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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE GENERALE

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..

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-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.

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.

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".
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;
▪ 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
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
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

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 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.

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.

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.

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.

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.

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.
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.

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 01

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 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, tali prescrizioni integrano, altresì, i principi di comportamento di cui al Modello e al Codice Etico.

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

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 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 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.

5 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*.

6 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, configurare le fattispecie delittuose di cui all'art. 25 quinquiesdecies del Decreto e, più in generale, di tutte le ipotesi criminali ivi previste;

ed hanno espresso divieto di:

- intrattenere rapporti commerciali con soggetti fisici o giuridici dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali di qualsiasi tipo;
- accettare denaro e titoli per importi superiori a quelli previsti dal D.lgs.25 maggio 2017 n. 90 ss.mm.ii., se non tramite intermediari a ciò