLITO 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 atrenta.*

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 BITCONTROL, 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.
- ✓ costituzione e gestione di RTI, consorzi, reti di impresa, avvalimenti, subappalti e altri accordi di collaborazione;
- ✓ selezione, qualifica e monitoraggio di fornitori, installatori, trasportatori, consulenti, intermediari commerciali e partner tecnologici, anche esteri;
- ✓ gestione di sponsorizzazioni, liberalità, omaggi, spese di rappresentanza e iniziative territoriali;
- ✓ apertura e gestione di sedi operative, cantieri, presidi tecnici e accessi presso impianti idrici, depuratori, potabilizzatori, impianti energetici e siti industriali;
- ✓ gestione di credenziali privilegiate e accessi fisici o remoti ai sistemi di telecontrollo e alle infrastrutture dei clienti;
- ✓ affidamento di lavorazioni o servizi in territori o settori caratterizzati da maggiore esposizione a fenomeni di infiltrazione criminale;
- ✓ gestione di rapporti con controparti estere, operazioni transfrontaliere e pagamenti verso Paesi ad alto rischio o soggetti sottoposti a misure restrittive.

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.

Inoltre è necessario evidenziare che nelle procedure di gara o affidamento in cui siano utilizzati sistemi di Intelligenza Artificiale, devono essere introdotti specifici obblighi di dichiarazione dell'utilizzo dei sistemi di IA, regolamentazione delle modalità di impiego degli strumenti autorizzati, controlli preventivi e successivi sugli output generati, tracciabilità dei prompt e degli output rilevanti, individuazione delle responsabilità dei soggetti coinvolti e specifici flussi informativi verso l'Organismo di Vigilanza.

L'OdV rileva che la Delibera impone agli operatori economici di dichiarare l'eventuale impiego di sistemi di IA nella predisposizione dell'offerta e della documentazione di gara, individuando le attività svolte mediante tali strumenti e confermando che la responsabilità giuridica, tecnica e professionale dei contenuti rimane integralmente in capo all'operatore economico.

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.

Sul punto, si rileva che la formazione obbligatoria deve essere aggiornata per recepire: il D.Lgs. n. 211/2025 in materia di misure restrittive UE; il D.Lgs. n. 83/2026 in materia di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare; la Legge n. 34/2026 in materia di lavoro agile e sicurezza; il D.Lgs. n. 81/2026 in materia ambientale; la disciplina interna sull'uso dell'Intelligenza Artificiale; la Procedura Whistleblowing.

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;

11) preventiva identificazione della controparte, dei titolari effettivi, degli amministratori, dei procuratori e della struttura proprietaria, con verifica della coerenza tra attività dichiarata, oggetto del rapporto e capacità tecnico-economica;

12) acquisizione, in misura proporzionata al rischio e alla tipologia del rapporto, di visura camerale aggiornata, DURC, dichiarazioni ex D.P.R. 445/2000, documentazione antimafia ove richiesta, iscrizioni ad albi o white list ove pertinenti, certificazioni, referenze e coordinate bancarie intestate alla controparte;

13) verifica preventiva e periodica delle controparti mediante fonti ufficiali e banche dati aziendalmente autorizzate, con particolare attenzione a interdittive antimafia, misure di prevenzione, sanzioni interdittive ex D.Lgs. 231/2001, procedure concorsuali, variazioni anomale dell'assetto proprietario e notizie rilevanti sulla reputazione commerciale;

14) obbligo di utilizzare esclusivamente strumenti di pagamento tracciabili, conti correnti intestati alla controparte e, per le commesse pubbliche, conti dedicati e CIG/CUP ove previsti dalla Legge n. 136/2010;

15) divieto di pagamenti in contanti oltre i limiti di legge, pagamenti frazionati artificiosamente, compensazioni anomale, pagamenti verso conti di terzi, Paesi diversi da quello della controparte o soggetti non indicati nel contratto, salvo preventiva motivazione e autorizzazione rafforzata;

16) inserimento nei contratti di clausole 231, antimafia, anticorruzione, tracciabilità, audit, obbligo di comunicare variazioni societarie e facoltà di sospensione o risoluzione in presenza di anomalie, interdittive o violazioni;

17) segregazione tra proposta, selezione, verifica, autorizzazione, stipula, contabilizzazione e pagamento; ogni deroga deve essere motivata, autorizzata e conservata;

18) divieto di ricorrere a consulenti, intermediari o subcontraenti privi di effettiva struttura, esperienza o utilità per il progetto, nonché di riconoscere compensi sproporzionati, success fee non giustificate o rimborsi privi di idonea documentazione;

19) monitoraggio continuativo dei subappaltatori e partner durante l'esecuzione, compresi accessi ai siti, personale impiegato, variazioni dei soggetti apicali, sub-affidamenti non autorizzati e corrispondenza tra prestazioni eseguite e fatturate;

20) obbligo di immediata escalation all'Organo Amministrativo, alla Funzione Legale/Compliance e all'OdV in presenza di indicatori di anomalia o tentativi di condizionamento, intimidazione, imposizione di fornitori, richieste di assunzione, pressioni sul personale, minacce o danneggiamenti.

I presidi generali sopra elencati devono intendersi integrati dai contenuti del Codice di Condotta, del Codice Etico, della Policy IA e della Procedura Whistleblowing vigente.
In particolare, i Destinatari sono tenuti a conformarsi ai principi di legalità, integrità, correttezza, tracciabilità, trasparenza, riservatezza, prevenzione dei conflitti di interesse e tutela delle informazioni sanciti dal Codice Etico e dal Codice di Condotta.
Le dichiarazioni periodiche dei Responsabili interni devono includere anche l'attestazione dell'assenza di anomalie rilevanti in materia di rapporti con controparti estere, misure restrittive UE, utilizzo di strumenti di IA in processi sensibili, irregolarità documentali e violazioni delle procedure di tracciabilità.
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.
Dunque, l'Organo amministrativo della Società potrà prevedere ulteriori misure a maggiore tutela delle aree di rischio individuate e a integrazione dei comportamenti sopra elencati.
In ultimo, si osserva che a seguito delle nuove disposizioni, l'utilizzo di strumenti di Intelligenza Artificiale nei processi disciplinati dalla presente Procedura è consentito esclusivamente nel rispetto della Policy IA aziendale, del Codice Etico, del Codice di Condotta e delle ulteriori procedure aziendali vigenti.
È consentito esclusivamente l'utilizzo di strumenti approvati dalla Società; è vietato l'uso di strumenti non approvati o di account personali per finalità aziendali.
L'IA deve operare sempre sotto il controllo di una persona autorizzata. Ogni output generato da un sistema di IA deve essere validato da un essere umano prima di produrre effetti giuridici, economici o significativi sulle persone.
I Destinatari si impegnano a non inserire in alcun strumento di IA – approvato o non approvato – dati personali non anonimizzati, dati appartenenti a categorie particolari ai sensi dell'art. 9 GDPR, ovvero informazioni classificate come riservate o confidenziali secondo la classificazione aziendale.
Devono essere assicurati logging, tracciabilità dei prompt e degli output rilevanti, conservazione documentale, verifica umana, possibilità di audit e, ove necessario, valutazione preventiva d'impatto per trattamenti ad alto rischio.
Qualsiasi uso improprio, violazione di dati o anomalia relativa a strumenti di IA impiegati nei processi disciplinati dalla presente Procedura deve essere segnalata immediatamente al Responsabile Sicurezza Informatica, al DPO e all'Organismo di Vigilanza.

AREA A RISCHIO N. 1: ADEMPIMENTI IN MATERIA DI PERSONALE

È VIETATA L'ASSUNZIONE O L'ATTRIBUZIONE DI INCARICHI QUALE CONTROPARTITA DI PRESSIONI, SEGNALAZIONI O RICHIESTE PROVENIENTI DA CLIENTI, FORNITORI, PUBBLICI UFFICIALI, ESPONENTI POLITICI O SOGGETTI RICONDUCIBILI A ORGANIZZAZIONI CRIMINALI. LE CANDIDATURE SEGNALATE DEVONO SEGUIRE IL MEDESIMO ITER SELETTIVO, CON EVIDENZA DELLA COMPETENZA, DELLA NECESSITÀ ORGANIZZATIVA E DELLA DECISIONE FINALE.

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.

L'anagrafica dei soggetti sensibili e dei destinatari della presente Procedura deve essere aggiornata anche in relazione alle nuove assunzioni, ove inseriti in processi rilevanti ai fini del Modello 231.

Nelle assunzioni o nell'impiego di personale straniero devono essere effettuati i controlli sulla regolarità del titolo di soggiorno e del permesso di lavoro, in coerenza con le modifiche introdotte dal D.Lgs. n. 83/2026 e con i rischi richiamati dall'art. 25-duodecies D.Lgs. 231/2001.

Per il personale operante in modalità agile devono essere rispettati gli obblighi informativi e documentali introdotti dalla Legge n. 34/2026 e dalle procedure aziendali sul lavoro agile, incluse l'informativa sui rischi, la sottoscrizione degli accordi individuali e il rispetto del regolamento aziendale sul lavoro agile.

AREA A RISCHIO N. 2: STIPULA E GESTIONE DI CONTRATTI

PER OGNI NUOVO FORNITORE O CONSULENTE DEVE ESSERE COMPILATA E ARCHIVIATA UNA SCHEDA DI QUALIFICA CONTENENTE ALMENO: RAGIONE SOCIALE, TITOLARE EFFETTIVO, COMPAGINE SOCIALE, AMMINISTRATORI, SEDE, OGGETTO SOCIALE, REFERENZE, DURC, ISCRIZIONI E AUTORIZZAZIONI, COORDINATE BANCARIE, ESITO DELLE VERIFICHE REPUTAZIONALI E

MOTIVAZIONE DELLA SCELTA. PER FORNITORI OPERANTI IN ATTIVITÀ MAGGIORMENTE ESPOSTE O IN SUBAPPALTI PUBBLICI, LA VERIFICA È AGGIORNATA ALMENO ANNUALMENTE E IN OCCASIONE DI VARIAZIONI SOCIETARIE.

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.

Sul punto, si precisa che la qualificazione di fornitori, consulenti, agenti, intermediari e partner deve includere, ove applicabile, lo screening della controparte, del beneficiario effettivo, della struttura proprietaria, delle coordinate bancarie e dell'eventuale esposizione a misure restrittive dell'Unione Europea.

Devono essere previsti criteri di escalation interna nei casi di controparte non chiaramente identificabile, utilizzo di intermediari non coerenti, richiesta di pagamento verso soggetti diversi dal contraente, documentazione incompleta o anomalie che possano far presumere finalità elusive o rischio di agevolazione criminale.

I contratti con agenti o intermediari devono essere stipulati per iscritto, con compensi proporzionati alla prestazione, pagamenti tracciabili su conti intestati al beneficiario effettivo e clausole anticorruzione e di adesione al Modello 231, al Codice Etico e al Codice di Condotta.

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

I PAGAMENTI DEVONO ESSERE DISPOSTI SOLO A FRONTE DI CONTRATTO O ORDINE AUTORIZZATO, VERIFICA DELL'ESECUZIONE DELLA PRESTAZIONE, FATTURA COERENTE E COORDINATE BANCARIE PREVIAMENTE VALIDATE. OGNI MODIFICA DELL'IBAN DEVE ESSERE VERIFICATA TRAMITE UN CANALE INDIPENDENTE. PER LE COMMESSE PUBBLICHE DEVONO ESSERE RISPETTATI GLI OBBLIGHI DI TRACCIABILITÀ E DEVONO ESSERE CONSERVATI I RIFERIMENTI CIG/CUP, OVE APPLICABILI.

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.

Prima di disporre o autorizzare pagamenti in favore di controparti esposte a rischio, controparti estere, intermediari o soggetti coinvolti in operazioni sensibili, devono essere effettuati controlli di screening sulla controparte, sul beneficiario effettivo, sul conto di destinazione e sull'assenza di collegamenti con soggetti designati o Paesi interessati da misure restrittive UE.

In presenza di elementi di anomalia, documentazione incoerente, beneficiario diverso dal contraente, operazioni sospette o rischio di violazione delle misure restrittive UE, l'operazione deve essere immediatamente sospesa e sottoposta a escalation al Responsabile amministrativo/legale e all'Organismo di Vigilanza.

Le verifiche svolte, le autorizzazioni, le sospensioni e le decisioni assunte devono essere tracciate e conservate agli atti.

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 BITCONTROL 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 BITCONTROL 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).

Prima di disporre o autorizzare pagamenti in favore di controparti esposte a rischio, controparti estere, intermediari o soggetti coinvolti in operazioni sensibili, devono essere effettuati controlli di screening sulla controparte, sul beneficiario effettivo, sul conto di destinazione e sull'assenza di collegamenti con soggetti designati o Paesi interessati da misure restrittive UE.

In presenza di elementi di anomalia, documentazione incoerente, beneficiario diverso dal contraente, operazioni sospette o rischio di violazione delle misure restrittive UE, l'operazione deve essere immediatamente sospesa e sottoposta a escalation al Responsabile amministrativo/legale e all'Organismo di Vigilanza.

Le verifiche svolte, le autorizzazioni, le sospensioni e le decisioni assunte devono essere tracciate e conservate agli atti.

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.

Costituiscono inoltre aree sensibili, ove concretamente ricorrenti nell'operatività aziendale:

– i rapporti con controparti estere, beneficiari effettivi, intermediari commerciali o soggetti coinvolti in operazioni internazionali;

– i processi di screening delle controparti e dei beneficiari effettivi ai fini della verifica di eventuali collegamenti con soggetti designati o destinatari di misure restrittive UE;

- l'utilizzo di strumenti di Intelligenza Artificiale nei processi di qualificazione di fornitori, consulenti, partner, intermediari, partecipazione a gare, predisposizione di documentazione o analisi di supporto;

– i processi connessi alla selezione, assunzione e gestione di personale straniero, ove rilevino i profili di regolarità del soggiorno richiamati dal D.Lgs. n. 83/2026;

– i processi interessati da lavoro agile, ove il relativo assetto organizzativo possa incidere sui controlli, sulla tracciabilità e sulla sicurezza delle attività sensibili ai fini del Modello 231.

6.1 PRESIDI SPECIFICI BITCONTROL E INDICATORI DI ANOMALIA

In ragione dell'attività svolta da BitControl nel settore dell'automazione, del telecontrollo e della manutenzione di sistemi destinati anche a utilities, impianti idrici, depuratori, potabilizzatori, siti energetici e industriali, devono essere applicati controlli rafforzati nei rapporti con soggetti che richiedono accessi a infrastrutture, credenziali, software, dati di processo o siti sensibili.

Costituiscono indicatori di anomalia, da valutare congiuntamente e non automaticamente: assetti proprietari opachi o frequentemente modificati; titolari effettivi non identificabili; sede o struttura non coerente con l'attività; prezzi o ribassi anomali; richiesta di subaffidamenti non previsti; personale non dichiarato; richiesta di pagamenti su conti di terzi o esteri; uso ingiustificato di contanti; intermediari senza ruolo effettivo; imposizione di fornitori locali; pressioni per evitare controlli; rifiuto di sottoscrivere clausole 231; documenti discordanti o apparentemente alterati; accessi remoti richiesti fuori dalle procedure; utilizzo di credenziali condivise; tentativi di disabilitare logging, allarmi o tracciabilità.

In presenza di uno o più indicatori, il processo è sospeso nei limiti consentiti dal contratto e sottoposto a due diligence rafforzata, con decisione motivata dell'Organo Amministrativo e informativa all'OdV. È vietata ogni ritorsione nei confronti di chi effettua in buona fede una segnalazione attraverso i canali previsti dalla Procedura Whistleblowing.

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.

Si precisa altresì che è fatto divieto di intrattenere rapporti, porre in essere operazioni o mettere a disposizione fondi, beni, servizi o risorse economiche in favore di soggetti designati o comunque sottoposti a misure restrittive dell'Unione Europea, nonché di porre in essere condotte elusive dei controlli mediante utilizzo di intermediari, documentazione falsa o operazioni non trasparenti.

È fatto divieto di omettere comunicazioni o informazioni dovute alle autorità competenti in materia di fondi, risorse economiche, beneficiari effettivi o operazioni riconducibili a soggetti designati.

È vietato intrattenere rapporti con fornitori, consulenti, agenti, intermediari o partner senza il rispetto delle procedure di qualificazione, delle verifiche di onorabilità, della tracciabilità dei pagamenti e delle clausole contrattuali di adesione al Modello 231, al Codice Etico e al Codice di Condotta.

È vietato falsificare, alterare, occultare o distruggere documentazione societaria, contabile, contrattuale, doganale, di gara, di qualifica fornitori o di altra natura rilevante ai fini della prevenzione dei reati presupposto e della tracciabilità dei rapporti con terzi.

La segnalazione è obbligatoria quando il destinatario abbia conoscenza diretta di: 1. condotte corruttive, anche solo tentate; 2. reati presupposto ai sensi del D.Lgs. 231/2001; 3. violazioni delle norme di sicurezza che abbiano causato o possano causare danni a persone; 4. frodi o falsificazioni documentali a danno della Società, dei clienti o di enti pubblici.

7 BIS GARE, RTI, SUBAPPALTI, PARTNER E ACCESSI AI SISTEMI DI TELECONTROLLO

Prima della partecipazione a una gara o della costituzione di RTI, consorzi, reti, avvalimenti o subappalti, l'Ufficio Gare e la Funzione competente verificano la controparte, il titolare effettivo, i requisiti generali, l'assenza di cause di esclusione, la documentazione antimafia ove applicabile e la coerenza del ruolo tecnico ed economico attribuito. Le verifiche e le autorizzazioni sono conservate nel fascicolo di gara o di commessa.

Gli accessi fisici e remoti ai sistemi SCADA, PLC, RTU, DCS e alle reti dei clienti devono essere nominativi, autorizzati, limitati nel tempo e nei privilegi, registrati e riesaminati. Sono vietati account condivisi, accessi tramite credenziali personali non autorizzate, disabilitazione dei log e trasferimento non autorizzato di dati o

configurazioni. I fornitori terzi devono sottoscrivere obblighi di sicurezza, riservatezza, legalità e rispetto del Modello 231.

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.

In particolare, si osserva che devono essere tempestivamente comunicati all'Organismo di Vigilanza anche:

– operazioni sospese, bloccate o sottoposte a escalation per rischio di collegamento con soggetti sanzionati o misure restrittive dell'Unione Europea;

- anomalie emerse nei controlli su controparti, beneficiari effettivi, intermediari o coordinate bancarie;

– irregolarità nella selezione o gestione di fornitori, consulenti, appaltatori, agenti o intermediari;

– violazioni o criticità relative all'impiego di personale straniero o al lavoro agile in processi sensibili;

– utilizzo di sistemi di IA nei processi disciplinati dalla presente Procedura, con indicazione delle finalità, degli strumenti autorizzati impiegati, dei controlli svolti sugli output e delle eventuali criticità riscontrate;

– segnalazioni whistleblowing ricevute aventi ad oggetto fatti rilevanti per i processi di prevenzione dei delitti di criminalità organizzata.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA del 14.11.2020	ADOZIONE
Rev. 1	CDA del 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA del 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA del 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA del 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA del 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

PARTE SPECIALE 15

SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

BITCONTROL considera prioritario promuovere una cultura aziendale ispirata a valori propri di una governance solida e trasparente ed è consapevole che il fenomeno della corruzione rappresenta un ostacolo allo sviluppo economico, politico e sociale, nonchè una pesante distorsione delle regole, della correttezza e della trasparenza del mercato in cui opera.

Pertanto, BITCONTROL si impegna a contrastare la corruzione in ogni sua forma, ove per corruzione si intende l'offerta o l'accettazione, in via diretta o indiretta, di denaro o di altra utilità in grado di influenzare il ricevente, al fine di indurre o premiare l'esecuzione di una funzione/attività o l'omissione della stessa.

Pertanto, BITCONTROL si impegna a contrastare sia la "corruzione attiva" (offerta) sia la "corruzione passiva" (accettazione), e ciò sia nel caso in cui venga coinvolto un soggetto pubblico ("corruzione pubblica") che nei rapporti tra soggetti privati (corruzione privata), sia la corruzione finalizzata a far compiere un atto contrario ai propri doveri di ufficio (corruzione propria) che quella avente per scopo il compimento di un atto del proprio ufficio (corruzione impropria), sia la corruzione antecedente che quella successiva al compimento degli atti di ufficio.

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
RCA	Responsabile interno conformità anticorruzione

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E AI RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

3 RIFERIMENTI NORMATIVI DEL MODELLO

- DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231 E SUCCESSIVE MODIFICHE E INTEGRAZIONI;

- CODICE PENALE, CON PARTICOLARE RIFERIMENTO AGLI ARTT. 317, 318, 319, 319-BIS, 319-TER, 319-QUATER, 320, 321, 322, 322-BIS E 346-BIS;

- CODICE CIVILE, CON PARTICOLARE RIFERIMENTO AGLI ARTT. 2635 E 2635-BIS;

- LEGGE 6 NOVEMBRE 2012, N. 190, PER QUANTO APPLICABILE E QUALE RIFERIMENTO DI BEST PRACTICE;

- DECRETO LEGISLATIVO 14 MARZO 2013, N. 33 E DECRETO LEGISLATIVO 8 APRILE 2013, N. 39, PER QUANTO APPLICABILI;

- ART. 53, COMMA 16-TER, DEL DECRETO LEGISLATIVO 30 MARZO 2001, N. 165, IN MATERIA DI ATTIVITÀ SUCCESSIVA ALLA CESSAZIONE DEL RAPPORTO DI PUBBLICO IMPIEGO (PANTOUFLAGE);

- DECRETO LEGISLATIVO 10 MARZO 2023, N. 24 E PROCEDURA AZIENDALE WHISTLEBLOWING VIGENTE;

- DECRETO LEGISLATIVO 31 MARZO 2023, N. 36 E SUCCESSIVE MODIFICHE E INTEGRAZIONI, CON RIFERIMENTO ALLE PROCEDURE DI AFFIDAMENTO E AI RAPPORTI CON LE STAZIONI APPALTANTI;

- LEGGE 9 AGOSTO 2024, N. 114, CHE HA ABROGATO L'ART. 323 C.P. E RIFORMULATO L'ART. 346-BIS C.P.;

- CODICE ETICO DI BITCONTROL S.R.L., APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE IL 25.06.2026;

- CODICE DISCIPLINARE DI BITCONTROL S.R.L.;

- POLITICA ANTICORRUZIONE DI BITCONTROL S.R.L.;

- MISURE INTEGRATIVE DEL MODELLO 231 IN MATERIA DI ANTICORRUZIONE E TRASPARENZA - TRIENNIO 2025/2028;

- MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI BITCONTROL S.R.L. E RELATIVE PROCEDURE SPECIALI.

4 CAMPO DI APPLICAZIONE E DESTINATARI DELLA PROCEDURA

La presente procedura si applica ai componenti degli organi sociali, ai soggetti apicali, ai dipendenti e a tutti coloro che, anche di fatto, operano in nome, per conto o nell'interesse di BITCONTROL S.r.l., nonché, per quanto compatibile, a fornitori, consulenti, professionisti, intermediari, partner commerciali, subappaltatori e ulteriori terze parti contrattuali. I Destinatari sono tenuti a conoscere e rispettare il Codice Etico, il Modello 231, la Politica Anticorruzione, le Misure Integrative e le altre procedure aziendali applicabili.

La procedura è riesaminata almeno annualmente e, in ogni caso, quando intervengano modifiche normative, organizzative o operative rilevanti, mutamenti delle aree di rischio, esiti di audit, segnalazioni o violazioni significative. Le modifiche sono sottoposte all'approvazione del Consiglio di Amministrazione, previo coinvolgimento delle funzioni competenti e informativa all'Organismo di Vigilanza.

5 I REATI CORRUTTIVI (ART. 25 E 25 TER D.LGS. 231/01)

La presente procedura presidia i rischi di corruzione pubblica e privata riconducibili, in particolare, ai reati richiamati dagli artt. 25 e 25-ter del D.Lgs. 231/2001. Essa considera altresì le condotte strumentali o prodromiche alla corruzione, quali la formazione di fondi occulti, l'interposizione di consulenti o intermediari, l'alterazione di procedure di gara, l'indebito condizionamento di selezioni, assunzioni o progressioni, la concessione di omaggi, sponsorizzazioni o liberalità non giustificate e la gestione non trasparente dei flussi finanziari.

I reati di corruzione tra privati e di istigazione alla corruzione tra privati, pur rientrando tra i reati societari di cui all'art. 25-ter del D.Lgs. 231/2001, sono inclusi nella presente area sensibile in ragione dell'omogeneità delle modalità realizzative e dei presidi di controllo applicabili.

La procedura è coordinata con il Codice Etico, la Politica Anticorruzione e le Misure Integrative, che estendono la prevenzione anche alle condotte corruttive commesse in danno della Società o comunque contrarie ai principi di legalità, trasparenza, correttezza e leale concorrenza.

TRAFFICO DI INFLUENZE ILLECITE (ART. 346-BIS C.P.)

Il reato, come riformulato dalla Legge n. 114/2024, punisce chi, fuori dei casi di concorso nei reati di corruzione espressamente richiamati, utilizzando intenzionalmente relazioni esistenti con un pubblico ufficiale, un incaricato di pubblico servizio o soggetti equiparati, indebitamente fa dare o promettere, a sé o ad altri, denaro o altra utilità economica per remunerare il pubblico agente in relazione all'esercizio delle sue funzioni ovvero per realizzare un'altra mediazione illecita. È punito anche chi dà o promette indebitamente il denaro o l'utilità economica.

È vietato avvalersi di consulenti, intermediari, procacciatori, partner o altri terzi per ottenere indebiti vantaggi, influenzare decisioni pubbliche o aggirare i divieti previsti dalla legge, dal Codice Etico e dalla presente procedura. Ogni incarico deve essere giustificato, autorizzato, formalizzato, congruo, tracciabile e sottoposto a verifica reputazionale e sul conflitto di interessi.

Agli effetti della legge penale si considera Ente della Pubblica Amministrazione qualsiasi persona giuridica che persegua e/o realizzi e gestisca interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa, disciplinata da norme di diritto pubblico e manifestantesi mediante atti autoritativi. A titolo meramente esemplificativo e anche avendo riguardo all'operatività della Società si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione: a) lo Stato, le Regioni, le Province, i Comuni; b) i Ministeri, i Dipartimenti, le Commissioni; c) gli Enti Pubblici non economici (INPS e INAIL); d) le ASL e le Agenzie delle Entrate; e) l'Autorità Giudiziaria; f) le Autorità di Vigilanza.

Le fattispecie di concussione, induzione indebita, corruzione, peculato e traffico di influenze illecite presuppongono, secondo la rispettiva struttura normativa, il coinvolgimento di un pubblico agente o di soggetti equiparati. Le qualifiche di Pubblico Ufficiale e di Incaricato di Pubblico Servizio sono definite dagli artt. 357 e 358 c.p.

Non è più richiamato il reato di abuso d'ufficio, abrogato dalla Legge n. 114/2024.
Tra le fattispecie penali qui considerate, i reati di concussione e di induzione indebita a dare o promettere utilità, nonché i reati di corruzione, nelle loro varie tipologie e i reati di "peculato" e di "abuso d'ufficio" presuppongono il coinvolgimento necessario di un pubblico agente, vale a dire di una persona fisica che assuma, ai fini della legge penale, la qualifica di "Pubblico Ufficiale" o di "Incaricato di Pubblico Servizio", nell'accezione rispettivamente attribuita dagli artt. 357 e 358 c.p.

IN PARTICOLARE:

- la qualifica di Pubblico Ufficiale è attribuita a coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. L'esercizio di una pubblica funzione amministrativa solitamente è riconosciuto sussistere in capo a coloro che formano o concorrono a formare la volontà dell'ente pubblico o comunque lo rappresentano di fronte ai terzi, nonché a coloro che sono muniti di poteri autoritativi o certificativi.
A titolo meramente esemplificativo si possono menzionare i seguenti soggetti, nei quali la giurisprudenza ha individuato la qualifica di Pubblico Ufficiale: ufficiale giudiziario, consulente tecnico del giudice, curatore fallimentare, esattore o dirigente di aziende municipalizzate anche se in forma di S.p.A., assistente universitario, portalettere, funzionario degli uffici periferici dell'Automobil Club d'Italia, consigliere comunale, geometra tecnico comunale, insegnante delle scuole pubbliche, ufficiale sanitario, notaio, dipendente dell'Istituto Nazionale della Previdenza Sociale, medico convenzionato con l'Azienda Sanitaria Locale, ecc.

- la qualifica di Incaricato di Pubblico Servizio è attribuita per via di esclusione, spettando a coloro che svolgono quelle attività di interesse pubblico, non consistenti in semplici mansioni d'ordine o meramente materiali, disciplinate nelle stesse forme della pubblica funzione, ma alle quali non sono ricollegati i poteri tipici del Pubblico Ufficiale. A titolo esemplificativo si elencano i seguenti soggetti nei quali la giurisprudenza ha individuato la qualifica di Incaricato di Pubblico Servizio: esattori dell'Enel, letturisti dei contatori di gas, energia elettrica, dipendente postale addetto allo smistamento ecc.

Quanto ai reati di cui agli artt. 25 e 25 ter del D.LGS. N. 231/2001 si analizzano di seguito:

- **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 OBIETTIVI DELLA PROCEDURA PER LA PREVENZIONE DEI REATI DI CORRUZIONE

La presente procedura, nell'ottica di attuare un effettivo contrasto al fenomeno corruttivo, ha i seguenti obiettivi:
1) vietare e contrastare la corruzione ed assicurare il raggiungimento della più elevata conformità agli standard normativi nazionali ed internazionali in materia di anticorruzione;
2) assicurare la sostenibilità, l'onestà e la trasparenza del business contrastando ogni fenomeno di malaffare;
3) contribuire alla diffusione della cultura di fare impresa sostenendo lealtà, integrità, onestà, concorrenza leale e trasparenza come elemento fondante del lavoro;
4) promuovere e sviluppare l'etica nelle relazioni economiche contrastando ogni forma di illegalità;

5) adottare ed attuare il sistema di gestione per la prevenzione della corruzione come strumento di effettivo contrasto ai fenomeni corruttivi, richiedendo un continuo impegno e *leadership* del Consiglio di Amministrazione e rafforzando il sistema dei controlli ad ogni livello aziendale;

6) sviluppare e diffondere la consapevolezza dell'impegno alla prevenzione ed alla lotta alla corruzione da parte di tutti gli *stakeholder*;

7) incoraggiare le segnalazioni di ogni sospetto di atto corruttivo tentato, certo, presunto mediante canali e modalità dedicate che, pur sempre in ossequio alla tutela della reputazione e dell'immagine della Società, permettano, da un lato, di svolgere indagini e approfondimenti al fine di valutare la fondatezza e approntare effettive misure di contrasto e, dall'altro, di garantire tutela al segnalante da ogni forma di ritorsione, nonché di tutela dei soggetti ingiustamente segnalati.

7 PRINCIPI DEL CODICE DI CONDOTTA ANTICORRUZIONE

BitControl S.r.l. richiede ai propri dipendenti e collaboratori di operare con costante onestà ed integrità. Il presente Codice di Condotta Anti-corruzione è stato redatto con lo scopo di proteggere i propri dipendenti da qualsivoglia violazione delle norme in materia di corruzione e si applica a tutti i dipendenti e a tutti gli altri soggetti che operano in nome e per conto di BitControl.

BitControl non ammette alcuna forma di corruzione e si impegna a rispettare le leggi anti-corruzione in vigore in tutti i paesi nei quali opera.

Lo scopo del Codice di Condotta è garantire i principi di trasparenza, assicurare la chiarezza nell'ambito dei comportamenti ammessi e la conformità alle relative normative anti-corruzione in qualsiasi luogo in cui BitControl svolga la propria attività, nonchè assicurare il mantenimento dei più elevati livelli di integrità.

Il Codice definisce, altresì, la politica di BitControl in merito alla ricezione e all'offerta di omaggi, ospitalità ed intrattenimenti, ovvero erogazioni gratuite di beni e servizi, a fini promozionali o di pubbliche relazioni.

BitControl ammette che l'elargizione e l'accettazione di omaggi, ospitalità e intrattenimenti possano verificarsi nello svolgimento delle consuete pratiche commerciali. Tuttavia, indipendentemente dalle disposizioni normative, determinati omaggi o atti di ospitalità possono essere interpretati come azioni svolte o subite da BitControl allo scopo di esercitare un'influenza inappropriata o possono indicare la presenza di un conflitto di

interesse. In particolare, in determinate circostanze l'offerta e/o la ricezione di omaggi e intrattenimenti possono essere considerate un atto di corruzione ed essere quindi illegali e lesivi della reputazione di BitControl, tanto che i soggetti coinvolti e la società potrebbero essere perseguiti penalmente.

Pertanto, a BitControl, ai suoi Dipendenti e/o ai Soggetti Terzi è fatto quindi divieto assoluto di elargire, promettere, offrire, richiedere o ricevere qualsivoglia omaggio, regalia, dono o ospitalità la cui natura o il cui valore possano essere ritenuti anche potenzialmente eccessivi o inusuali. Questo principio intende assicurare che nessun omaggio o atto di ospitalità ricevuto o elargito legittimamente possa essere considerato un reato di induzione volto a creare un vantaggio commerciale indebito per BitControl.

Il presente Codice definisce, inoltre, le linee guida per assicurare l'ottemperanza ai principi sopraccitati. Lo scopo del Codice è garantire che vengano rispettati i più elevati standard di integrità, tanto da non far sorgere alcun dubbio in ordine all'offerta o all'accettazione dell'omaggio o dell'atto di ospitalità, ovvero un'influenza indebita esercitata sul ricevente, o da parte del ricevente che accetti tale offerta. Il presente documento va considerato in combinato disposto con il Codice Etico di BitControl.

8 GESTIONE DEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

La presente procedura ha lo scopo di definire i principi comportamentali e deontologici cui tutto il personale della Società deve attenersi nella gestione dei rapporti e degli adempimenti verso i soggetti pubblici al fine di prevenire l'insorgenza di comportamenti corruttivi.

IN PARTICOLARE:

• gli adempimenti nei confronti della Pubblica Amministrazione e la predisposizione della relativa documentazione devono essere effettuati con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando e comunque segnalando, nella forma e nei modi idonei, situazioni di conflitto di interesse;

• i rapporti con i soggetti appartenenti alla Pubblica Amministrazione devono essere improntati a correttezza, trasparenza, collaborazione, disponibilità e al pieno rispetto del loro ruolo istituzionale, dando puntuale e sollecita esecuzione alle prescrizioni e agli adempimenti richiesti;

• il divieto di promettere od offrire beni e/o vantaggi a soggetti appartenenti alla Pubblica Amministrazione al fine di influenzarne l'autonomia di giudizio o di indurli a favorire ingiustificatamente i prodotti della Società;
• tutta la documentazione destinata alla Pubblica Amministrazione deve essere elaborata in modo puntuale ed in un linguaggio chiaro, oggettivo ed esaustivo ed essere verificata e sottoscritta da parte di responsabili di BITCONTROL coinvolti o da altro soggetto munito di idonei poteri delegati.

Nei rapporti con la Pubblica Amministrazione devono essere previamente individuati i soggetti autorizzati a rappresentare la Società. Gli incontri rilevanti sono, ove possibile, svolti con la presenza di almeno due esponenti aziendali e devono essere tracciati mediante verbale, nota interna, e-mail o altro documento equivalente, con indicazione di data, partecipanti, oggetto ed esito.

È vietato presentare dichiarazioni, attestazioni o documenti non veritieri, omettere informazioni dovute, alterare dati tecnici o economici, concordare offerte o condizioni con concorrenti, ottenere informazioni riservate, esercitare pressioni indebite o promettere vantaggi in relazione a gare, affidamenti, autorizzazioni, ispezioni, contributi, finanziamenti o contenziosi.

La documentazione predisposta con strumenti di Intelligenza Artificiale deve essere sottoposta a revisione umana integrale, verifica delle fonti e validazione del responsabile competente; è vietato utilizzare tali strumenti per generare contenuti falsi, alterare dichiarazioni o eludere obblighi di trasparenza, tracciabilità o dichiarazione previsti dalla disciplina di gara e dalle policy aziendali.

9 DONAZIONI, LIBERALITÀ, SPONSORIZZAZIONI, OMAGGI ED OSPITALITÀ

La presente procedura ha lo scopo di definire i ruoli, le responsabilità, i principi comportamentali cui il personale di BITCONTROL deve adottare nella gestione di donazioni, atti di liberalità, sponsorizzazioni offerte dalla società e omaggi erogati dalla Società a favore di terzi, sia su iniziativa della stessa Società che a seguito di richiesta di terzi. La procedura disciplina, altresì, le cortesie commerciali, stabilendone limiti e criteri autorizzativi.

Invero, così come previsto dalla procedura speciale del Modello di Gestione, Organizzazione e Controllo ex D.Lgs. 231/2001 adottato da BitControl S.r.l., la Società stabilisce che non è consentito corrispondere né offrire, direttamente o

indirettamente, pagamenti e benefici materiali di qualsiasi entità a terzi, pubblici ufficiali o privati, per influenzare o compensare un atto del loro ufficio. Ogni dipendente dovrà rifiutare omaggi o trattamenti di favore non direttamente ascrivibili a normali relazioni di cortesia. Omaggi e atti di cortesia e di ospitalità verso rappresentanti di governi, pubblici ufficiali e pubblici dipendenti possono essere consentiti solo quando siano di modico valore e comunque tali da non compromettere l'integrità o la reputazione di una delle parti e da non poter essere
intesi come finalizzati ad acquisire vantaggi in modo improprio.

IN PARTICOLARE È FATTO ESPRESSO DIVIETO DI:

1) non è ammesso promettere o offrire denaro, benefici, promesse di favori o altra utilità, anche se indirettamente per il tramite di un' interposta persona - come un consulente o un agente -, sia a soggetti appartenenti alla Pubblica Amministrazione, sia a soggetti privati con la finalità, anche indiretta, di acquisire trattamenti di favore per sé o per la Società;

2) che il dipendente non deve chiedere, sollecitare od accettare, per sé o per altri, denaro, regali o altre utilità, salvo gli omaggi di modico valore offerti occasionalmente nell'ambito delle normali relazioni di cortesia;

3) gli omaggi possono essere erogati a persone fisiche o Enti solitamente in occasione delle principali festività;

4) la Società non consente di corrispondere od offrire, direttamente o indirettamente, pagamenti e benefici di qualsiasi entità allo scopo di accelerare prestazioni già dovute alla Società.

Omaggi, ospitalità, spese di rappresentanza, liberalità e sponsorizzazioni devono avere finalità lecite, valore modico e proporzionato, essere coerenti con le normali relazioni istituzionali o commerciali, non essere in denaro o equivalenti, non coincidere con fasi decisionali sensibili e risultare preventivamente autorizzati e documentati secondo i livelli di delega vigenti.

Sono vietate erogazioni a favore di soggetti indicati o collegati, anche indirettamente, a pubblici ufficiali, clienti o partner quando possano essere interpretate come contropartita per un vantaggio indebito. Le sponsorizzazioni e liberalità richiedono verifica del beneficiario, assenza di conflitti di interesse, congruità dell'iniziativa, tracciabilità del pagamento e verifica dell'effettiva realizzazione.

10 COLLABORAZIONI ESTERNE E AFFIDAMENTO DI INCARICHI A DIPENDENTI O EX DIPENDENTI DELLA PUBBLICA AMMINISTRAZIONE

La presente procedura definisce l'iter autorizzativo per le collaborazioni esterne e per l'assegnazione di incarichi a dipendenti della Pubblica Amministrazione o comunque a terzi operanti con organismi pubblici.

La procedura e le modalità operative previste garantiscono una corretta e trasparente gestione dei rapporti con i collaboratori esterni della BITCONTROL, riducendo il rischio di commissione dei reati ed in particolare quelli di corruzione.

Il ricorso a collaborazioni esterne deve essere limitato ai casi nei quali le stesse siano strettamente necessarie e la relativa prestazione deve essere di natura temporanea e altamente qualificata.

L'individuazione e la valutazione del collaboratore deve essere preceduta da un giudizio sulla sussistenza dei requisiti di onorabilità, professionalità e idoneità dello stesso, oltre che da motivate esigenze della prestazione, verificando che non sussistano divieti o limiti al conferimento dell'incarico, effettuando una due diligence ed un'analisi del curriculum.

Deve, inoltre, essere acquisita una dichiarazione del collaboratore in tema di conflitto di interessi, di assenza di cause di inconferibilità e incompatibilità rispetto alla normativa applicabile e di impegno al rispetto dei principi etici e del Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs 231/01 della società.

A seconda dell'oggetto e del valore della prestazione la società ha definito diversi livelli di autorizzazione che possono coinvolgere, il Legale Rappresentante, i componenti del Consiglio di Amministrazione ed i soggetti a cui è stata conferita apposita delega o procura.

L'accordo contrattuale deve prevedere una durata definita, un corrispettivo congruo, modalità di pagamento in linea con la normativa in materia, la consegna di output specifici o avanzamenti verificabili.

Viene inoltre prevista una clausola risolutiva espressa nei casi in cui il soggetto abbia fornito dichiarazioni/autocertificazioni in relazione all'incarico non veritiere e nel caso in cui ci sia inosservanza del Modello di organizzazione, gestione e controllo ex D. Lgs. 231/01 di BITCONTROL.

Il conferimento di un incarico di collaborazione esterna professionale in favore di dipendenti ed ex dipendenti della Pubblica Amministrazione ovvero di Persone Giuridiche/Altre Entità Giuridiche che impiegano ex dipendenti della Pubblica Amministrazione è consentito:

• per i dipendenti della Pubblica Amministrazione se in possesso di regolare autorizzazione rilasciata dalla stessa, oppure per i dipendenti esonerati dal richiedere l'autorizzazione;
• per gli ex dipendenti della pubblica amministrazione nel caso che la prestazione sia considerata indispensabile per il perseguimento degli interessi della società. In tale caso occorre verificare la sussistenza delle condizioni previste dalla legge (cessazione del rapporto di pubblico impiego da oltre tre anni, oppure mancato esercizio negli ultimi tre anni di servizio di poteri autoritativi o negoziali nei confronti di BITCONTROL). L'assegnazione dell'incarico è sottoposta all'approvazione del Legale Rappresentante.

Regole analoghe vengono seguite anche nell'ipotesi di instaurazione di rapporti di attività lavorativa o professionale in favore di dipendenti ed ex dipendenti della Pubblica Amministrazione.

L'ente richiedente la collaborazione ha la responsabilità di monitorare periodicamente le prestazioni e garantire il rispetto dei tempi e dei costi originariamente stabiliti, e sulla base di tale attività di verifica e monitoraggio viene rilasciato il benestare a procedere al pagamento del collaboratore esterno.

Prima dell'affidamento devono essere svolte verifiche proporzionate al rischio sulla reputazione, titolarità effettiva ove rilevante, competenza, esperienza, eventuali rapporti con soggetti pubblici, conflitti di interesse, sanzioni o procedimenti noti e ragionevolezza del compenso. L'esito delle verifiche deve essere documentato e aggiornato nei rapporti continuativi.

I contratti con consulenti, intermediari, partner, fornitori e subappaltatori devono contenere clausole di rispetto del Codice Etico, del Modello 231 e della Politica Anticorruzione, obblighi di tracciabilità e cooperazione con i controlli, nonché clausole risolutive e rimedi contrattuali in caso di violazione.

In applicazione dell'art. 53, comma 16-ter, D.Lgs. 165/2001, è vietato instaurare rapporti di lavoro o professionali con ex dipendenti pubblici che, negli ultimi tre anni di servizio, abbiano esercitato poteri autoritativi o negoziali nei confronti di BITCONTROL, per i tre anni successivi alla cessazione del rapporto. La verifica è documentata mediante apposita dichiarazione e controlli ragionevoli.

11 CONFLITTI DI INTERESSE

La presente procedura stabilisce i requisiti per individuare e gestire eventuali conflitti di interesse, reali o potenziali. Inoltre, individua i principi di comportamento a cui ciascun

dipendente deve attenersi nell'ambito delle proprie mansioni ed in particolare nella gestione dei rapporti verso terzi.

Per conflitto di interessi s'intende una qualsiasi situazione in cui l'interesse personale o l'attività di un individuo interferisce o potrebbe interferire con gli interessi della Società.

Una situazione di conflitto si può verificare quando un dipendente pone in essere un'azione o è soggetto ad interessi che interferiscono con la sua capacità di svolgere in maniera imparziale ed efficace i suoi compiti.

Ogni situazione che possa costituire o determinare un conflitto di interessi deve essere tempestivamente comunicata al responsabile amministrativo, il quale, esaminate le circostanze, valuta se la situazione realizza un conflitto di interesse idoneo a ledere l'imparzialità dell'agire amministrativo.

A titolo esemplificativo ma non esaustivo, determinano conflitti di interesse le seguenti situazioni:

• interessi economici e finanziari del dipendente e/o il coniuge, i propri parenti e gli affini entro il 2° grado, i conviventi di fatto e coloro che rientrano nella sua sfera affettiva, in attività di fornitori, clienti e concorrenti;

• utilizzo della propria posizione in azienda o delle informazioni acquisite nel proprio lavoro in modo che si possa creare conflitto tra i propri interessi personali e gli interessi aziendali;

• rapporti esistenti tra dipendenti legati da rapporti gerarchici (il coniuge, i propri parenti e gli affini entro il 2° grado, i conviventi di fatto e coloro che rientrano nella sua sfera affettiva);

• svolgimento di attività lavorative, di qualsiasi tipo, presso clienti, fornitori, concorrenti;

• accettazione di denaro, favori o utilità da persone o aziende che sono o intendono entrare in rapporti di affari con BITCONTROL.

Il soggetto in conflitto, anche solo potenziale o apparente, deve effettuare tempestiva dichiarazione scritta e astenersi da ogni valutazione, decisione, negoziazione o controllo relativo alla situazione segnalata. La funzione competente definisce le misure di gestione, che possono includere sostituzione, supervisione rafforzata, segregazione dei compiti o esclusione dal processo.

Le dichiarazioni sui conflitti di interesse devono essere rinnovate periodicamente e in occasione di mutamenti rilevanti, assunzioni, affidamenti di incarichi, gare, partnership e operazioni con parti correlate.

12 PREVENZIONE REATI SOCIETARI - ADEMPIMENTI IN MATERIA DI BILANCI E DI DELIBERE SOCIALI IN APPLICAZIONE DEL D. LGS. 231/01

La presente procedura ha lo scopo di evidenziare compiti, responsabilità e principi di comportamento da porre in essere nelle attività di predisposizione dei Bilanci e delle delibere sociali e nei rapporti con i soci e con le Autorità Pubbliche di vigilanza.
In particolare, i principi comportamentali previsti dalla presente procedura sono di seguito indicati:

1) nella gestione delle attività contabili devono essere osservate scrupolosamente le regole di corretta, completa e trasparente contabilizzazione, secondo i criteri indicati dalla Legge e dai principi contabili
applicabili, in modo tale che ogni operazione sia autorizzata, verificabile, legittima, coerente e congrua;

2) la correttezza del processo di registrazione e l'accuratezza delle transazioni che confluiscono in bilancio devono essere verificate dai responsabili competenti per voce di bilancio, attraverso i controlli previsti dalle procedure amministrative e contabili;

3) le registrazioni contabili possono essere effettuate esclusivamente dai soggetti abilitati ed i livelli autorizzativi sono determinati e rivisti secondo quanto previsto dalle procedure aziendali;

4) durante lo svolgimento delle attività di verifica e controllo da parte dei Soci o dalle Autorità Pubbliche di Vigilanza è necessario agire con trasparenza e prestare la massima collaborazione;

5) le operazioni straordinarie devono essere poste in essere nel rispetto della disciplina prevista dal Codice Civile, dalle disposizioni di Legge e dalle procedure aziendali.

13 GESTIONE CONTROLLI FINANZIARI E CONTABILI

BITCONTROL garantisce l'accuratezza, la completezza e la tempestività delle transazioni finanziarie e contabili. Ogni operazione deve essere autorizzata, giustificata, congrua, verificabile e supportata da idonea documentazione. Sono applicati la segregazione dei compiti, livelli autorizzativi differenziati, la verifica del beneficiario e dell'IBAN, il divieto di conti o fondi non registrati, la limitazione del contante nei limiti aziendali e di legge, la riconciliazione periodica e audit finanziari. Sono vietati pagamenti a soggetti diversi dalla controparte contrattuale, su conti

non riconducibili alla stessa o in Paesi non coerenti con l'operazione, salvo motivata autorizzazione e verifica rafforzata.

14 ASSUNZIONE E GESTIONE DEL PERSONALE

BITCONTROL garantisce specifici percorsi di selezione, assunzione e passaggi di carriera, garantendo trasparenza, imparzialità e tracciabilità di tutte le attività poste in essere. I processi di selezione, assunzione e gestione del personale devono essere svolti nel rispetto di quanto previsto dalle procedure aziendali e dalle normative applicabili e, nello specifico, in riferimento alla verifica di aspetti reputazionali e di conflitto di interessi in fase di assunzione. Nella fase di gestione del rapporto di lavoro è richiesto il rispetto di tutta la normativa applicabile, con riferimento in particolare agli aspetti di remunerazione della prestazione lavorativa, inclusa, la definizione/assegnazione di sistemi di incentivazione.

La componente fissa della retribuzione viene determinata dal CCNL di riferimento, tenendo conto dell'esperienza e delle competenze, dell'anzianità di servizio ed in particolare degli obiettivi aziendali perseguiti.

È vietata l'assunzione, la promessa di assunzione, la progressione, l'attribuzione di premi o altri vantaggi a candidati o dipendenti segnalati da pubblici ufficiali, clienti, fornitori o partner quale contropartita per favori o vantaggi indebiti. Le decisioni devono fondarsi su criteri oggettivi, documentati e coerenti con le esigenze organizzative.

Per i ruoli maggiormente esposti al rischio corruzione sono previste formazione periodica, dichiarazioni sui conflitti di interesse e, ove proporzionato, verifiche reputazionali nel rispetto della normativa applicabile.

15 RAPPORTI CON IL PARTNER

BITCONTROL garantisce che il processo di selezione e scelta di un Partner sia preceduta da adeguati controlli finanziari e non finanziari, ovvero un controllo sull'etica e sulla reputazione, verificando che il processo di contrattualizzazione sia improntato al principio di trasparenza, tracciando le operazioni ed il processo di

elaborazione di applicazione di condizioni particolari e di gestione dei crediti nel corso del rapporto.

La due diligence deve essere commisurata al livello di rischio e comprendere, ove pertinente, assetto proprietario, titolare effettivo, reputazione, competenze, eventuali rapporti con pubblici ufficiali, conflitti di interesse, provenienza delle risorse, capacità economico-finanziaria e precedenti violazioni. Le condizioni economiche devono essere congrue e i pagamenti correlati a prestazioni effettive e verificabili.

Nei raggruppamenti, reti, consorzi, subappalti e partnership per gare pubbliche sono vietati accordi collusivi, scambi di informazioni sensibili sulle offerte, ripartizioni concordate del mercato, compensi non giustificati e qualsiasi intesa volta ad alterare la concorrenza o l'esito della procedura.

16 SEGNALAZIONI E WHISTLEBLOWING

BITCONTROL garantisce, in conformità al D.Lgs. 24/2023 e alla Procedura Whistleblowing vigente, canali interni che assicurano la riservatezza dell'identità del segnalante, della persona coinvolta e del contenuto della segnalazione. Possono essere segnalati atti corruttivi sospettati, tentati o consumati, violazioni del Codice Etico, del Modello 231, della Politica Anticorruzione, delle Misure Integrative e della presente procedura.

Le segnalazioni devono essere effettuate attraverso i canali e secondo le modalità indicati nella Procedura Whistleblowing tempo per tempo vigente, alla quale si rinvia integralmente. La gestione è affidata al soggetto formalmente individuato dalla Società, con garanzia di autonomia, imparzialità, riservatezza e tracciabilità.

I canali interni consentono la segnalazione in forma scritta e orale e, su richiesta, mediante incontro diretto, nel rispetto dei requisiti normativi e organizzativi applicabili.

Le segnalazioni anonime sono trattate quando sufficientemente circostanziate. È vietata ogni ritorsione, minaccia o discriminazione nei confronti del segnalante e degli altri soggetti protetti dalla legge. Restano ferme le responsabilità per segnalazioni scientemente false, diffamatorie o calunniose, secondo quanto previsto dalla legge e dal sistema disciplinare.

BITCONTROL garantisce, in coerenza con la *policy di Whistleblowing*, la possibilità di effettuare segnalazioni di ogni atto corruttivo sospettato, tentato, certo, presunto, nonché di ogni eventuale violazione dei principi stessi nel Codice Etico, della Politica Anti-corruzione e della presente procedura.

Pertanto, qualora un Destinatario abbia il ragionevole sospetto che si sia verificato o che possa verificarsi un Comportamento illecito, può comunicarlo all'ODV, attraverso la compilazione dell'apposito modulo di cui all'Allegato A della Procedura Interna di Segnalazione di Whistleblowing, utilizzando uno dei seguenti canali:

a) comunicazione inviata tramite posta elettronica crittografata, fuori dai server aziendali, all'indirizzo dedicato al Whistleblowing, gestito esclusivamente dall'Organismo di Vigilanza, a tutela della riservatezza del Segnalante contenente i dati identificativi (parte I del modulo di cui all'Allegato A) del Segnalante: organismodivigilanza@bitcontrol.it.

b) lettera recapitata in busta chiusa indirizzata presso la sede legale della Società in via Stazione n. 39, 95047, Paternò (CT), indirizzata all'attenzione dell'Organismo di Vigilanza con la dicitura "RISERVATA PERSONALE"; all'interno della busta contenente la Segnalazione deve essere inserita un'altra busta che può contenente i dati identificativi (parte I del modulo di cui all'Allegato A) del Segnalante. Tale busta deve essere tempestivamente recapitata all'OdV, il quale provvederà a conservarla ed archiviarla sotto la propria responsabilità.

c) lettera recapitata in busta chiusa indirizzata presso il domicilio eletto dall'ODV in via E. Bellia n. 35, 95047, Paternò (CT), indirizzata all'attenzione dell'Organismo di Vigilanza con la dicitura "RISERVATA PERSONALE"; all'interno della busta contenente la Segnalazione deve essere inserita un'altra busta che può contenente i dati identificativi (parte I del modulo di cui all'Allegato A) del Segnalante. In tal caso, l'OdV, provvederà a conservarla ed archiviarla sotto la propria responsabilità.

Le segnalazioni possono essere effettuate anche in forma anonima e, qualora, il segnalante si identifichi, le segnalazioni sono trattate in modo confidenziale, al fine di proteggere l'identità del segnalante e di coloro che risultano coinvolti nella segnalazione.

Nei confronti del segnalante in buona fede, o di colui che segnala sulla base di convinzioni ragionevoli, non è consentita alcuna forma di ritorsione o discriminazione per motivi collegati alla denuncia, intendendo con misure discriminatorie qualsiasi azione disciplinare ingiustificata, le molestie sul luogo di lavoro, il licenziamento, i cambi di mansione e ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili o anche più semplicemente gravose.

E', tuttavia, fermamente vietata ogni forma di abuso della segnalazione quali a titolo meramente significativo e non esaustivo la volontà di accusare falsamente una persona, l'utilizzo improprio o di intenzionale strumentalizzazione di tale istituto; in ordine alle citate condotte la società si riserva di agire nei confronti di coloro che le pongono in essere, poiché l'abuso del sistema di segnalazione rischia concretamente di inficiare l'intero sistema di gestione e la sua reale funzione.

17 SISTEMA SANZIONATORIO

La commissione di atti in violazione della presente procedura nonché, più in generale, la violazione delle norme per la prevenzione della corruzione e l'abuso delle attività di segnalazione, costituisce inadempienza agli obiettivi contrattuali e al rispetto delle regole aziendali e dà corso all'avvio di procedimenti disciplinari per l'irrogazione di sanzioni così come previste nel sistema aziendale oltre che alle possibili conseguenze di natura penale e civile.

18 COMUNICAZIONE, DIFFUSIONE E DIVULGAZIONE

La Politica Anticorruzione, il Codice Etico, le Misure Integrative e la presente procedura sono comunicate e rese disponibili a tutti i Destinatari con modalità adeguate al ruolo e al rischio. BITCONTROL assicura formazione iniziale e periodica, con particolare attenzione ai soggetti operanti nelle gare, nei rapporti con la Pubblica Amministrazione, negli acquisti, nella selezione del personale, nella gestione finanziaria, nelle sponsorizzazioni e nei rapporti con terze parti. La partecipazione e l'efficacia della formazione sono documentate e verificate.

L'efficacia dei presidi è riesaminata mediante controlli periodici, audit, analisi dei flussi informativi, indicatori di anomalia, esiti delle segnalazioni e verifica dell'attuazione delle azioni correttive. Ove la rotazione del personale non sia concretamente attuabile, sono rafforzati segregazione dei compiti, doppia verifica, tracciabilità e supervisione.

18 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Le funzioni aziendali competenti trasmettono tempestivamente all'Organismo di Vigilanza le anomalie, le violazioni e gli eventi rilevanti ai fini della presente procedura. Devono essere inoltre messi a disposizione, con periodicità definita nei flussi informativi 231, dati e documenti relativi almeno a: gare e affidamenti rilevanti; rapporti e incontri significativi con la Pubblica Amministrazione; omaggi, sponsorizzazioni e liberalità; incarichi a consulenti e intermediari; assunzioni o collaborazioni di ex dipendenti pubblici; conflitti di interesse; operazioni finanziarie anomale; contestazioni, indagini, ispezioni, segnalazioni e procedimenti disciplinari in materia anticorruzione.

Tutti i *Destinatari* coinvolti e, precisamente coloro che hanno rilevato una situazione anomala o una violazione del Modello, sono tenuti ad informare tempestivamente l'Organismo di Vigilanza delle situazioni anomale e/o effettuate in contrasto con la presente procedura, nonché eseguite in violazione delle disposizioni del Modello, del Codice Etico e della Politica Anticorruzione.

In ogni caso, 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.

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA del 14.11.2020	ADOZIONE
Rev. 1	CDA del 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA del 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA del 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA del 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA del 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	ADOZIONE

SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

La presente procedura disciplina la gestione, l'accesso, l'utilizzo, il controllo e il monitoraggio dei sistemi di intelligenza artificiale autorizzati da BITCONTROL, 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
RAM/RRU	Responsabile Amministrazione - Risorse Umane
RCOM/APVG	Responsabile Commerciale
RATTR	Responsabile Attrezzature e Mezzi
CDL	Consulente del Lavoro
REC	Responsabile Esterno Contabilità
RIA	Responsabile IA
RIDC	Responsabile interno di conformità

LE SUDDETTE ABBREVIAZIONI CORRISPONDONO ALLE FUNZIONI INDICATE E AI RELATIVI SOGGETTI AFFIDATARI, PER LA CUI IDENTIFICAZIONE SI RIMANDA ALL'ORGANIGRAMMA AZIENDALE DI BITCONTROL S.R.L..

3 RIFERIMENTI NORMATIVI DEL MODELLO

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 BITCONTROL 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 BITCONTROL) 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 BITCONTROL, 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 BITCONTROL. 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), con particolare riguardo ai limiti dei controlli a distanza e alla tutela della dignità e riservatezza dei lavoratori.

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 BITCONTROL S.R.L.

- MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 231/01 (PARTE GENERALE E SPECIALE).

- POLITICA IA DI BITCONTROL S.R.L.;

- PMOG 08 "GESTIONE PER LA PREVENZIONE DEI REATI INFORMATICI E DI INDEBITO UTILIZZO DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI";

- PMOG 11 "GESTIONE E UTILIZZO OPERE DELL'INGEGNO";

- PROCEDURE AZIENDALI IN MATERIA DI PRIVACY, SICUREZZA DELLE INFORMAZIONI, GESTIONE INCIDENTI, BUSINESS CONTINUITY, DISASTER RECOVERY, GARE, FLUSSI INFORMATIVI E WHISTLEBLOWING.

4 CAMPO DI APPLICAZIONE E DESTINATARI DELLA PROCEDURA

La presente Procedura si applica a tutti coloro che agiscono in nome e per conto di BITCONTROL 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 BITCONTROL 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: BITCONTROL, 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, codice sorgente, logiche di automazione, configurazioni SCADA/PLC/RTU/DCS, credenziali, chiavi e token, architetture IT/OT e di rete, dati di processo, dati economici riservati, informazioni relative a clienti, impianti e commesse pubbliche o private 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.

In particolare, i principi cardine possono essere articolati come segue:

6.1. PRINCIPIO DI SUPERVISIONE UMANA SIGNIFICATIVA E RESPONSABILITÀ PROFESSIONALE:

Questo è il principio fondamentale che governa l'intero ecosistema IA di BITCONTROL. 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 BITCONTROL) 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 BITCONTROL:

Progettazione, automazione e telecontrollo: qualsiasi architettura di sistema, logica di automazione, configurazione, schema funzionale, specifica tecnica, analisi di processo o proposta relativa a sistemi SCADA, PLC, RTU, DCS, telemetria e IoT generata con il supporto dell'IA deve essere considerata una bozza preliminare. Il Responsabile Tecnico o il Responsabile Progettazione ha l'obbligo di verificarla, validarla e, ove necessario, rielaborarla autonomamente prima dell'impiego in commessa o della sottoscrizione. L'output IA non può mai costituire l'elaborato tecnico definitivo.

Sviluppo software e integrazione di sistemi: il codice, gli script, le query, le configurazioni o le proposte di integrazione generate con il supporto dell'IA devono essere sottoposti a code review, test, debug, verifica delle dipendenze e controllo di sicurezza da parte degli sviluppatori e dei responsabili tecnici. La responsabilità della sicurezza, dell'efficienza e della correttezza funzionale del software e delle configurazioni finali ricade interamente sul personale BITCONTROL e non può essere delegata all'IA.

6.2. 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 BITCONTROL - 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.

6.3 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 BITCONTROL:

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 BITCONTROL 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 BITCONTROL o per i suoi clienti.

6.4. PRINCIPIO DI TRASPARENZA E RESPONSABILITÀ CONTRATTUALE

BITCONTROL 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 BITCONTROL:

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 BITCONTROL 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.

6.5. USI CONSENTITI

L'utilizzo dei sistemi di intelligenza artificiale è consentito esclusivamente per finalità aziendali inerenti alle mansioni assegnate, mediante account aziendali nominativi e nei limiti delle

autorizzazioni rilasciate. In conformità alla Politica IA, BITCONTROL autorizza l'uso della sola piattaforma ChatGPT nella versione Business subscription o di eventuali ulteriori strumenti previamente valutati e approvati per iscritto dal Responsabile IA/IT e dalla Società. È vietato l'uso di account personali o di piattaforme non approvate per attività aziendali.

In coerenza con le attività svolte da BITCONTROL nei settori dell'automazione industriale, del telecontrollo, della telemetria e IoT, della progettazione e integrazione di sistemi SCADA, PLC, RTU e DCS, dello sviluppo software, della gestione di dati e database, dell'assistenza e manutenzione e della predisposizione di offerte tecniche, i sistemi di IA possono essere utilizzati, quali strumenti meramente preparatori e di supporto, per:

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 BITCONTROL 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.

6.6. 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.

7. PROPRIETÀ INTELLETTUALE, OPERE DELL'INGEGNO E SEGRETI COMMERCIALI

7.1 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 BITCONTROL, 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.

7.2 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 BITCONTROL, 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) BITCONTROL 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 BITCONTROL, che regolano i rapporti con i clienti in ordine ai diritti sugli elaborati prodotti nell'ambito delle commesse.

7.3 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.

7.4 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 BITCONTROL – 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.

7.5 TUTELA DEI SEGRETI COMMERCIALI E DEL KNOW-HOW AZIENDALE

Costituiscono segreti commerciali di BITCONTROL, 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:

le metodologie proprietarie di progettazione, programmazione, integrazione, collaudo, manutenzione e gestione dei sistemi di automazione, supervisione e telecontrollo;

gli algoritmi e gli strumenti software sviluppati internamente;
le specifiche tecniche dei sistemi SIT realizzati per i clienti;
i dati tecnici, le architetture, le configurazioni di rete, i parametri di processo e le informazioni relative alle infrastrutture e agli impianti dei clienti;
le strategie commerciali, le condizioni economiche delle offerte, i dati di gara;
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.

7.6 RAPPORTI CON FORNITORI E SUBFORNITORI

Nei rapporti con fornitori di componenti software, dataset, modelli di IA o servizi cloud, BITCONTROL deve formalizzare per iscritto le condizioni di utilizzo dei dati e degli output, con particolare attenzione a:
titolarità e licenza degli output e dei modelli prodotti o sviluppati nell'ambito della commessa;
divieto di utilizzo dei dati aziendali per l'addestramento del modello del fornitore;
obblighi di riservatezza e di non-divulgazione dei segreti commerciali di BITCONTROL e dei suoi clienti;
audit rights e diritto di verifica del rispetto delle condizioni contrattuali;
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.

7.7 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:
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;
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.);

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.;
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.

7.8 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.

8. 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 BITCONTROL 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.

9. VALUTAZIONE PREVENTIVA E AUTORIZZAZIONE D'USO

9.1 FINALITÀ E AMBITO DEL PARAGRAFO

L'utilizzo di qualsiasi sistema di intelligenza artificiale da parte del personale di BITCONTROL 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 BITCONTROL e dei suoi clienti.

9.2 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.

riceve le richieste di accesso ai sistemi IA;
verifica la sussistenza dei requisiti tecnici, organizzativi e giuridici;
approva o rigetta la richiesta, anche su parere delle funzioni di controllo;
gestisce il registro degli utenti autorizzati;
revoca o sospende le autorizzazioni in caso di violazione, cessazione del rapporto o mutamento del contesto di rischio.

L'AUTORIZZAZIONE HA CARATTERE:

personale: non è cedibile né condivisibile con altri soggetti;
limitato: circoscritto alle finalità, agli strumenti e ai dati indicati nel documento di autorizzazione;
revocabile: può essere sospesa o revocata in qualsiasi momento al ricorrere dei presupposti;
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:

supervisione umana e validazione degli output;
rispetto dei divieti procedurali;
tutela della riservatezza e dei segreti commerciali;
osservanza della normativa sulla proprietà intellettuale;
segnalazione di anomalie, incidenti o violazioni.

9.3 RIESAME PERIODICO DELLE AUTORIZZAZIONI

Le autorizzazioni rilasciate devono essere soggette a riesame periodico, con cadenza almeno annuale, e comunque in occasione di:
variazione delle mansioni o del ruolo dell'utente;
aggiornamento degli strumenti IA autorizzati o modifica dei termini di servizio del fornitore;
variazione del contesto operativo o della commessa di riferimento;
rilevazione di un incidente di sicurezza o di una violazione della presente procedura;
aggiornamento normativo rilevante;
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.

9.4 REVOCA E SOSPENSIONE DELL'AUTORIZZAZIONE

L'autorizzazione è revocata o sospesa con effetto immediato nei seguenti casi:
violazione accertata o anche solo sospettata della presente procedura o della Policy IA;

utilizzo dello strumento per finalità diverse da quelle autorizzate;
inserimento di dati vietati nei prompt del sistema IA;
incidente di sicurezza riconducibile all'uso del sistema;
cessazione del rapporto lavorativo o di collaborazione;
indisponibilità o revoca della formazione obbligatoria;
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.

10. 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: architetture di automazione e telecontrollo, schemi funzionali, logiche di controllo, configurazioni SCADA/PLC/RTU/DCS, specifiche di comunicazione M2M e IoT, report di collaudo, manuali e documentazione di commessa.

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 BITCONTROL: 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.

10.1 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.

11. Gare pubbliche e contratti

Per i servizi di natura intellettuale, la procedura deve recepire integralmente le dichiarazioni richieste da ANAC, distinguendo:

mancato uso dell'IA;

uso dell'IA nella redazione dell'offerta tecnica;

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:

conservazione della documentazione per almeno 5 anni;

tracciabilità dei prompt/output rilevanti;

prevalenza del lavoro umano;

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 BITCONTROL 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.

11-BIS. GESTIONE DELL'IA NELLE PROCEDURE DI GARA PUBBLICA E NEGLI APPALTI

11-BIS.1 AMBITO E FINALITÀ DEL CAPITOLO

Il presente capitolo disciplina le modalità operative con cui BITCONTROL 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 BITCONTROL.

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.

11-BIS.2 PRINCIPI APPLICABILI ALLE GARE PUBBLICHE

In coerenza con la normativa vigente, l'uso dell'IA nelle attività di gara di BITCONTROL 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: BITCONTROL 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).

11- BIS.3 ATTIVITÀ CONSENTITE E ATTIVITÀ VIETATE NELLA PREDISPOSIZIONE DELL'OFFERTA

11-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.

11-BIS.3.2 ATTIVITÀ VIETATE

È fatto espresso divieto di utilizzare l'IA per:

1. la generazione automatica di elaborati tecnici vincolanti (architetture di sistema, logiche di automazione, configurazioni SCADA/PLC/RTU/DCS, specifiche di rete, relazioni di collaudo o manuali operativi), anche parziale, senza revisione critica documentata del responsabile tecnico competente;

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 manipolazione di immagini, video, sinottici, interfacce HMI, schemi funzionali, diagrammi di rete o altri elaborati grafici tecnici senza validazione del responsabile competente.

11-BIS.4 DICHIARAZIONI OBBLIGATORIE IN GARA: SCHEMA OPERATIVO

11-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:

«BITCONTROL 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):

«*BITCONTROL 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):

«*BITCONTROL 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, BITCONTROL 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:

«*BITCONTROL 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).*»

11-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.

11-BIS.6 OBBLIGHI DI TRACCIABILITÀ E CONSERVAZIONE

11-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.

11-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.

11-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.

11-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 BITCONTROL 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:

la corretta tenuta del Registro gare con uso IA;

la conformità delle dichiarazioni rese nelle offerte rispetto all'effettivo utilizzo documentato dell'IA;

la completezza della documentazione di verifica pre-offerta e della documentazione di validazione tecnica;

la regolarità dei flussi informativi ricevuti dal RAM in ordine agli eventi rilevanti;

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.»

11-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.

12. 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 BITCONTROL, 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:

escalation interna tempestiva;

sospensione dell'uso del sistema in caso di rischio;

gestione dell'incidente secondo i playbook cyber aziendali;
eventuale notifica al Garante entro 72 ore nei casi di data breach;
eventuale segnalazione al CSIRT Italia per incidenti significativi.

12.1 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.

12.2 INCIDENTI PRIVACY E CONFIDENZIALITÀ

COMPRENDONO:

inserimento nei prompt di dati personali o riservati non anonimizzati;
fuga di dati verso provider esterni;
output contenenti dati di clienti, dipendenti, reti infrastrutturali o informazioni tecniche riservate;
conservazione impropria di conversazioni o file allegati.

12.3 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 BITCONTROL questo punto è particolarmente critico, poiché un output errato può incidere sulla sicurezza e continuità dei sistemi di automazione e telecontrollo, sulle logiche di processo, sulle configurazioni SCADA/PLC/RTU/DCS, sull'integrazione di database e reti, sui collaudi e sulle specifiche tecniche di commessa.

12.4 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.

13. 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

13.1 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.

13.2 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.

13.3 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.

14. MONITORAGGIO, AUDIT E FLUSSI VERSO ODV

14.1 FINALITÀ E AMBITO

Il presente paragrafo definisce il sistema di monitoraggio e controllo sull'utilizzo dei sistemi di Intelligenza Artificiale (IA) autorizzati in BITCONTROL S.r.l., con lo scopo di:

verificare il rispetto delle disposizioni della presente Procedura e della Policy IA aziendale;

garantire la tracciabilità degli accessi, dei prompt, degli output e delle validazioni effettuate;

assicurare flussi informativi strutturati e tempestivi verso l'Organismo di Vigilanza (OdV) e il Consiglio di Amministrazione (CDA);

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.

14.2 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:

pianifica e supervisiona l'esecuzione dei controlli periodici di cui ai punti 16.3 e 16.4;

raccoglie e analizza gli esiti delle verifiche;

predispone il reporting periodico verso OdV e CDA;

gestisce le segnalazioni di anomalie, incidenti e non conformità;

funge da punto di contatto operativo per OdV e DPO in materia di sistemi IA;

propone misure correttive e ne monitora l'attuazione.

B) FUNZIONE IT/SICUREZZA INFORMATICA

Supporta il Responsabile IA nelle verifiche tecniche, assicurando in particolare:

estrazione e messa a disposizione dei log di sistema;

controllo sugli account attivi, sulle credenziali, sui privilegi e sull'autenticazione a più fattori (MFA);

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.

14.3 CONTROLLI PERIODICI: TIPOLOGIA, CONTENUTO E PERIODICITÀ

14.3.1 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.

14.3.2 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:

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;
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;
ogni consultazione dei log deve essere essa stessa tracciata, con registrazione del soggetto, della data e della finalità della consultazione;
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.

14.3.3 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 rilevanti (architetture di automazione, logiche di controllo, configurazioni SCADA/PLC/RTU/DCS, codice sorgente, specifiche di comunicazione, manuali e 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.

14.3.4 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. 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 allo sviluppo software, all'integrazione di database, alla telemetria, all'IoT, ai dati di processo e alle basi di conoscenza tecniche;
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 di schemi, manuali, librerie software, database, dati di processo, configurazioni e documentazione tecnica eventualmente impiegati nei sistemi IA nell'ambito delle attività di automazione e telecontrollo.

EVIDENZA DOCUMENTALE: verbale di audit licenze/dati, con check-list e documentazione contrattuale allegata; conservato nel Registro Audit IA.

14.4 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.

14.5 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".*

14.6 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.

14.7 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.

14.8 RINVIO ALLE PROCEDURE DI FLUSSO INFORMATIVO E WHISTLEBLOWING

Per le modalità operative di comunicazione e segnalazione all'OdV si rinvia alle procedure aziendali:

"Flussi informativi verso l'Organismo di Vigilanza ex D.Lgs. 231/01";

"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.

14.9 DISPOSIZIONI FINALI

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.

COSTITUISCE PARTE INTEGRANTE DEL PRESENTE MODELLO 231/01 LA PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING E L'ALLEGATO MODULO PER LA SEGNALAZIONE DI CONDOTTE ILLECITE O VIOLAZIONI DEL MEDESIMO MODELLO.

CODICE ETICO

Il presente Codice Etico è stato approvato con delibera del 25.06.2026 dal Consiglio di Amministrazione di BitControl S.r.l.

Sommario

PREMESSA

OBIETTIVI DELLA BITCONTROL S.R.L.

La BitControl S.r.l. è una società che si occupa di progettazione, sviluppo, assistenza e manutenzione di soluzioni informatiche per sistemi di telecontrollo. Al fine di migliorare le prestazioni offerte ed affermarsi nel settore di riferimento a livello nazionale ed internazionale, la BitControl S.r.l. ha individuato i seguenti obiettivi:

- diffondere il proprio Codice etico e la propria politica aziendale a tutte le parti interessate: (operatori aziendali e responsabili di processo, fornitori, partners ed altri soggetti esterni);
- coinvolgere tutti gli addetti nell'individuazione delle esigenze implicite ed espresse del Cliente;
- sensibilizzare, coinvolgere e motivare il personale verso la condivisione ed il perseguimento degli specifici obiettivi di processo;
- ricercare il miglioramento continuo delle prestazioni, riuscendo ad ottimizzare l'impiego delle risorse umani e materiali e gestendo i processi aziendali per politiche ed obiettivi specifici, coerenti con la presente politica;
- riesaminare sistematicamente la Politica ed adeguarla o modificarla tutte le volte che le condizioni operative o di mercato lo richiedessero;
- ottimizzare la comunicazione tra le aree aziendali;
- diffondere a tutti i livelli dell'organizzazione, l'importanza di ottemperare ai requisiti del cliente ed a quelli cogenti;
- adoperarsi per ottenere e mantenere la certificazione del proprio Sistema per la Qualità.

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162
info@bitcontrol.it
bitcontrol@pec.it
www.bitcontrol.it

LA VISIONE DI BITCONTROL S.R.L.

BitControl S.r.l. è consapevole che l'autorevolezza di un'azienda si riconosca, oltre che dalla competenza dei suoi collaboratori e dall'alta qualità del servizio fornito ai clienti, anche dall'attenzione posta alle esigenze dell'intera collettività.

I principi che ispirano il lavoro della BitControl S.r.l. vengono raccolti formalmente in un Codice Etico di Comportamento, nella convinzione che l'affidabilità di una società si fonda sul rispetto delle norme vigenti, nonché sull'esperienza e la competenza del proprio personale e dei collaboratori esterni.

Il Codice Etico della BitControl S.r.l. rappresenta, quindi, un elemento distintivo ed identificativo nei confronti del mercato e dei terzi, la cui conoscenza e condivisione, richiesta a tutti coloro che operano nella Società o che con essa collaborano, costituiscono il fondamento della nostra attività. Infatti, il Codice Etico è la carta dei diritti e dei doveri fondamentali attraverso i quali la BitControl S.r.l. chiarisce le proprie responsabilità etiche e sociali sia verso l'interno che verso l'esterno. Esso risponde all'esigenza di chiarire su quali criteri la società intende bilanciare gli interessi degli stakeholder interni ed esterni. Invero, il presente Codice Etico offre la possibilità a tutti gli interessati di poter verificare se le loro aspettative e le loro legittime pretese sono state considerate secondo equità, ponendo le basi per un accordo morale di cooperazione vantaggiosa per tutti.

BitControl S.r.l. riconosce che l'intelligenza artificiale rappresenta uno strumento di supporto all'attività professionale e non un sostituto del giudizio umano. L'adozione di soluzioni di IA avviene in maniera antropocentrica, nel rispetto della dignità delle persone e dei diritti fondamentali, in linea con i principi sanciti dalla Carta dei diritti fondamentali dell'Unione Europea e con gli orientamenti etici per un'IA affidabile elaborati dall'AI HLEG della Commissione Europea.

FINALITÀ E DESTINATARI

Il presente Codice Etico esprime l'insieme dei principi etici e morali e delle responsabilità etiche che sono alla base dell'attività di BitControl S.r.l., nonché le linee di comportamento adottate dalla Società sia all'interno della propria attività – nei rapporti con i propri dipendenti -, sia all'esterno –

nei rapporti con le istituzioni, i fornitori, i clienti, i partner commerciali, i collaboratori esterni, i consulenti e gli organi di informazione – (di seguito indicati come "Collaboratori e Partners").
Il presente Codice è vincolante per gli amministratori e i dipendenti di BitControl Srl, nonché per tutti coloro che operano e collaborano, stabilmente o a tempo determinato, per conto della Società (di seguito indicati come "Destinatari").

1. PRINCIPI GENERALI

La condotta dei Destinatari, a tutti i livelli aziendali, è improntata ai principi di legalità, correttezza, non discriminazione, riservatezza, diligenza, e lealtà.

1.1. Legalità

BitControl S.r.l. opera nell'assoluto rispetto della legge, dei regolamenti, delle procedure interne e dei principi sanciti nel presente Codice Etico.
Tutti i Destinatari sono, pertanto, tenuti ad osservare ogni normativa applicabile e ad aggiornarsi costantemente sulle evoluzioni legislative, anche avvalendosi delle opportunità formative offerte da BitControl S.r.l.
Nell'ambito del principio di legalità, tutti i Destinatari sono tenuti ad osservare, oltre alle normative generalmente applicabili, anche:

1. il Regolamento UE 2024/1689 (AI Act), che stabilisce regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione Europea;
2. la Legge 23 settembre 2025, n. 132, recante disposizioni in materia di intelligenza artificiale, applicabile in tutti i settori strategici del Paese;
3. il Regolamento UE 2016/679 (GDPR), con specifico riguardo ai trattamenti automatizzati e ai processi decisionali che coinvolgono dati personali.

I Destinatari sono tenuti ad aggiornarsi costantemente sulle evoluzioni di tale quadro normativo e a fare riferimento alla Policy IA aziendale per le indicazioni operative di dettaglio.

1.2 Correttezza

La correttezza e l'integrità morale sono un dovere indefettibile per tutti i Destinatari del presente Codice Etico.

I Destinatari sono tenuti a non instaurare alcun rapporto privilegiato con terzi, che sia frutto di sollecitazioni esterne finalizzate ad ottenere vantaggi impropri.

L'intrinseca convinzione di agire nell'interesse della Società non esonera i Destinatari dall'obbligo di osservare puntualmente le regole ed i principi del presente Codice Etico.

1.3 Non Discriminazione

Nei rapporti con i Collaboratori ed in particolare nella selezione e gestione del personale, nell'organizzazione lavorativa, nella scelta, selezione e gestione dei fornitori, nonché nei rapporti con gli Enti e le Istituzioni, BitControl S.r.l. non pone in essere alcuna discriminazione concernente l'età, il sesso, la razza, gli orientamenti sessuali, lo stato di salute, le opinioni politiche e sindacali, la religione, la cultura e la nazionalità.

1.4 Riservatezza

BitControl S.r.l. si impegna ad assicurare la protezione e la riservatezza dei dati personali dei Dipendenti, Destinatari e dei Collaboratori, nel rispetto della normativa applicabile in materia di protezione dei dati personali.

Infatti, BitControl S.r.l. tratta tutti i dati personali e sensibili dei Dipendenti, Destinatari e dei Collaboratori nel pieno del GDPR 2016/679.

I Dipendenti, i Destinatari e i Collaboratori sono previamente informati in ordine alla possibilità che la società può trattare i propri dati personali per ragioni strettamente connesse all'espletamento dell'attività lavorativa.

Con specifico riguardo all'uso di sistemi di intelligenza artificiale, i Destinatari si impegnano a non inserire in alcun strumento di IA – approvato o non approvato – dati personali non anonimizzati, dati appartenenti a categorie particolari ai sensi dell'art. 9 GDPR, ovvero informazioni classificate come riservate o confidenziali secondo la classificazione aziendale. Le misure di dettaglio sono disciplinate dalla Policy IA aziendale, della quale il presente Codice Etico costituisce parte integrante sul piano valoriale.

1.5 Informazioni di proprietà esclusiva

Preliminarmente, si precisa che i Dipendenti, i Collaborati e tutti i Destinatari del presente Codice Etico sono tenuti a non utilizzare informazioni riservate, apprese in ragione della propria attività

lavorativa, per scopi estranei all'esercizio di tale attività e, comunque, ad agire sempre nel rispetto degli obblighi di riservatezza assunti da BitControl S.r.l. nei confronti di tutti i terzi.

Per "informazioni di proprietà esclusiva" si intendono quelle di proprietà della BitControl S.r.l..

Non tutte le "informazioni di proprietà esclusiva" della BitControl S.r.l. sono informazioni riservate e potrebbero essere coperte da brevetti o altri diritti di proprietà intellettuale.

Tali informazioni comprendono piani gestionali, finanziari, commerciali e di assistenza connessa ai servizi e prodotti offerti; sono inoltre compresi i dati relativi al personale e alle retribuzioni.

Le informazioni di proprietà esclusiva comprendono anche i progetti, *Know-how* e processi tecnici e di produzione, piani commerciali e di produzione con i fornitori esterni e società partecipate e numerosi software e *data base* interni, oltre a tutto il materiale protetto da diritti d'autore di terzi (copyright).

1.6 Diligenza

Il rapporto tra BitControl S.r.l. ed i propri Dipendenti e Collaboratori è fondato sulla reciproca fiducia.

Pertanto, i Dipendenti ed i Collaboratori sono tenuti ad operare per favorire gli interessi dell'azienda, nel rispetto dei valori di cui al presente Codice Etico.

I Destinatari devono astenersi da qualsiasi attività che possa configurare conflitto con gli interessi di BitControl S.r.l. rinunciando al perseguimento di interessi personali in conflitto con i legittimi interessi della Società.

Nei casi in cui si possa raffigurare la possibilità di sussistenza di un conflitto di interessi, i Destinatari sono tenuti a comunicarlo, senza alcun ritardo, al datore di lavoro, affinchè l'azienda possa valutare, ed eventualmente autorizzare, l'attività potenzialmente in conflitto.

Nei casi di violazione, la Società adotterà ogni misura idonea a far cessare il conflitto di interessi, riservandosi di agire a propria tutela.

La BitControl S.r.l. potrà, altresì, adottare i provvedimenti disciplinari di cui al CCNL di riferimento, nonchè quelli di cui al proprio regolamento disciplinare, ciò nel caso in cui i comportamenti posti in essere siano in contrasto con l'etica aziendale puntualmente descritta nel presente Codice Etico e nelle procedure interne.

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162
info@bitcontrol.it
bitcontrol@pec.it
www.bitcontrol.it

1.7 Lealtà

BitControl S.r.l. ed i Destinatari si impegnano a realizzare una concorrenza leale, nel rispetto della normativa nazionale e comunitaria, nella consapevolezza che una concorrenza virtuosa costituisce un sano incentivo ai processi di innovazione e sviluppo, tutela altresì gli interessi dei consumatori e della collettività.

1.8 Salvaguardia dell'ambiente

L'impegno di BitControl S.r.l. nei riguardi dell'ambiente, è volto a salvaguardarne l'abbondanza e la bellezza per le generazioni presenti e future, con l'obiettivo di trasmettere loro i valori e le tradizioni che sostengono lo sviluppo a lungo termine delle comunità umane e ambientali.

BitControl S.r.l. si impegna in ogni fase del suo agire ad applicare criteri di cautela – il "Principio di Precauzione"– e un approccio preventivo nei riguardi dell'ambiente e della sua biodiversità; a promuovere iniziative per una maggiore responsabilità ambientale aziendale; a sviluppare l'impiego di mezzi e di tecnologie che non solo non danneggino l'ambiente ma che migliorino la sostenibilità ambientale degli impianti nei quali BitControl S.r.l. interviene con la propria attività di progettazione.

L'impegno di BitControl S.r.l. a salvaguardare il pianeta ed il benessere delle generazioni presenti e future include il benessere degli animali.

1.9 Uso Etico dell'Intelligenza Artificiale

BitControl S.r.l. riconosce che l'intelligenza artificiale, se non correttamente governata, può generare rischi per i diritti fondamentali, perpetuare pregiudizi e discriminazioni, compromettere la riservatezza dei dati e alterare l'equilibrio nei rapporti di lavoro. Per tali ragioni, tutti i Destinatari sono tenuti a:

A) RISPETTARE IL PRINCIPIO DI SUPERVISIONE UMANA. L'IA deve operare sempre sotto il controllo di una persona autorizzata. Ogni output generato da un sistema di IA deve essere validato da un essere umano prima di produrre effetti giuridici, economici o significativi sulle persone. L'IA non può assumere decisioni autonome su materie di rilievo contrattuale, legale o gestionale. Tale principio è coerente con quanto previsto dall'art. 14 del Regolamento UE 2024/1689, che impone la supervisione umana come requisito fondamentale per i sistemi di IA ad alto rischio.

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162
info@bitcontrol.it
bitcontrol@pec.it
www.bitcontrol.it

B) GARANTIRE TRASPARENZA. Quando nell'ambito delle attività aziendali o nella prestazione di servizi a clienti si faccia ricorso a sistemi di IA, i Destinatari sono tenuti a darne adeguata comunicazione in forma chiara, semplice ed esaustiva, in conformità all'art. 13 della Legge 132/2025, che dispone che le informazioni relative ai sistemi di IA utilizzati dal professionista siano comunicate al soggetto destinatario della prestazione intellettuale. Analogamente, laddove si utilizzino sistemi di IA generativa o chatbot nelle interazioni con clienti, deve essere sempre resa nota l'interazione con un sistema automatizzato.

C) EVITARE UTILIZZI DISCRIMINATORI. È fatto espresso divieto ai Destinatari di utilizzare sistemi di IA per generare contenuti discriminatori ovvero per prendere decisioni che incidano negativamente su persone o gruppi di persone in ragione di età, sesso, razza, orientamento sessuale, stato di salute, opinioni politiche o sindacali, religione, cultura o nazionalità.

D) RISPETTARE LA POLICY IA AZIENDALE. Tutti i Destinatari sono tenuti a conoscere e osservare la Policy IA di BitControl S.r.l., adottata dal Consiglio di Amministrazione in data 12.11.2025, che disciplina in dettaglio gli strumenti consentiti, i divieti, le misure di sicurezza, la supervisione umana e le procedure di segnalazione degli incidenti. Il presente Codice Etico e la Policy IA si integrano reciprocamente: il primo fissa i valori e i principi; la seconda traduce tali principi in regole operative vincolanti.

E) SEGNALARE ANOMALIE E VIOLAZIONI. I Destinatari che vengano a conoscenza di utilizzi impropri di sistemi di IA, di anomalie nel funzionamento degli stessi o di potenziali violazioni di dati, sono tenuti a segnalarlo immediatamente al Responsabile Sicurezza Informatica e, ove coinvolti dati personali, al DPO/Responsabile Privacy, secondo le modalità previste dalla Policy IA.

F) MANTENERE ADEGUATA ALFABETIZZAZIONE IN MATERIA DI IA. In conformità all'art. 4 del Regolamento UE 2024/1689, i fornitori e i deployer dei sistemi di IA adottano misure per garantire un livello sufficiente di alfabetizzazione in materia di IA del loro personale CIT. 4. BitControl S.r.l. si impegna a garantire la formazione continua del proprio personale sull'uso responsabile e sicuro dei sistemi di IA, anche attraverso aggiornamenti periodici previsti dalla Policy IA.

2 RAPPORTI CON I DIPENDENTI E CON I COLLABORATORI

2.1 Selezione del personale

La valutazione e la selezione del personale sono effettuati secondo correttezza e trasparenza, rispettando le pari opportunità al fine di coniugare le esigenze di BitControl S.r.l., con i profili professionali, le ambizioni e le aspettative dei candidati.

Il personale assunto, anche mediante l'attuazione del presente Codice Etico, riceve un'informazione chiara e corretta circa ruoli, responsabilità, diritti e doveri delle parti.

2.2 Gestione del personale

BitControl S.r.l. tutela e valorizza le proprie risorse umane, impegnandosi a mantenere costanti le condizioni necessarie per la crescita professionale, le conoscenze e le abilità di ogni persona, effettuando l'opportuna formazione per l'aggiornamento professionale e qualsiasi iniziativa volta a perseguire tale scopo.

Ferma restando la massima disponibilità nei confronti della Società, nessun lavoratore può essere obbligato ad eseguire mansioni, prestazioni o favori non dovuti in base al proprio contratto di lavoro ed al proprio ruolo all'interno dell'azienda.

La Società si impegna fermamente a contrastare episodi di mobbing, stalking, violenza psicologica ed ogni comportamento discriminatorio o lesivo della dignità della persona dentro e fuori i locali aziendali.

I rapporti tra dipendenti devono svolgersi con lealtà, correttezza e rispetto reciproco, in osservanza dei valori della civile convivenza e della liberà delle persone.

BitControl S.r.l. si impegna affinché l'introduzione di sistemi di IA nell'ambiente di lavoro non determini forme di controllo occulto sui lavoratori né comprometta la loro dignità professionale. L'IA è adottata quale strumento di supporto all'attività lavorativa e non di sostituzione del lavoratore. Nessuna decisione che incida in modo significativo sul rapporto di lavoro – ivi incluse valutazioni delle prestazioni, attribuzione di mansioni o provvedimenti disciplinari – potrà essere adottata esclusivamente sulla base di processi decisionali automatizzati, in conformità all'art. 22 del GDPR e al principio di supervisione umana sancito dalla Policy IA.

3 AMBIENTE DI LAVORO

BitControl S.r.l. si impegna ad offrire al proprio personale un ambiente di lavoro sano, sicuro, efficiente e rispettoso della dignità dei lavoratori.

La sicurezza sui luoghi di lavoro è assicurata sia implementando rigorosamente le disposizioni previste dalla legge in vigore, sia promuovendo attivamente la cultura della sicurezza attraverso specifici programmi formativi. La formazione del personale rappresenta un elemento centrale del sistema di gestione adottato.

BitControl S.r.l. tutela la salute dei propri lavoratori, garantendo altresì il rispetto delle norme igieniche e di prevenzione sanitaria.

La cultura della sicurezza promossa da BitControl S.r.l. include la sicurezza informatica e la protezione dei sistemi di IA da minacce cibernetiche. I programmi formativi aziendali comprendono, tra l'altro, la formazione sull'uso sicuro, etico e responsabile degli strumenti di intelligenza artificiale adottati dalla Società.

4 GESTIONE DELL'IMPRESA

4.1 Osservanza delle procedure interne

BitControl S.r.l. ritiene che l'efficienza gestionale e la cultura del controllo siano elementi indispensabili per il raggiungimento degli obiettivi.

I Destinatari sono tenuti alla rigorosa osservanza delle procedure e delle istruzioni interne all'azienda.

I Destinatari devono agire in base ai rispettivi profili di autorizzazione e devono conservare ogni idonea documentazione per tenere traccia delle azioni intraprese per conto dell'azienda.

Con specifico riguardo all'uso dell'intelligenza artificiale, i Destinatari sono tenuti alla rigorosa osservanza della Policy IA aziendale e delle istruzioni operative emanate dal Responsabile IT e dal DPO. In nessun caso è consentito l'utilizzo di strumenti di IA non approvati per attività lavorative senza previa autorizzazione scritta del Responsabile IT o del datore di lavoro.

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162
info@bitcontrol.it
bitcontrol@pec.it
www.bitcontrol.it

4.2 Comunicazione e diffusione del Codice Etico

BitControl S.r.l. si impegna a favorire e garantire adeguata conoscenza del Codice Etico divulgandolo presso i Dipendenti, i Collaboratori e tutti i Destinatari, mediante apposite ed adeguate attività di comunicazione.

Affinché chiunque possa uniformare i suoi comportamenti a quelli qui descritti, BitControl S.r.l. assicurerà un adeguato programma di formazione e una continua sensibilizzazione dei valori e delle norme etiche contenuti nel Codice Etico.

La Policy IA aziendale è parte integrante del sistema valoriale e normativo interno di BitControl S.r.l. Essa è diffusa unitamente al presente Codice Etico attraverso la intranet aziendale e mediante comunicazione diretta ai Destinatari, al fine di garantirne la massima accessibilità e conoscenza.

4.3 Beni di BitControl S.r.l.

I locali, le attrezzature, i sistemi, le vetture aziendali e tutti gli altri beni di BitControl S.r.l. possono essere utilizzati, esclusivamente, per lo svolgimento delle attività aziendali o per scopi autorizzati dalla società.

4.4 Protezione del Patrimonio di BitControl S.r.l.

Il patrimonio di BitControl S.r.l. è costituito da beni materiali mobili e immateriali (ovvero informazioni e prodotti di proprietà esclusiva, che possono rappresentare oggetto di tutela di proprietà intellettuale) per il mantenimento della sua competitività e del suo successo.

Tra i predetti beni vi sono dati riservati ai dipendenti per l'espletamento della propria attività lavorativa. La perdita, il furto o l'uso improprio dei predetti beni potrebbe pregiudicare la Società e per questa ragione ogni Dipendente e Collaboratore è responsabile della protezione del patrimonio aziendale in generale. A questo scopo, si richiede il rispetto e la conoscenza delle procedure di sicurezza oltre la diligenza necessaria ad evitare ogni tipo di pregiudizio.

Infatti, ogni Dipendente e Collaboratore deve prestare attenzione a qualsiasi situazione che possa condurre alla perdita, al furto o all'uso improprio dei beni della BitControl S.r.l. e denunciare ai responsabili della Sicurezza o al proprio superiore non appena ne venga a conoscenza.

5 RAPPORTI CON L'ESTERNO

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162
info@bitcontrol.it
bitcontrol@pec.it
www.bitcontrol.it

5.1 Rapporti con Autorità e Pubbliche Amministrazioni

I rapporti con le Autorità e con la Pubblica Amministrazione devono essere improntati alla massima chiarezza, trasparenza e collaborazione, nel pieno rispetto della legge e secondo i più alti standard morali e professionali.

I Destinatari, salva espressa autorizzazione, non possono relazionarsi in nome e per conto di BitControl S.r.l. con le Autorità e con la Pubblica Amministrazione.

Nei rapporti con i Pubblici Ufficiali, con gli Incaricati di Pubblico Servizio, e la Pubblica Amministrazione in generale, i Destinatari autorizzati si atterrano a massimi livelli di correttezza e integrità, astenendosi da qualsiasi forma di pressione, esplicita o velata, finalizzata a ottenere qualsiasi vantaggio indebito per sé o per BitControl S.r.l.

A tal proposito i Destinatari autorizzati saranno tenuti a osservare strettamente quanto disposto dal presente Codice, nonché, più in generale, a quanto previsto dalle direttive impartite dal management di BitControl S.r.l.

5.2 Rapporto con clienti e fornitori

I clienti costituiscono parte integrante del patrimonio aziendale di BitControl S.r.l..

La Società intrattiene rapporti con clienti che rispettano i principi fondamentali e, tenuto conto del loro ordinamento giuridico, sociale, economico e culturale di riferimento, le norme del presente Codice.

I Destinatari si rapportano con i terzi con cortesia, competenza e professionalità, nella convinzione che dalla loro condotta dipende la tutela dell'immagine e della reputazione dell'azienda e conseguentemente il raggiungimento degli obiettivi aziendali.

In particolare, i Destinatari devono astenersi da qualsiasi forma di comportamento sleale o ingannevole che possa indurre i clienti o i fornitori a fare affidamento su fatti o circostanze infondati.

I Destinatari sono tenuti impegnarsi con costanza per offrire servizi puntuali e di alta qualità ai clienti, cercando di limitare qualsiasi forma di disservizio o ritardo al fine di massimizzare la soddisfazione della clientela.

Le relazioni con i fornitori sono improntate a lealtà, correttezza e trasparenza.

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162
info@bitcontrol.it
bitcontrol@pec.it
www.bitcontrol.it

La scelta dei fornitori viene effettuata in base a criteri oggettivi di economicità, opportunità ed efficienza.

È preclusa la scelta di fornitori su basi meramente soggettive e personali o, comunque, in virtù di interessi contrastanti con quelli di società.

I Destinatari devono porre in essere ogni controllo possibile affinché anche fornitori e clienti siano in grado di rispettare i principi etici fondamentali di cui al presente Codice.

Nei rapporti con clienti e fornitori, laddove BitControl S.r.l. utilizzi sistemi di IA per la fornitura di servizi o nella predisposizione di offerte commerciali, i Destinatari sono tenuti a garantire la massima trasparenza sull'utilizzo di tali tecnologie. In conformità all'art. 13 della Legge 132/2025, le informazioni sui sistemi di IA utilizzati devono essere comunicate al destinatario della prestazione con linguaggio chiaro, semplice ed esaustivo. Nelle procedure di gara pubblica, i Destinatari sono tenuti a rendere le dichiarazioni previste dalla normativa vigente in materia di utilizzo di sistemi di IA, in conformità alle indicazioni dell'ANAC

6 SISTEMA DI CONTROLLO INTERNO

Il rispetto delle prescrizioni del presente Codice Etico è affidato alla prudente, ragionevole ed attenta sorveglianza di ciascuno dei Destinatari, nell'ambito dei rispettivi ruoli e funzioni all'interno dell'azienda.

Tutti i Destinatari sono invitati a riportare ai loro diretti superiori i fatti e le circostanze potenzialmente in contrasto con i principi e le prescrizioni del presente Codice.

Il management di BitControl S.r.l. e gli organi all'uopo preposti adottano ogni necessaria misura per porre fine alle violazioni, potendo ricorrere a qualsiasi provvedimento disciplinare nel rispetto della legge e dei diritti dei lavoratori, ivi inclusi i diritti sindacali.

Il sistema di controllo interno include la verifica del corretto utilizzo dei sistemi di IA da parte dei Destinatari, in conformità alla Policy IA aziendale. A tal fine, BitControl S.r.l. adotta sistemi di logging e tracciabilità per i processi che utilizzano strumenti di IA, garantendo la possibilità di ricostruire le decisioni adottate con il supporto di tali tecnologie e la relativa supervisione umana. Gli audit interni condotti secondo ISO/IEC 27001:2022 comprendono la verifica della conformità all'uso degli strumenti di IA approvati.

7 LINEE GUIDA DEL SISTEMA SANZIONATORIO

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162
info@bitcontrol.it
bitcontrol@pec.it
www.bitcontrol.it

Il sistema di controllo interno è orientato all'adozione di strumenti e metodologie volti a contrastare i potenziali rischi aziendali, al fine di garantire il rispetto non solo delle leggi, ma anche delle disposizioni e procedure interne.

Infatti, la violazione dei principi fissati nel Codice Etico e nelle procedure indicate nei controlli interni compromette il rapporto fiduciario tra la Società ed i propri amministratori, dipendenti, consulenti, collaboratori a vario titolo, clienti, fornitori, partners commerciali e finanziari.

Tali violazioni saranno quindi immediatamente perseguite da BitControl S.r.l. in maniera incisiva e tempestiva, mediante l'adozione di provvedimenti disciplinari adeguati e proporzionati.

Gli effetti delle violazioni del Codice Etico e dei protocolli interni devono essere tenuti in considerazione da tutti coloro che, a qualsiasi titolo, intrattengono rapporti con BitControl S.r.l. A seconda della gravità della condotta posta in essere dal soggetto coinvolto in una delle attività illecite previste dal Codice Etico, BitControl S.r.l. provvederà senza indugio ad adottare i provvedimenti opportuni, indipendentemente dall'eventuale esercizio dell'azione penale da parte dell'autorità giudiziaria.

Fermo quanto sopra esposto, i comportamenti in violazione del Codice Etico costituiscono:

- o grave inadempimento per i dipendenti (operai, impiegati, quadri e dirigenti), con le sanzioni, applicate a seconda della gravità, previste dal CCNL di categoria (rimprovero verbale, rimprovero scritto, multa non superiore a tre ore di retribuzione, sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni lavorativi, licenziamento per giusta causa o giustificato motivo); nel caso di pendenza dell'azione penale ovvero di esecuzione di un provvedimento restrittivo della libertà personale assunto nei confronti del dipendente, prima di adottare il provvedimento disciplinare, potrà essere adottata la sanzione della sospensione dal servizio e dalla retribuzione, per la durata corrispondente all'esito dell'azione penale ovvero fino al termine della durata del provvedimento restrittivo della libertà personale;
- o giusta causa per revoca del mandato agli amministratori;
- o causa di risoluzione immediata del rapporto, nei casi più gravi, per i collaboratori esterni e parasubordinati;
- o causa di risoluzione immediata del rapporto, nei casi più gravi, per i fornitori, appaltatori e subappaltatori.

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162 bitcontrol@pec.it
info@bitcontrol.it www.bitcontrol.it

L'individuazione e l'applicazione delle sanzioni terrà sempre conto dei principi generali di proporzionalità e di adeguatezza rispetto alla violazione contestata.

In tutte le suddette ipotesi, BitControl S.r.l. si riserva altresì il diritto di esercitare tutte le azioni che riterrà opportune per il risarcimento del danno subito in conseguenza del comportamento in violazione del Codice Etico.

COSTITUISCONO ALTRESÌ VIOLAZIONI DEL PRESENTE CODICE ETICO, SOGGETTE ALLE SANZIONI PROPORZIONATE IVI PREVISTE:

1. l'utilizzo di strumenti di IA non approvati per attività lavorative;
2. l'inserimento in sistemi di IA di dati personali non anonimizzati, dati sensibili o informazioni riservate;
3. l'omessa supervisione umana su output di sistemi di IA che producano effetti significativi sulle persone;
4. la mancata segnalazione di incidenti, anomalie o potenziali violazioni connesse all'uso di sistemi di IA;
5. l'utilizzo di sistemi di IA per generare contenuti discriminatori, offensivi, manipolativi o illeciti;

qualsiasi condotta in violazione della Policy IA aziendale.

Le sanzioni sono applicate nel rispetto dei principi di proporzionalità e adeguatezza, secondo le modalità previste al precedente paragrafo 7, ferma restando la responsabilità civile e penale nei casi previsti dalla legge.

8. 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 21041 e 21052 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 BitControl 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 BitControl 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.

8.1 Tutela del Capitale Sociale, dei Creditori e del Mercato

Uno degli aspetti centrali che qualificano la condotta di BitControl S.r.l. è rappresentato dal rispetto dei princìpi di comportamento intesi a garantire l'integrità del capitale sociale, la tutela dei creditori e dei terzi che instaurano rapporti con la Società.

I suddetti principi sono tutelati, anche, da norme penali e ai sensi del D.Lgs. 231/01 la violazione di tali disposizioni può costituire fonte di responsabilità per BitControl S.r.l. ove le fattispecie di reato sia realizzata nell'interesse della Società stessa.

Pertanto, è posto l'espresso divieto a carico dei dipendenti, dei Collaboratori e di tutti i Destinatari del presente Codice Etico di porre in essere, collaborare o dare causa alla realizzazione di

comportamenti tali da integrare le fattispecie di reato previste dall'art. 25 ter del D.Lgs. 231/01 e porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo, ovvero comportamenti che possano favorire la commissione dei predetti reati.

I Dipendenti, i Collaboratori e tutti i Destinatari del presente Codice Etico, nell'ambito delle funzioni e attività svolte, sono responsabili della definizione e del corretto funzionamento del sistema di controllo e sono tenuti a comunicare in forma scritta alla Società o al proprio superiore le eventuali omissioni, falsificazioni o irregolarità contabili delle quali fossero venuti a conoscenza.

8.2 Pubblica Amministrazione

L'assunzione di impegni con le Istituzioni Pubbliche Locali, Statali, Comunitarie e Internazionali è riservata esclusivamente alle funzioni preposte e autorizzate. Per questo motivo è opportuno che venga raccolta e conservata la documentazione che riassume le modalità attraverso le quali BitControl S.r.l. è entrata in contatto con le Istituzioni.

È fatto assoluto divieto di:

- ai Dipendenti, ai Collaboratori esterni e ai consulenti delle Società e a tutti i Destinatari del presente Codice Etico di:

- falsificare e/o alterare i rendiconti al fine di ottenere un indebito vantaggio o qualsiasi altro beneficio per la Società;

- falsificare e/o alterare i dati documentali al fine di ottenere il favore o l'approvazione di un progetto non conforme alle normative vigenti in materia;

- destinare fondi pubblici a finalità diverse da quelle per cui si sono ottenuti.

8.3 Conflitto d'interessi

Per garantire la massima trasparenza, BitControl S.r.l. e i propri dipendenti si impegnano a non trovarsi in situazioni di conflitto di interessi con dipendenti di qualsiasi Authority e loro familiari. Ciascun Dipendente, Collaboratore e Destinatario del presente Codice Etico che ritenga di trovarsi in una situazione di conflitto tra il proprio interesse personale, per suo conto o per conto di terzi, e gli interessi della Società, deve darne comunicazione immediata secondo l'opportunità, al proprio

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162
info@bitcontrol.it
bitcontrol@pec.it
www.bitcontrol.it

superiore gerarchico, al Consiglio di Amministrazione, restando valide le norme specifiche previste dal Codice Civile.

8.4 Utilizzo dell'Intelligenza Artificiale e Responsabilità ex D.Lgs. 231/2001

Il Modello di Organizzazione, Gestione e Controllo adottato da BitControl S.r.l. ai sensi del D.Lgs. 231/2001 integra i presidi relativi all'utilizzo dei sistemi di intelligenza artificiale. La Policy IA aziendale costituisce parte del Modello, disciplinando i controlli preventivi volti a evitare che l'uso di sistemi di IA possa dar luogo a condotte penalmente rilevanti, ivi incluse quelle connesse a trattamenti illeciti di dati personali, violazioni di proprietà intellettuale, frodi informatiche o condotte discriminatorie.

I Destinatari sono tenuti a rispettare integralmente le disposizioni della Policy IA nell'ambito delle proprie funzioni, consapevoli che la violazione delle stesse può rilevare ai fini della responsabilità amministrativa della Società ai sensi del citato Decreto.

SEDE LEGALE: Via Stazione, 39 - 95047 Paternò (CT)
UFFICI: Via G.B.Nicolosi, 334 - 95047 Paternò (CT)
P.IVA: 04761870874 – **R.E.A.:** CT-317371
Capitale Sociale Euro 15.000
095/855162
info@bitcontrol.it
bitcontrol@pec.it
www.bitcontrol.it

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev.6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

- ALLEGATO - 2 -

Clausola contrattuale

BITCONTROL intende garantire l'osservanza e la divulgazione del Modello Organizzativo di cui al D.Lgs. 231/2001 dunque, a tal fine, ha inserito tra le clausole generali di contratto la seguente dichiarazione.

CLAUSOLA CONTRATTUALE PER CONTROPARTE

"La parte X dichiara di essere stata informata e di aver preso atto che BitControl S.r.l. ha adottato il Modello di organizzazione, gestione e controllo di cui al citato Decreto, nonchè un proprio Codice Etico contenente i principi di etica aziendale, entrambi consultabili all'indirizzo Internet www.bitcontrol.it.

La parte X dichiara, altresì, 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 BitControl ha enunciato nel proprio Codice Etico, di cui dichiara di aver preso visione.

La parte X si obbliga ad ottemperare a tutti obblighi informativi verso l'Organismo monocratico di Vigilanza nominato dalla BitControl S.r.l. ai sensi dell'art. 6 del D.Lgs 231/2001, nonché a tutti gli adempimenti di legge previsti dal predetto modello e dallo Statuto e dal Regolamento dell'Organismo di Vigilanza".

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

- ALLEGATO - 5 -

COMPENSI, CAUSE DI (IN) ELEGGIBILITÀ, DECADENZA E SOSPENSIONE DEI COMPONENTI DELL'ORGANISMO DI VIGILANZA

Il compenso annuo spettante al componente dell'Organismo di Vigilanza viene determinato, per l'intera durata della carica, dal Consiglio di Amministrazione di BitControl.
Peraltro, al componente dell'Organismo di Vigilanza spetta anche il rimborso delle spese vive e documentate sostenute nell'espletamento dell'incarico.

Ineleggibilità

Presupposto indefettibile per assolvere all'incarico di componente dell'Organismo di Vigilanza deve essere quello di possedere i 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..
Inoltre, si precisa che non può essere nominato alla carica di componenti 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.
Infatti, i candidati alla carica di componente monocratico dell'Organismo di Vigilanza devono autocertificare con dichiarazione sostitutiva di notorietà di non trovarsi in alcuna delle condizioni indicate dal numero 1 al numero 10, impegnandosi espressamente a comunicare eventuali variazioni rispetto al contenuto di tali dichiarazioni.
Il Consiglio di Amministrazione di BitControl può revocare il componente dell'Organismo nei casi in cui si verifichino rilevanti inadempimenti rispetto al mandato conferito, in ordine ai compiti indicati nel regolamento; per ipotesi di violazione degli obblighi di riservatezza, nonchè quando si manifestino cause di ineleggibilità di cui sopra, anteriori alla nomina a componente dell'OdV e non indicate nell'autocertificazione; quando intervengano le cause di decadenza di seguito specificate.

Decadenza

Il componente 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.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

- ALLEGATO 4 -

COMPOSIZIONE DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza di BITCONTROL è Monocratico e risulta costituito dal componente esterno, avv. Rosaria Anna Borzì.

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

- ALLEGATO 3 -

ELENCO REATI SANZIONATI DAL DECRETO

L'elenco di seguito riportato comprende i seguenti aggiornamenti normativi:

ULTIMI PROVVEDIMENTI APPORTATI dal Decreto Legislativo n. 128 del 25 giugno 2026

"Attuazione della delega di cui all'articolo 19-bis della legge 5 marzo 2024, n. 21, per la riforma organica e il riordino del sistema sanzionatorio e di tutte le procedure sanzionatorie recati dal testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58"
Il provvedimento ha interessato la disciplina degli Abusi di mercato. In particolare, sono stati modificati gli Artt. 187-ter.1 (Sanzioni relative alle violazioni delle disposizioni del Regolamento (UE) n. 596/2014) e 187-quinquies (Responsabilità dell'ente) del D.Lgs. 24 febbraio 1998, n. 58 (TUF), disposizioni richiamate dall'Art. 25-sexies del D.Lgs. n. 231/2001, nell'ambito della riforma organica del sistema sanzionatorio e delle procedure applicabili in materia di abusi di mercato.

ULTIMI PROVVEDIMENTI APPORTATI dal Decreto Legislativo n. 115 del 12 giugno 2026

"Attuazione della direttiva (UE) 2024/1712 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che modifica la direttiva 2011/36/UE concernente la prevenzione e la repressione della tratta di esseri umani e la protezione delle vittime"

Il provvedimento ha interessato i "Delitti contro la personalità individuale" con la modifica del testo dell'Art. 25-quinquies del D.Lgs. n. 231/2001 e delle fattispecie di reato ad esso collegate. In particolare, sono stati modificati gli Artt. 600 c.p. (Riduzione o mantenimento in schiavitù), 601 c.p. (Tratta di persone) e 602-ter c.p. (Circostanze aggravanti), nonché introdotto il nuovo Art. 601.1 c.p. (Approfittamento della vittima di riduzione in schiavitù o di tratta)

ULTIMI PROVVEDIMENTI APPORTATI dal Decreto Legislativo n. 83 del 16 aprile 2026

"Attuazione della direttiva (UE) 2024/1233 del Parlamento europeo e del Consiglio, del 24 aprile 2024, relativa a una procedura unica di domanda per il rilascio di un permesso unico che consente ai cittadini di Paesi terzi di soggiornare e lavorare nel territorio di uno Stato membro e a un insieme comune di diritti per i lavoratori di Paesi terzi che soggiornano regolarmente in uno Stato membro"

Modifica Art.22 D. Lgs. n.286/98 (Lavoro subordinato a tempo determinato e indeterminato) facente parte dell'Art.25-duodecies D.Lgs. 231/01 "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare"

ULTIMI PROVVEDIMENTI APPORTATI dal Decreto Legislativo n. 81 del 21 aprile 2026

"Attuazione della direttiva (UE) 2024/1203 del Parlamento europeo e del Consiglio dell'11 aprile 2024 sulla tutela penale dell'ambiente che sostituisce le direttive 2008/99/CE e 2009/123/CE"

Il D.Lgs. n. 81/2026 interviene sui Reati ambientali modificando l'Art.25-undecies D.Lgs. n.231/01 e le principali fattispecie del codice penale e del D.Lgs. n.152/2006 (TUA).

Sono stati modificati gli Artt. 452-bis c.p. (Inquinamento ambientale) e 256 TUA (Attività di gestione di rifiuti non autorizzata), introdotti gli Artt. 452-bis.1 c.p. (Commercio di prodotti inquinanti), Art. 452-ter c.p. (Morte o lesioni come conseguenza del delitto di inquinamento ambientale e di commercio di prodotti inquinanti), 452-quinquiesdecies c.p. (Nozione di abusività) e 452-sexiesdecies c.p. (Circostanze aggravanti) e abrogato l'Art. 733-bis c.p. (Distruzione o deterioramento di habitat all'interno di un sito protetto)

ULTIMI PROVVEDIMENTI APPORTATI dalla Legge n. 75 del 21 aprile 2026

"Disposizioni sanzionatorie a tutela dei prodotti alimentari italiani"

Modifica al testo dell'Art. 25-bis.1 del D. Lgs. 231/2001 "Delitti contro l'industria e il commercio"

Abrogazione dell'Art. 516 c.p. e modifica alla rubrica ed al testo dell'Art. 517-quater c.p. (Contraffazione dei segni di indicazione geografica e di denominazione protetta dei prodotti agroalimentari) che hanno interessato sia l'Art. 25-bis.1 del D. Lgs 231/01che l'Art.12 della Legge n.9/2013 (Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato)

Introduzione degli articoli 517-sexies c.p. (Frode alimentare), 517-septies c.p. (Commercio di alimenti con segni mendaci) e Art. 517-octies c.p. (Pena accessoria e circostanze aggravanti) che hanno interessato unicamente l'Art. 25-bis.1 del D.Lgs. 231/01.

Modifica al testo dell'Art. 9 della Legge n. 146/2006 (Operazioni sotto copertura) che hanno interessato i Reati transnazionali (Legge n.146/2006), l'Art. 25-quater del D. Lgs 231/01 (Delitti con finalità di terrorismo o di eversione dell'ordine democratico), l'Art.25-undecies del D. Lgs 231/01 (Reati ambientali) e l'Art.25-duodevicies del D. Lgs 231/01 (Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici)

ULTIMI PROVVEDIMENTI APPORTATI dal Decreto Legge n. 23 del 24 febbraio 2026 coordinato con Legge di conversione n. 54 del 24 aprile 2026

"Disposizioni urgenti in materia di sicurezza pubblica, di attività di indagine dell'autorità giudiziaria in presenza di cause di giustificazione, di funzionalità delle forze di polizia e del Ministero dell'interno, nonché di immigrazione e protezione internazionale "

Modifica del testo dell'Art. 518-quater (Ricettazione di beni culturali) facente parte dell'Art. 25-septiesdecies del D. Lgs. 231/01 "Delitti contro il patrimonio culturale" e dell'Art. 648 c.p. (Ricettazione) facente parte dell'Art. 25-octies del D. Lgs. 231/01 "Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio"

ULTIMI PROVVEDIMENTI APPORTATI dalla Legge n. 34 dell'11 marzo 2026

"Legge annuale sulle piccole e medie imprese "

Le modifiche hanno interessato l'articolo 3 del D. Lgs. 81/2008 in cui si chiarisce che, anche nel lavoro agile, il datore di lavoro è tenuto a garantire tutti gli obblighi di sicurezza compatibili con tale modalità e l'articolo 55 del D. Lgs. 81/2008 che rafforzando il quadro sanzionatorio ha interessato il perimetro dei reati presupposto Art. 25-septies del D. Lgs. 231/01 "Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle

norme sulla tutela della salute e sicurezza sul lavoro", con tutte le implicazioni in termini di responsabilità amministrativa dell'ente.

ULTIMI PROVVEDIMENTI APPORTATI dal D.Lgs. n. 211 del 30 dicembre 2025:

"Attuazione della direttiva 2024/1226/UE del Parlamento europeo e del Consiglio, del 24 aprile 2024, relativa alla definizione dei reati e delle sanzioni per la violazione delle misure restrittive dell'Unione e che modifica la direttiva (UE) 2018/1673 "

Introduzione del nuovo Art. 25-octies.2 del D.Lgs. 231/2001 "Reati in materia di violazione di misure restrittive dell'Unione europea" che inserisce nel catalogo dei reati presupposto le fattispecie previste dal codice penale nel nuovo capo I-bis (del Libro II – Titolo I) i seguenti articoli di Codice Penale:

Art. 275-bis (Violazione delle misure restrittive dell'Unione europea);

Art. 275-ter (Violazione di obblighi informativi imposti da una misura restrittiva dell'Unione europea) Art. 275-quater (Violazione delle condizioni dell'autorizzazione allo svolgimento di attività);

Art. 275-quinques (Violazione colposa di misure restrittive dell'Unione europea)

Art. 275-sexies (Circostanze aggravanti);

Art. 275-septies (Circostanze attenuanti);

Art. 275-octies (Confisca obbligatoria);

Art. 275-novies (Pubblicazione della sentenza di condanna);

Art. 275-decies (Giurisdizione);

Modifica Art.12 D.Lgs n.286 /1998 "Disposizioni contro le immigrazioni clandestine" con l'aggiunta del comma 1-bis;

Modifiche agli Artt. 10 e 13 del D.Lgs 231/01 in merito alla sanzione amministrativa pecuniaria ed alle sanzioni interdittive;

Modifica Art. 1 del D.Lgs n. 24/2023 mediante l'introduzione del comma 1-bis ad opera dell'Art. 7 del D.Lgs n. 211/2025, con estensione dell'ambito di applicazione oggettivo della tutela alle persone che segnalano violazioni delle misure restrittive dell'Unione europea;

ULTIMI PROVVEDIMENTI APPORTATI dal D.L. n.146 del 3 Ottobre 2025 coordinato con la Legge di conversione n.179 del 1 Dicembre 2025:

"Disposizioni urgenti in materia di ingresso regolare di lavoratori e cittadini stranieri, nonché di gestione del fenomeno migratorio";

Modifica all'Art.22 D. Lgs. n.286/98 "Lavoro subordinato a tempo determinato e indeterminato "con l'inserimento dei commi 2-bis.1 e 2-bis.2;

ULTIMI PROVVEDIMENTI APPORTATI dalla Legge n.147 del 03.10.25:

"Conversione in legge, con modificazioni, del decreto-legge 8 agosto 2025, n. 116, recante 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";

Modifica dell'Art. 25-undecies D.Lgs. 231/01 (Reati ambientali);

Modifica Art. 452-quaterdecies c.p. (Attività organizzate per il traffico illecito di rifiuti), e Conversione Art. 452-sexies c.p., (Traffico e abbandono di materiale ad alta radioattività), Art. 452-septies c.p. (Impedimento del controllo) e 452-terdecies c.p. (Omessa bonifica);

Modifica di articoli del D.Lgs n.152/2006 (Norme in materia ambientale): Art. 212 (Albo nazionale gestori ambientali), Art. 255 (Abbandono di rifiuti non pericolosi), Art. 256 (Attività di gestione di rifiuti non autorizzata), Art. 258 (Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari) e conversione dell'Art. 255-bis (Abbandono di rifiuti non pericolosi in casi particolari), Art. 255-ter (Abbandono di rifiuti pericolosi), Art. 256- bis (Combustione illecita di rifiuti), Art. 259 (Spedizione illegale di rifiuti), Art. 259-bis (Aggravante dell'attività d'impresa), Art. 259-ter (Delitti colposi in materia di rifiuti);

Estensione per le operazioni sotto copertura, già contemplate dai reati transnazionali, anche ai reati ambientali con la modifica dell'Art.9 comma 1 lettera a) Legge n.146 del 16 marzo 2006.

ULTIMI PROVVEDIMENTI APPORTATI dalla Legge n.132 del 23.09.25:

"Disposizioni e deleghe al Governo in materia di intelligenza artificiale";

Modifica agli articoli di Codice Civile, della L.633/1941 e del D.Lgs n.58/1998 (TUF) Art. 2637 c.c. (Aggiotaggio) facente parte dell'Art. 25-ter D. Lgs.231/01; Art. 171 L.633/1941 comma 1, lett. a-bis (Messa a disposizione del pubblico di un'opera dell'ingegno protetta o parte di essa) facente parte dell'Art. 25- novies D. Lgs.231/01; Art.185-TUF (Manipolazione del mercato) facente parte dell'Art. 25-sexies D. Lgs.231/01;

ULTIMI PROVVEDIMENTI APPORTATI dal Decreto Legge n.116 dell'8 agosto 2025

" Disposizioni urgenti per il contrasto alle attivita' illecite in materia di rifiuti, per la bonifica dell'area denominata Terra dei fuochi, nonche' in materia di assistenza alla popolazione colpita da eventi calamitosi ";

Modifica nei reati presupposto D.Lgs231/01 dell'Art. 25- undecies "Reati ambientali" con un generale aumento delle quote relative alle sanzioni pecuniarie per tutti i reati;
Modifiche e nuove introduzioni di reati del Codice Penale in materia di bonifiche e contrasto all'inquinamento e al disastro ambientale;
Modificati Art. 452-sexies (Traffico e abbandono di materiale ad alta radioattività), Art. 452-quaterdecies (Attività organizzate per il traffico illecito di rifiuti).
Inseriti Art. 452-septies (Impedimento del controllo) e Art. 452-terdecies (Omessa bonifica);
Modifiche e nuove introduzioni di reati contemplati dal D.Lgs n.152/2006 (Norme in materia ambientale);
Modificati Art.255 (Abbandono di rifiuti non pericolosi), Art.256 (Attività di gestione di rifiuti non autorizzata), Art.258 (Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari), Art.259 (Spedizione illegale di rifiuti).
Inseriti Art.212 comma 19-ter (Albo nazionale gestori ambientali), Art.255-bis (Abbandono di rifiuti non pericolosi in casi particolari), Art.255-ter (Abbandono di rifiuti pericolosi), Art.256-bis (Combustione illecita di rifiuti), Art.259-bis (Aggravante dell'attività di impresa), Art.259-ter (Delitti colposi in materia di rifiuti).
Estensione di quanto previsto per le operazioni sotto copertura, già contemplate dai reati transnazionali, anche ai reati ambientali con la modifica dell'Art.9 comma 1 lettera a) Legge n.146 del 16 marzo 2006.

ULTIMI PROVVEDIMENTI APPORTATI dalla L. n.82 del 6 giugno 2025:

"Modifiche al codice penale, al codice di procedura penale e altre disposizioni per l'integrazione e l'armonizzazione della disciplina in materia di reati contro gli animali";
Inserimento nei reati presupposto D.Lgs 231/01 dell'Art.25-undevicies "Delitti contro gli animali" con relativa modifica testo e introduzione: Art.544- bis c.p. (Uccisione di animali), Art.544-ter c.p. (Maltrattamento di animali), Art. 544-quater c.p. (Spettacoli o manifestazioni vietati), Art.544- quinquies c.p. (Divieto di combattimenti tra animali), introduzione Art. 544-septies (Circostanze aggravanti) e sostituzione e introduzione Art. 638 c.p. (Uccisione o danneggiamento di animali altrui).
Modifiche testo Art. 727-bis c.p. (Uccisione, distruzione, cattura, prelievo, detenzione e commercio di esemplari di specie animali o vegetali selvatiche protette) e Art. 733-bis c.p. (Distruzione o deterioramento di habitat all'interno di un sito protetto) facenti parte dell'Art. 25-undecies del D. Lgs 231/01 (Reati ambientali) [Leggi notizia completa sul sito]

ULTIMI PROVVEDIMENTI APPORTATI dal D.Lgs. n. 81 del 12 giugno 2025:

"Disposizioni integrative e correttive in materia di adempimenti tributari, concordato preventivo biennale, giustizia tributaria e sanzioni tributarie" Modifiche testo Art. 88 (Circostanze aggravanti del contrabbando) del D. Lgs n.141 del 26 settembre 2024 facente parte dell'Art. 25-sexiesdecies del D. Lgs 231/01 (Contrabbando).

ULTIMI PROVVEDIMENTI APPORTATI dalla L. n.80 del 9 giugno 2025 che ha convertito il D.L. n. 48 dell'11 aprile 2025:

"Disposizioni urgenti in materia di sicurezza pubblica, di tutela del personale in servizio, nonchè di vittime dell'usura e di ordinamento penitenziario";

Introduzione testo Art.270-quinquies.3 c.p. (Detenzione di materiale con finalità di terrorismo), ed introduzione e modifica Art.435 c.p. (Fabbricazione o detenzione di materie esplodenti) facenti parte dell'Art. 25-quater del D. Lgs 231/01 (Delitti con finalità di terrorismo o di eversione dell'ordine democratico);

Tale provvedimento ha comportato anche modifiche all'Art. 640 c.p. (Truffa) facente parte dell'Art. 24 del D. Lgs 231/01 (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).

ELENCO AGGIORNATO DEI REATI PRESUPPOSTO

Art. 24

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 [Articolo modificato dalla L. 161/2017 e dal D.Lgs.n.75 del 14 luglio 2020]

Art. 24-bis

Delitti informatici e trattamento illecito di dati [Articolo aggiunto dalla L. n. 48/2008, modificato dai D.Lgs. n.7 e n. 8/2016, dal D.L. n. 105/2019 e da Legge n.90 del 28 Giugno 2024]

Art. 24-ter

Delitti di criminalità organizzata [Articolo aggiunto dalla L. n. 94/2009, modificato dalla L. 69/2015 e da D.Lgs.n.19 del 2 Marzo 2023]

Art. 25

Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione [Articolo modificato dalla L. n. 190/2012, dalla Legge n. 3 del 9 gennaio 2019 dalD.Lgs.n.75
del 14 luglio 2020 e dalla Legge n.112 dell'8 agosto 2024]

Art. 25-bis

Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento 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.n.125/2016]

Art. 25-bis.1

Delitti contro l'industria e il commercio [Articolo aggiunto dalla L. n. 99/2009]

Art. 25-ter

Reati societari [Articolo aggiunto dal D.Lgs.n.61/2002, modificato dalla L. n. 190/2012, dalla L. 69/2015 e successivamente dal D.Lgs. n.38/2017 e da D.Lgs.n.19 del 2 Marzo 2023]

Art. 25-quater

Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal Codice penale e dalle leggi speciali [Articolo aggiunto dalla L. n. 7/2003]

Art. 25-quater.1

Pratiche di mutilazione degli organi genitali femminili (Art. 583-bis c.p.) [Articolo aggiunto dalla L. n. 7/2006]

Art. 25-quinquies

Delitti contro la personalità individuale [Articolo aggiunto dalla L. n. 228/2003 e modificato dalla L. n. 199/2016]

Art. 25-sexies

Reati di abuso di mercato [Articolo aggiunto dalla L. n. 62/2005] e altre fattispecie in materia di abusi di mercato (Art. 187-quinquies TUF) [articolo modificato dal D.Lgs. n. 107/2018 e dalla Legge n.238 del 23 Dicembre 2021]

Art. 25-septies

Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro [Articolo aggiunto dalla L. n. 123/2007]

Art. 25-octies

Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonchè autoriciclaggio [Articolo aggiunto dal D.Lgs.n.231/2007; modificato dalla L. n. 186/2014 e da D.Lgs.n.195 dell'8 novembre 2021]

Art. 25-octies.1

Delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori [Articolo aggiunto dal D.Lgs.n.184 del 18 novembre 2021e modificato da D.L.10 agosto 2023 n.105 coordinato con la Legge di conversione n.137 del 9 ottobre 2023]

Art. 25-octies.2

Reati in materia di violazione di misure restrittive dell'Unione europea [Articolo aggiunto dal D.Lgs. n.211 del 30 dicembre 2015]

Art. 25-novies

Delitti in materia di violazione del diritto d'autore [Articolo aggiunto dalla L. n. 99/2009]

Art. 25-decies

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria [Articolo aggiunto dalla L. n. 116/2009]

Art. 25-undecies

Reati ambientali [Articolo aggiunto dal D.Lgs.n.121/2011, modificato dalla L. n. 68/2015, dal D.Lgs. n. 21/2018 e dal Decreto Legge n.116 dell'8 agosto 2025]

Art. 25-duodecies

Impiego di cittadini di paesi terzi il cui soggiorno è irregolare [Articolo aggiunto dal D.Lgs.n.109/2012 e modificato dalla Legge n. 161/2017]

Art. 25-terdecies

Razzismo e xenofobia [Articolo aggiunto dalla L. n. 167/ 2017 e modificato dal D.Lgs.n.21/2018]

Art. 25-quaterdecies

Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati [Articolo aggiunto dall'Art.5 della L.n.39/2019]

Art. 25-quinquiesdecies

Reati tributari [Articolo aggiunto dal D.L. n.124/2019 coordinato con Legge di conversione n.157/2019 e modificato dal D.Lgs.n.75/2020)

Art. 25-sexiesdecies

Contrabbando [Articolo aggiunto dal D.Lgs.n.75/2020 e modificato dal D.Lgs. n.141 del 26 settembre 2024]

Art. 25-septiesdecies

Disposizioni in materia di reati contro il patrimonio culturale [Articolo aggiunto da L.n.22 del 09 marzo 2022]

Art. 25-duodevicies

Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici [Articolo aggiunto da L.n.22 del 09 marzo 2022]

Art. 25-undevicies

Delitti contro gli animali [Articolo aggiunto da L. n.82 del 6 giugno 2025]

Art. 26

Delitti tentati

Art. 12, Legge n. 9/2013

Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato [Costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva]

Legge n.146/2006

Reati transnazionali [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]

REVISIONE	DATA DI APPROVAZIONE	NATURA DELLA MODIFICA
Rev. 0	CDA DEL 14.11.2020	ADOZIONE
Rev. 1	CDA DEL 12.11.2021	AGGIORNAMENTO
Rev. 2	CDA DEL 23.03.2022	AGGIORNAMENTO
Rev. 3	CDA DEL 09.01.2023	AGGIORNAMENTO
Rev. 4	CDA DEL 23.05.2023	AGGIORNAMENTO
Rev. 5	CDA DEL 13.11.2023	AGGIORNAMENTO
Rev. 6	CDA DELL'11.07.2024	AGGIORNAMENTO
Rev. 7	CDA DEL 31.12.2025	AGGIORNAMENTO
Rev. 8	CDA DEL 27.07.2026	AGGIORNAMENTO

BIT CONTROL
PROGETTAZIONE E SVILUPPO
SOFTWARE PER L'AUTOMAZIONE

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

- ALLEGATO - 6 -

PROCEDURA INTERNA DI SEGNALAZIONE WHISTLEBLOWING

1. Sommario

*

1. INTRODUZIONE

BitControl S.r.l. opera in un quadro di concorrenza leale, con onestà, integrità, correttezza e buona fede, nel rispetto dei legittimi interessi dei dipendenti, collaboratori, consulenti, clienti, fornitori, partner commerciali e finanziari, nonché nel rispetto delle comunità locali in cui la società svolge la propria attività professionale.

In particolare, la BitControl S.r.l. promuove valori come lealtà, etica, rispetto, merito, eccellenza e innovazione, ma anche sicurezza e tutela della salute dei lavoratori e dell'ambiente.

Invero, la BitControl S.r.l. si ispira ai citati principi per assicurare un rapporto di fiducia con tutti i suoi Stakeholders, ovvero con i propri portatori di interesse, quali dipendenti, collaboratori, consulenti, fornitori e clienti.

L'impegno della BitControl S.r.l. nei riguardi dell'ambiente, è volto a salvaguardarne l'abbondanza e la bellezza per le generazioni presenti e future, con l'obiettivo di trasmettere loro i valori e le tradizioni che sostengono lo sviluppo a lungo termine delle comunità umane e ambientali.

La BitControl S.r.l. si impegna in ogni fase del suo agire: **1)** ad applicare criteri di cautela – il "Principio di Precauzione"– e un approccio preventivo nei riguardi dell'ambiente e della sua biodiversità; **2)** a promuovere iniziative per una maggiore responsabilità ambientale aziendale; **3)** a sviluppare l'impiego di mezzi e di tecnologie che non solo non danneggino l'ambiente, ma che migliorino la sostenibilità ambientale degli impianti nei quali BitControl S.r.l. interviene con la propria attività di progettazione.

Infatti, tutti coloro che lavorano o operano in Italia e all'estero per conto o in favore di BitControl S.r.l. sono chiamati ad operare nel pieno rispetto dei suddetti principi e valori, nonché ad osservare ed a fare osservare tali principi nell'ambito delle proprie funzioni e responsabilità. In nessun modo la convinzione di agire nell'interesse e/o a vantaggio della Società può giustificare l'adozione di comportamenti in contrasto con i suddetti principi e valori sui quali si fonda l'attività della BitControl S.r.l..

Per tale ragione, la corruzione è un ostacolo intollerabile alla capacità della Società di fare Business ed, infatti, la BitControl S.r.l. promuove una leale competizione per il perseguimento del proprio interesse a garanzia dei propri clienti, dei fornitori e degli stakeholders in genere.

Invero, per la BitControl S.r.l. il puntuale rispetto delle leggi e dei regolamenti, l'integrità etica, la correttezza, trasparenza ed onestà sono un impegno ed un dovere costante e continuativo di tutto il personale della società e, pertanto, la stessa contrasta e condanna il ricorso a comportamenti illegittimi o comunque scorretti per raggiungere gli obiettivi economici che si è data, obiettivi che sono perseguiti esclusivamente con l'eccellenza delle proprie performance in termini di innovazione, qualità, sostenibilità economica, sociale e ambientale.

La BitControl S.r.l. conferma, altresì, il proprio impegno nella lotta alla corruzione in ogni sua forma, attraverso un costante rafforzamento del grado di integrità e trasparenza nei comportamenti interni in modo da influire positivamente sulla reputazione della stessa Azienda nei contesti in cui opera.

2. OBIETTIVO

La presente Procedura, che costituisce parte integrante del Modello 231/01 adottato dalla BitControl S.r.l. ha la finalità di:

• regolamentare il processo di "Whistleblowing";

• definire i ruoli, compiti e responsabilità dei soggetti coinvolti nel suddetto processo;

• definire chi può segnalare, cosa può essere segnalato e con quali tutele;

• disciplinare canali scritti e orali idonei a garantire la riservatezza;

• regolare ricezione, valutazione preliminare, istruttoria, riscontro e chiusura;

• prevenire e gestire conflitti di interessi, assenze e indisponibilità del Gestore;

• assicurare conformità al D.Lgs. 24/2023, alle Linee Guida ANAC n. 1/2025 e alla normativa in materia di protezione dei dati personali;

• integrare il sistema whistleblowing con il Modello 231 e con i processi aziendali di compliance.

La presente Procedura disciplina il canale interno di segnalazione della Società ai sensi del D.Lgs. 10 marzo 2023, n. 24, recante attuazione della Direttiva (UE) 2019/1937, e delle Linee Guida ANAC n. 1/2025 (Delibera n. 478 del 26 novembre 2025). Essa si applica alle segnalazioni di violazioni rilevanti ai sensi del citato decreto, apprese nel contesto lavorativo, incluse le violazioni del diritto dell'Unione, delle disposizioni normative nazionali richiamate dal decreto, del Modello 231, del Codice Etico e delle procedure interne rilevanti ai fini della prevenzione degli illeciti.

La presente Procedura sostituisce e aggiorna ogni precedente disciplina interna in materia di whistleblowing fondata esclusivamente sulla Legge 30 novembre 2017, n. 179 e sulla previgente formulazione dell'art. 6, comma 2-bis, del D.Lgs. 231/2001. Restano ferme le disposizioni del Modello 231 in quanto compatibili con la nuova normativa.

3 PROFILO E AMBITO DI APPLICAZIONE DI BITCONTROL S.R.L.

BitControl opera nella progettazione, sviluppo, integrazione, assistenza e manutenzione di soluzioni informatiche e di automazione per sistemi di telecontrollo, supervisione e controllo. Le attività comprendono, tra l'altro, sistemi SCADA e MES, programmazione e configurazione di PLC, RTU e DCS, infrastrutture di comunicazione industriale e M2M, telemetria e IoT, integrazione di applicazioni e banche dati, gestione dati e reportistica, software su specifica del cliente, formazione e facility management evolutivo.

La Società opera sul mercato nazionale e internazionale per utilities e multiutilities pubbliche e private, industrie e gestori nei settori acqua, energia e gas, nonché in ambiti industriali e di processo, petrolchimico, farmaceutico, ambientale, idrico, depurazione e potabilizzazione, reti elettriche, irrigazione, building e infrastrutture critiche.

In relazione a tale operatività, possono assumere particolare rilievo, a titolo esemplificativo, segnalazioni riguardanti:

1. rapporti con pubbliche amministrazioni, stazioni appaltanti, gestori di servizi pubblici e clienti a partecipazione pubblica;
2. gare, affidamenti, subappalti, forniture, consulenze, partnership e rapporti con intermediari;
3. corruzione, frodi, conflitti di interessi, omaggi o utilità indebite;
4. sicurezza informatica, accessi abusivi, alterazione o perdita di dati, vulnerabilità di sistemi di telecontrollo e infrastrutture critiche;
5. violazioni in materia di salute e sicurezza sul lavoro, ambiente, rifiuti, cantieri e attività presso siti dei clienti;
6. violazioni relative a proprietà intellettuale, licenze software, segreti industriali, know-how e riservatezza;
7. violazioni contabili, fiscali, societarie, antiriciclaggio, pagamenti e tracciabilità;
8. violazioni del Modello 231, Codice Etico, Politica Anticorruzione e procedure aziendali.

4. RIFERIMENTI NORMATIVI

Per la redazione della presente procedura sono stati adottati riferimenti normativi sia esterni che interni.

I riferimenti normativi esterni sono:

➢ D.lgs. dell'8 giugno 2001, n. 231 "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300";

➢ Linee guida per la costruzione dei Modelli di Organizzazione, Gestione e Controllo ex D.lgs. 231/01 emanate da Confindustria in data 7 marzo 2002 (aggiornate al 31 marzo 2014);

➢ D.lgs. del 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali", così come modificato dal D.lgs. 101/2018 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";

➢ Legge 30 novembre 2017, n. 179 "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*" **abrogata e sostituita dal D.Lgs. 24/2023 per le disposizioni relative al settore privato;**

- 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;

- Decreto Legislativo 10 marzo 2023, n. 24, recante attuazione della Direttiva (UE) 2019/1937 e disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali;

- Linee Guida ANAC n. 1/2025 in materia di whistleblowing sui canali interni di segnalazione, adottate con Delibera n. 478 del 26 novembre 2025;

Regolamento (UE) 2016/679 (GDPR) e D.Lgs. 196/2003 s.m.i., in materia di protezione dei dati personali.

Invero, la Legge 30 novembre 2017, n. 179 recante "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*" aveva previsto un sistema di tutela sia per i lavoratori appartenenti al settore pubblico che per i lavoratori appartenenti al settore privato, nonché per i terzi che segnalino un illecito di cui abbiano avuto conoscenza per ragioni di lavoro.

In particolare la suddetta Legge, aggiungendo i nuovi commi 2 bis, 2 ter e 2 quater all'art. 6 del D.lgs. 231/01, ha introdotto anche nel settore privato talune tutele (ad es. divieto di atti ritorsivi o discriminatori per i motivi collegati, direttamente o indirettamente, alla Segnalazione etc…) nei confronti dei soggetti apicali e/o dei loro subordinati che segnalino condotte illecite, rilevanti ai sensi del D.lgs. 231/01 o violazioni del relativo Modello 231/01, di cui siano venuti a conoscenza in ragione del loro ufficio.

A tal fine, il Modello di organizzazione e gestione adottato ai sensi del D.lgs. 231/01 prevede, quale proprio requisito di idoneità, l'implementazione di una apposita procedura, che è parte integrante del medesimo Modello 231/01, finalizzata a disciplinare il predetto sistema di segnalazione di illeciti e violazioni del Modello 231/01 (c.d. whistleblowing).

I riferimenti normativi interni sono:

➢ Statuto;

➢Modello di Organizzazione, Gestione e Controllo ex. D.lgs. 231/01 di BitControl S.r.l.;

➢ Codice Etico di BitControl S.r.l.

5. VIOLAZIONI SEGNALABILI ED ESCLUSIONI

Sono segnalabili informazioni, compresi fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse, nonché condotte volte ad occultarle. Rientrano, nei limiti applicabili a BitControl:

1. illeciti rilevanti ai sensi del D.Lgs. 231/2001 e violazioni del Modello 231;
2. illeciti che rientrano negli ambiti del diritto dell'Unione indicati dal D.Lgs. 24/2023, inclusi appalti pubblici, sicurezza dei prodotti e dei trasporti, tutela dell'ambiente, salute pubblica, protezione dei consumatori, privacy, sicurezza delle reti e dei sistemi informativi;
3. atti od omissioni che ledono gli interessi finanziari dell'Unione o riguardano il mercato interno;
4. violazioni del Codice Etico, della Politica Anticorruzione e di procedure interne quando connesse agli illeciti tutelati o rilevanti ai fini del Modello 231.

Non rientrano nel perimetro protetto le contestazioni, rivendicazioni o richieste legate esclusivamente a un interesse personale del segnalante e ai rapporti individuali di lavoro, salvo che siano collegate a una violazione rilevante; i reclami commerciali o tecnici privi di profili di illecito; le informazioni classificate o coperte dai segreti e dalle esclusioni previste dall'art. 1 del D.Lgs. 24/2023; le segnalazioni fondate esclusivamente su voci prive di elementi concreti.

6 SOGGETTI CHE POSSONO EFFETTUARE LE SEGNALAZIONI E OGGETTO DELLA SEGNALAZIONE

I componenti del Consiglio di Amministrazione, i dipendenti e i soggetti terzi possono segnalare i comportamenti illeciti di cui al D.lgs. 231/01, rilevanti in sede penale e/o disciplinare, di cui siano venuti a conoscenza, diretta o indiretta, durante lo svolgimento delle proprie funzioni.

In particolare, possono effettuare segnalazioni interne i soggetti legittimati ai sensi del D.Lgs. 24/2023, in quanto persone che operano nel contesto lavorativo della Società, ivi inclusi:

- lavoratori subordinati;
- lavoratori autonomi, collaboratori, consulenti, liberi professionisti che svolgono la propria attività lavorativa presso la Società;
- volontari e tirocinanti, retribuiti e non retribuiti;
- persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto;
- i soggetti che operano presso fornitori, subappaltatori e subfornitori della Società;
- i soggetti le cui segnalazioni riguardano violazioni apprese durante il processo di selezione o in altre fasi precontrattuali, o durante il periodo di prova.

Pertanto, può costituire oggetto di Segnalazione ogni comportamento, atto o fatto che integri o possa integrare una violazione rilevante ai sensi del D.Lgs. 24/2023, ivi incluse le violazioni del diritto dell'Unione europea, delle disposizioni normative nazionali richiamate dal decreto, del Modello 231, del Codice Etico e delle procedure interne rilevanti, di cui il Segnalante sia venuto a conoscenza nell'ambito del proprio contesto lavorativo.

Pertanto, può costituire oggetto di Segnalazione ogni comportamento, atto o fatto idoneo a pregiudicare l'idoneità del Modello, posto in essere dai soggetti sopra indicati nell'interesse o a vantaggio della Società, che costituisca, anche solo potenzialmente:

➢ una condotta illecita integrante una o più fattispecie di reato da cui può derivare una responsabilità per la Società ai sensi del D.lgs. 231/01;

➢ una condotta che, pur non integrando alcuna predetta fattispecie di reato, sia stata posta in essere in violazione delle prescrizioni del Modello e del Codice Etico della società.

Le Segnalazioni che determinano l'attivazione della presente Procedura devono basarsi su elementi di fatto, precisi e concordanti.

Non rientrano nell'ambito della presente Procedura le contestazioni, rivendicazioni o richieste connesse a un interesse di carattere esclusivamente personale della persona segnalante che attengano ai propri rapporti individuali di lavoro, di impiego pubblico o ai rapporti con il superiore gerarchico o con i colleghi, salvo che esse siano connesse o collegate a violazioni rilevanti ai sensi del D.Lgs. 24/2023

Non sono, pertanto, meritevoli di tutela le Segnalazioni aventi ad oggetto questioni di carattere personale del Segnalante o del Segnalato - salvo che non si tratti di aspetti che abbiano un impatto a livello aziendale -, rivendicazioni o istanze attinenti alla disciplina del rapporto di lavoro o rapporti con il superiore gerarchico o con i colleghi. Pertanto, a titolo meramente esemplificativo e non esaustivo, la procedura di Segnalazione, con le relative tutele, non sarà attivata, anche se la Segnalazione sarà inviata/recapitata tramite le modalità previste dal presente documento, nelle seguenti ipotesi:

• Segnalazione non circostanziata che non consente di individuare elementi di fatto ragionevolmente sufficienti per avviare un'istruttoria (ad es.: **1)** illecito commesso; **2)** periodo di riferimento; **3)** cause e finalità dell'illecito; **4)** persone/unità coinvolte, etc.), ovvero qualora si tratti di segnalazioni fondate su meri sospetti o voci;

• Segnalazione priva di fondamento, ovvero fatta allo scopo di danneggiare o recare pregiudizio alla/e persona/e segnalata/e.

Dunque, a tutela del soggetto Segnalato, rimane fermo il requisito della veridicità dei fatti, delle circostanze e delle situazioni che sono oggetto di segnalazione. A tal fine, non è necessario che il

Segnalante sia certo dell'effettivo avvenimento, o del carattere illecito, dei fatti segnalati e/o dell'autore degli stessi, essendo, invece, sufficiente che il Segnalante, in base alle proprie conoscenze, ritenga altamente probabile che si sia verificato un fatto e che lo stesso possa costituire un illecito. Invero, lo scopo della norma è proprio quello di incentivare la collaborazione di chi lavora all'interno della Società per fare emergere fenomeni corruttivi o illeciti.

Le Segnalazioni anonime, vale a dire prive di elementi che consentano di identificare il loro autore, anche se recapitate tramite le modalità previste dal presente documento, potranno essere prese in considerazione ai fini della presente Procedura qualora esse presentino gli elementi sopra indicati.

sono registrate e conservate dal Gestore al fine di consentirne il reperimento qualora la persona segnalante o chi abbia sporto denuncia comunichi all'ANAC di aver subìto misure ritorsive a causa di quella segnalazione o denuncia anonima, ai sensi dell'art. 16, comma 4, del D.Lgs. 24/2023.

Le Segnalazioni anonime potranno essere prese in considerazione per ulteriori verifiche solo se aventi un contenuto adeguatamente dettagliato e circostanziato.

Il perseguimento dell'interesse all'idoneità del Modello 231 e alla prevenzione delle violazioni rilevanti ai sensi del D.Lgs. 24/2023, che con la presente Procedura la Società intende perseguire, costituisce giusta causa di rivelazione di notizie coperte dall'obbligo del segreto, con riferimento alle fattispecie di reato di cui agli artt. 326 c.p. (Rivelazione ed utilizzazione di segreti d'ufficio), 622 c.p. (Rivelazione di segreto professionale) e 623 c.p. (Rivelazione di segreti scientifici o industriali), oltreché in relazione all'obbligo di fedeltà del dipendente di cui all'art. 2105 c.c. nei limiti e alle condizioni previsti dal D.Lgs. 24/2023.

Tale clausola di salvezza delle condotte rivelatorie non si applica, tuttavia, se l'obbligo di segreto professionale sia riferibile ad un rapporto di consulenza professionale o di assistenza, ovvero se la rivelazione sia stata effettuata con modalità eccedenti rispetto alle finalità di eliminazione dell'illecito, con particolare riferimento al rispetto del canale di comunicazione a tal fine specificamente predisposto.

7. DESTINATARIO DELLA SEGNALAZIONE – GESTORE INTERNO

Il canale interno di segnalazione è gestito dal soggetto formalmente individuato dalla Società nell'atto organizzativo/Modello 231 quale Gestore del canale interno (di seguito "Gestore"), dotato di autonomia, imparzialità, specifica formazione e autorizzazione al trattamento dei dati personali ai fini della gestione delle segnalazioni.

Il Gestore del canale interno della BitControl S.r.l. è l'Organismo di Vigilanza. Qualora la gestione sia affidata all'Organismo di Vigilanza, la Società disciplina espressamente nell'atto organizzativo/Modello

231 i casi di conflitto di interessi, incompatibilità, astensione e sostituzione temporanea o prolungata del Gestore.

Il Gestore è l'unico soggetto che può ricevere la segnalazione e compiere le attività necessarie a darvi seguito. Nell'ipotesi in cui un diverso soggetto interno riceva per errore la segnalazione, dovrà trasmetterla al Gestore entro sette giorni, in conformità all'art. 4, comma 6, del D.Lgs. 24/2023, nel rispetto della riservatezza del Segnalante e del contenuto della segnalazione.

Il Gestore provvede a garantire la riservatezza delle informazioni contenute nelle Segnalazioni ed a tutelare l'identità dei Segnalanti agendo in modo da garantirli contro qualsiasi forma di ritorsione o comportamento discriminatorio, diretto o indiretto, per motivi collegati, direttamente o indirettamente, alle stesse Segnalazioni.

Il Gestore:

1. riceve le segnalazioni e rilascia l'avviso di ricevimento entro sette giorni;
2. mantiene le interlocuzioni con il segnalante e richiede integrazioni quando necessario;
3. dà diligente seguito alla segnalazione e conduce o coordina l'istruttoria;
4. fornisce riscontro entro tre mesi;
5. assicura riservatezza, tracciabilità, corretta conservazione e limitazione degli accessi;
6. segnala agli organi competenti gli esiti che richiedono misure correttive, disciplinari o ulteriori approfondimenti, senza comunicare dati identificativi non necessari.

Chiunque riceva per errore una segnalazione deve trasmetterla al Gestore entro sette giorni, utilizzando modalità sicure, dando contestuale notizia della trasmissione al segnalante e astenendosi da ogni ulteriore trattamento o divulgazione.

7.1 CONTENUTO DELLE SEGNALAZIONI

Il soggetto che effettua la Segnalazione deve fornire tutti gli elementi utili e necessari per consentire all'OdV di condurre un'istruttoria procedendo alle verifiche e agli accertamenti del caso, al fine di valutare la ricevibilità e la fondatezza della Segnalazione che deve contenere i seguenti elementi:

a) generalità del soggetto che effettua la Segnalazione con indicazione della qualifica ricoperta e/o della funzione/attività svolta nell'ambito della Società (generalità che saranno tenute riservate dall'OdV);

b) una chiara e completa descrizione dei fatti precisi e concordanti oggetto di Segnalazione che costituiscano o possano costituire una violazione rilevante ai sensi del D.Lgs. 24/2023 e/o un illecito rilevante ai fini del D.Lgs. 231/01 e/o una violazione del Modello e/o del Codice Etico;

un illecito rilevante ai fini del D.lgs. 231/01 e/o una violazione del Modello e/o del Codice Etico;

c) se conosciute, le circostanze di tempo e di luogo in cui sono stati commessi i fatti oggetto della Segnalazione;

d) se conosciute, le generalità o altri elementi che consentano di identificare il soggetto e/o i soggetti che hanno posto in essere i fatti segnalati (ad esempio qualifica ricoperta e area in cui svolge l'attività);

e) l'indicazione di eventuali altri soggetti che possono riferire sui fatti oggetto di Segnalazione;

f) l'indicazione di eventuali documenti che possono confermare la fondatezza dei fatti oggetto di Segnalazione;

g) ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti oggetto di Segnalazione ed in genere ogni altra informazione o documento che possa essere utile a comprendere i fatti segnalati.

Ai fini di cui sopra, deve essere utilizzato il modulo di cui all'Allegato A della presente Procedura, fermo restando che in ogni caso l'OdV, in sede di istruttoria, potrà richiedere al Segnalante un'integrazione della documentazione che riterrà opportuna o necessaria a corredo della Segnalazione.

7.2 MODALITÀ DI SEGNALAZIONE

La Società, al fine di agevolare l'invio e la ricezione delle Segnalazioni, predispone i seguenti alternativi canali di comunicazione:

a) L'utilizzo della posta elettronica ordinaria (PEO) o certificata (PEC) non costituisce canale standard di segnalazione. In conformità alle Linee Guida ANAC n. 1/2025, la posta elettronica può essere utilizzata solo ove assistita da adeguate misure di mitigazione tecniche e organizzative — incluse crittografia end-to-end e autenticazione a due fattori (2FA) — opportunamente individuate attraverso una specifica valutazione d'impatto sulla protezione dei dati (DPIA). In tali casi, la casella email dedicata al Whistleblowing, gestita esclusivamente dal Gestore, rimane: organismodivigilanza@bitcontrol.it, accessibile esclusivamente previo adozione delle misure di mitigazione sopra indicate.

b) lettera recapitata in busta chiusa indirizzata presso la sede legale della Società in via Stazione n. 39, 95047, Paternò (CT), indirizzata all'attenzione dell'Organismo di Vigilanza con la dicitura "**RISERVATA PERSONALE**"; all'interno della busta contenente la Segnalazione deve essere inserita un'altra busta che può contenente i dati identificativi (parte I del modulo di cui all'Allegato A) del Segnalante. Tale busta deve essere tempestivamente recapitata all'OdV, il quale provvederà a conservarla ed archiviarla sotto la propria responsabilità.

c) lettera recapitata in busta chiusa indirizzata presso il domicilio eletto dall'ODV in via E. Bellia n. 35, 95047, Paternò (CT), indirizzata all'attenzione dell'Organismo di Vigilanza con la dicitura "**RISERVATA PERSONALE**"; all'interno della busta contenente la Segnalazione deve essere inserita

un'altra busta che può contenente i dati identificativi (parte I del modulo di cui all'Allegato A) del Segnalante. In tal caso, l'OdV, provvederà a conservarla ed archiviarla sotto la propria responsabilità.

7.3 VERIFICA DELLA SEGNALAZIONE

Il Gestore provvede esegue l'istruttoria necessaria a verificare la fondatezza e la rilevanza della Segnalazione, nel rispetto dei principi di imparzialità e di riservatezza, nonché nel rispetto della normativa giuslavoristica ed in tema di privacy.

Il procedimento si suddivide in diverse fasi.

FASE 1 — AVVISO DI RICEVIMENTO (entro 7 giorni)

Il Gestore è tenuto a rilasciare alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione, ai sensi dell'art. 5, comma 1, lett. a), del D.Lgs. 24/2023. L'avviso non implica alcuna valutazione dei contenuti oggetto della segnalazione, ma assume carattere meramente informativo nei confronti della persona segnalante con riferimento alla ricezione e presa in carico della segnalazione. L'avviso è comunicato mediante la piattaforma informatica o, in caso di mancato utilizzo della piattaforma, al recapito indicato dalla persona segnalante.

FASE 2 — ESAME PRELIMINARE DELLA SEGNALAZIONE

Ricevuta la segnalazione, il Gestore verifica preliminarmente:

(i) la legittimazione soggettiva della persona segnalante ai sensi del D.Lgs. 24/2023;

(ii) la riconducibilità dell'oggetto della segnalazione all'ambito di applicazione del D.Lgs. 24/2023 (presupposti oggettivi);

(iii) la sufficiente specificità dei fatti esposti che essi siano circostanziati.

Qualora la segnalazione non rientri nell'ambito del whistleblowing, il Gestore potrà trasmetterla, nel rispetto della riservatezza, al competente soggetto/ufficio interno che la tratterà, ove previsto, come segnalazione ordinaria, dandone contestualmente comunicazione alla persona segnalante.

FASE 3 — ISTRUTTORIA

Il Gestore assicura, altresì, la predisposizione di un report periodico di tutte le Segnalazioni ricevute, sugli esiti delle verifiche relative a tali Segnalazioni nonché sui casi di archiviazione, avendo cura di mantenere riservati i dati identificativi del Segnalante.

Il Gestore, in quanto preposto alla verifica e alla gestione della Segnalazione, può procedere ad ogni attività ritenuta opportuna al fine di:

➢ valutare la gravità degli illeciti, delle violazioni e delle irregolarità segnalate e ad ipotizzarne le potenziali conseguenze pregiudizievoli;

➢ individuare le attività da svolgere in relazione alle tematiche segnalate con riferimento al Modello 231;

➢ effettuare le attività di accertamento circa l'effettiva commissione dell'illecito e/o dell'irregolarità, valutando ad esempio l'opportunità di:

- convocare il Segnalante per ottenere maggiori chiarimenti;
- convocare i soggetti che nella Segnalazione sono indicati come persone informate sui fatti;
- acquisire documentazione utile o attivarsi per poterla rinvenire ed acquisire;
- convocare, ove ritenuto opportuno, il soggetto indicato nella Segnalazione come l'autore dell'irregolarità (cd. Segnalato);

➢ individuare, ove necessario, gli accorgimenti da adottare immediatamente al fine di ridurre il rischio che si verifichino eventi pregiudizievoli o eventi simili a quelli segnalati, verificati o accertati.

Il Gestore mantiene le interlocuzioni con la persona segnalante e può richiedere, se necessario, integrazioni, chiarimenti o documentazione ulteriore, ai sensi dell'art. 5, comma 1, lett. b), del D.Lgs. 24/2023.

Nell'istruttoria delle Segnalazioni l'OdV può avvalersi del supporto e della collaborazione di funzioni ed uffici della Società ed in particolare del Responsabile delle Risorse Umane, o di consulenti esterni, assicurando, anche in tal caso, la massima riservatezza. Qualora all'esito dell'istruttoria, la Segnalazione dovesse risultare fondata e rilevante ai sensi del D.lgs. 231/01, l'OdV provvederà a comunicare l'esito dell'accertamento ad uno o più dei seguenti soggetti, in relazione alle circostanze della fattispecie concrete:

a. al Consiglio di Amministrazione;

b. al Responsabile dell'area Risorse Umane;

I soggetti di cui alle precedenti lett. a) e b) provvederanno, a loro volta, ad informare il Gestore in merito agli eventuali provvedimenti adottati a seguito dell'accertamento dell'illecito, della violazione o dell'irregolarità segnalata.

Nel caso in cui all'esito dell'istruttoria, la Segnalazione dovesse risultare non rilevante ai fini del D.lgs. 231/01 o ai fini delle prescrizioni contenute nel Modello 231, il Gestore provvederà ad inoltrare la Segnalazione ricevuta alla Funzione aziendale competente e nei casi in cui non sia possibile individuare univocamente la Funzione aziendale competente, provvederà ad inviarla al RHR.

Qualora la Segnalazione dovesse apparire infondata o irrilevante, il Gestore provvederà ad archiviarla precisandone le relative motivazioni; tale decisione è comunicata ai soggetti di cui alle precedenti lett. a) e b).; resta fermo l'esercizio di eventuali azioni nei confronti del Segnalante da parte degli organi e/o

delle funzioni competenti. Nel caso in cui la Segnalazione riguardi un illecito già oggetto di un procedimento penale, l'attività istruttoria di cui alla presente Procedura rimarrà sospesa sino alla definizione del giudizio penale.

FASE 4 — RISCONTRO FINALE (entro 3 mesi)

Il Gestore è tenuto a fornire riscontro alla persona segnalante entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione, ai sensi dell'art. 5, comma 1, lett. d), del D.Lgs. 24/2023.

Il Gestore assicura, altresì, la predisposizione di un report periodico di tutte le Segnalazioni ricevute, sugli esiti delle verifiche relative a tali Segnalazioni nonché sui casi di archiviazione, avendo cura di mantenere riservati i dati identificativi del Segnalante, salvo che i dati stessi non siano in altro modo già emersi o comunque già noti.

Al fine di garantire la corretta gestione e la tracciabilità delle Segnalazioni e della relativa attività di istruttoria, l'OdV archivia per almeno 5 anni dalla conclusione del procedimento, nel rispetto degli standard di sicurezza e riservatezza, tutta la documentazione relativa alla Segnalazione ricevuta, alla gestione ed agli esiti della stessa (email, comunicazioni, pareri di esperti, verbali, documentazione allegata, ecc.).

7.4 TUTELA DEL SEGNALANTE

a) Obbligo di riservatezza.

L'identità della persona segnalante, delle persone coinvolte e delle persone comunque menzionate nella segnalazione, nonché il contenuto della segnalazione e la relativa documentazione, sono trattati nel rispetto dell'obbligo di riservatezza previsto dal D.Lgs. 24/2023 e delle norme in materia di protezione dei dati personali.

Fatti salvi i casi in cui, una volta esperita l'istruttoria, sia configurabile una responsabilità a titolo di calunnia o di diffamazione ai sensi del codice penale o dell'art. 2043 del c.c. e delle ipotesi in cui il riserbo sulle generalità non sia opponibile per legge (es. indagini penali, tributarie o amministrative, ispezioni di organi di controllo), l'identità del Segnalante viene protetta in ogni fase del trattamento della Segnalazione.

Pertanto, fatte salve le eccezioni di cui sopra, l'identità del Segnalante non può essere rivelata senza il suo previo consenso espresso e, nei casi di cui all'art. 12, comma 5, del D.Lgs. 24/2023, senza previa comunicazione scritta al Segnalante delle motivazioni che rendono necessario il disvelamento della sua identità. Tutti coloro che ricevono o sono coinvolti nella gestione della Segnalazione sono tenuti a tutelare la riservatezza di tale informazione.

b) Divieto di discriminazione.

I soggetti che, a norma della presente Procedura, segnalano condotte illecite o violazioni del Modello 231/01 di cui siano venuti a conoscenza in ragione del loro ufficio, non possono essere sanzionati, licenziati, revocati, sostituiti, trasferiti o sottoposti ad alcuna misura discriminatoria per motivi collegati, direttamente o indirettamente, alla Segnalazione. Per misure ritorsive si intendono le azioni od omissioni, anche solo tentate o minacciate, che derivano dalla segnalazione e che provocano o possono provocare alla persona segnalante un danno ingiusto, ivi incluse: azioni disciplinari ingiustificate, molestie sul luogo di lavoro, licenziamento, demansionamento, trasferimento, mancata conversione di contratto a termine, mancata concessione di permessi, ogni altra forma di ritorsione e/o reazione sfavorevole.

È vietata qualsiasi forma di ritorsione, anche solo tentata o minacciata, nei confronti della persona segnalante e degli altri soggetti protetti ai sensi del D.Lgs. 24/2023 (tra cui i facilitatori, i colleghi e i familiari della persona segnalante), quando ricorrono i presupposti di legge.

La persona segnalante che ritenga di aver subìto una ritorsione può comunicarlo all'ANAC secondo le modalità previste dal D.Lgs. 24/2023.

Gli atti e i provvedimenti adottati in violazione del divieto di ritorsione sono nulli ai sensi di quanto previsto dal D.Lgs. 24/2023.

Il Segnalante che ritenga di aver subìto una misura ritorsiva provvede a dare notizia circostanziata dell'avvenuta ritorsione al Gestore affinché provveda a valutarne la fondatezza, nonché, ai sensi del D.Lgs. 24/2023, all'ANAC per i provvedimenti di relativa competenza.

Nel caso in cui l'Organismo di Vigilanza ritenga integrata la discriminazione valuta – con l'ausilio del Responsabile delle Risorse Umane- possibili interventi di azione da parte degli organi e/o delle Funzioni competenti della Società, volti a ripristinare la situazione di regolarità e/o per rimediare agli effetti negativi della discriminazione e, far perseguire, se del caso, in via disciplinare e/o penale, l'autore della discriminazione o ritorsione.

In ogni caso la violazione dell'obbligo di riservatezza e/o del divieto di discriminazione o ritorsione di cui sopra è fonte di responsabilità disciplinare anche secondo quanto previsto dal sistema disciplinare adottato ai sensi della parte Generale del Modello 231/01 adottato dalla Società e del D.lgs. 231/01 e al D.Lgs. 24/2023, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

7.5 RESPONSABILITÀ DEL SEGNALANTE

Il Segnalante è consapevole delle responsabilità e delle conseguenze civili e penali previste in caso di dichiarazioni mendaci e/o di formazione o di uso di atti falsi.

Ai sensi dell'art. 16 del D.Lgs. 24/2023, qualora sia accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di calunnia o diffamazione, ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele previste dal presente decreto non si applicano e alla persona segnalante può essere irrogata una sanzione disciplinare.

Qualora a seguito di verifiche interne la Segnalazione risulti priva di fondamento saranno effettuati da parte del Responsabile dell'Area Risorse Umane accertamenti sulla sussistenza di grave colpevolezza o dolo circa l'indebita Segnalazione e, di conseguenza, in caso affermativo, si darà corso alle azioni disciplinari, ai sensi del sistema sanzionatorio adottato in conformità al Modello 231/01 e al D.Lgs. 24/2023 e/o denunce anche penali nei confronti del Segnalante salvo che questi non produca ulteriori elementi a supporto della propria Segnalazione.

8. ARCHIVIAZIONE DELLA DOCUMENTAZIONE

Le segnalazioni interne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni dalla data della comunicazione dell'esito finale della procedura di segnalazione, in conformità all'art. 14 del D.Lgs. 24/2023.

L'accesso alla documentazione è consentito esclusivamente ai soggetti espressamente autorizzati alla gestione delle segnalazioni. La documentazione è archiviata nel rispetto degli standard di sicurezza e riservatezza, garantendo l'integrità e la non alterabilità dei dati.

Tutta la documentazione di supporto relativa alle attività descritte nella presente Procedura, cartacea e/o elettronica (i.e. e mail), deve essere correttamente depositata in archivi, per la durata prevista dalla legge in vigore, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi.

La documentazione relativa alle eventuali azioni disciplinari indicate al par. 7.5 sarà archiviata in modalità cartacea in apposito raccoglitore ed in modalità digitale all'interno di una cartella catalogata sul server aziendale utilizzata ed accessibile esclusivamente dalla Funzione Risorse Umane.

9. GOVERNO DELLA PROCEDURA E SISTEMA DI SEGNALAZIONE

Le responsabilità in termini di aggiornamento, modifica, approvazione, distribuzione e conservazione della Procedura sono del Consiglio di Amministrazione.

Tutti coloro che venissero a conoscenza direttamente o indirettamente di fatti e/o comportamenti non conformi alle disposizioni descritte, devono effettuare una Segnalazione direttamente all'Organismo di Vigilanza secondo le modalità e i canali previsti dal Modello 231/01.

In dettaglio:

a. qualora si verifichino circostanze:

• non espressamente regolamentate dalla Procedura;

• che si prestano a dubbie interpretazioni/applicazioni;

• tali da originare obiettive e gravi difficoltà di applicazione della Procedura medesima;

ciascun dipendente della Società è tenuto ad esprimerli tempestivamente al Responsabile dell'Area Legale;

b. tutti coloro – invece – che venissero a conoscenza direttamente o indirettamente di fatti e/o comportamenti non conformi alle disposizioni descritte, devono effettuare una Segnalazione al Gestore.

Per maggiori dettagli sul sistema di rilevamento degli illeciti e segnalazioni all'Organismo di Vigilanza si rimanda a quanto definito nel Modello 231/01.

Sistema disciplinare. Il sistema disciplinare della Società, adottato ai sensi del Modello 231/01, è aggiornato per prevedere specifiche sanzioni disciplinari, graduate in ragione della gravità della condotta, nei confronti dei soggetti responsabili di:

- ritorsioni nei confronti della persona segnalante o degli altri soggetti protetti;
- ostacolo o tentato ostacolo alla segnalazione;
- violazione dell'obbligo di riservatezza sull'identità della persona segnalante;
- mancata gestione conforme del canale interno;
- effettuazione di segnalazioni con dolo o colpa grave accertata ai sensi del D.Lgs. 24/2023.

10. CANALE ESTERNO ANAC E DIVULGAZIONE PUBBLICA

La presente Procedura disciplina il canale interno di segnalazione e non limita in alcun modo il diritto della persona segnalante di avvalersi, ricorrendone i presupposti di legge, del canale esterno istituito presso l'ANAC, della denuncia all'autorità giudiziaria o contabile, ovvero della divulgazione pubblica, secondo le condizioni previste dagli artt. 6 e 15 del D.Lgs. 24/2023.

La Società informa in modo chiaro e accessibile, sul sito istituzionale (ove disponibile) e nei luoghi di lavoro, circa la possibilità di effettuare segnalazioni anche mediante il canale esterno istituito presso ANAC, nonché circa i presupposti normativi della divulgazione pubblica e della denuncia all'autorità giudiziaria o contabile.

Si rammenta, in particolare, che la persona segnalante può ricorrere direttamente al canale esterno ANAC, tra l'altro, nei seguenti casi previsti dall'art. 6 del D.Lgs. 24/2023:

- non è previsto, nell'ambito del contesto lavorativo, l'obbligo di attivare canali di segnalazione interna, ovvero questo canale non è attivo o non è conforme;
- la persona segnalante ha già effettuato una segnalazione interna e non è stato dato seguito nei termini previsti;
- la persona segnalante ha fondato motivo di ritenere che la segnalazione interna possa non avere efficace seguito o possa determinare il rischio di ritorsioni.

Resta salvo il dovere di rivolgersi all'Autorità Giudiziaria laddove ne ricorrano i presupposti.

11. FORMAZIONE E PUBBLICITÀ INTERNA

La Società assicura:

1. la diffusione della presente Procedura a tutti i destinatari, mediante pubblicazione nell'intranet aziendale e/o comunicazione diretta;
2. la pubblicazione sul sito istituzionale — ove disponibile — delle informazioni essenziali sull'utilizzo del canale interno e del canale esterno ANAC, con indicazione chiara delle modalità di presentazione e dei presupposti per effettuare le segnalazioni, ai sensi dell'art. 5, comma 1, lett. e), del D.Lgs. 24/2023;
3. l'esposizione nei luoghi di lavoro delle informazioni relative al canale di segnalazione interna, in forma facilmente visibile e accessibile;
4. l'erogazione di specifiche attività formative al personale, con particolare riguardo ai soggetti incaricati della gestione delle segnalazioni, volte a garantire la corretta applicazione della presente Procedura e del D.Lgs. 24/2023.

Allegato A

Modulo per la Segnalazione ~~di condotte illecite o violazioni del Modello di cui al D.lgs. 231/01~~

ALLEGATI

Modulo per la segnalazione di violazioni rilevanti ai sensi del D.Lgs. 24/2023 e/o di condotte illecite o violazioni del Modello di cui al D.Lgs. 231/01

Dati del segnalante *(riservati — conservati in busta separata)*

1

Nome del segnalante:	
Cognome del segnalante:	
Codice fiscale:	
Qualifica attuale:	
Incarico (Ruolo) attuale:	
Unità Organizzativa/Area di servizio attuale:	
Qualifica all'epoca del fatto segnalato:	
Incarico (Ruolo) all'epoca del fatto segnalato:	
Unità Organizzativa/Area di servizio all'epoca del fatto:	
Telefono:	
E-mail:	

2 Dati e informazioni della condotta illecita o violativa del Modello

Ente in cui si è verificato il fatto:	

Periodo in cui si è verificato il fatto:	
Data in cui si è verificato il fatto:	
Luogo fisico in cui si è verificato il fatto:	
Soggetto che ha commesso il fatto: nome, cognome, qualifica (possono essere inseriti più nomi):	
Eventuali soggetti terzi coinvolti (nome, cognome, qualifica, recapiti):	
Modalità con cui è venuto a conoscenza del fatto:	
Eventuali altri soggetti che possono riferire sul fatto (nome, cognome, qualifica, recapiti):	
Area/Funzione/Unità organizzativa a cui può essere riferito il fatto:	
"Altro", specificare (es. esistenza di eventuali denunce del fatto (ove note) alla pubblica Autorità):	

Tipo di violazione (es. violazione D.Lgs. 24/2023 / violazione Modello 231 / violazione Codice Etico / altro)

3 Descrizione del fatto:

4 La condotta è illecita perché:

Altro da Specificare: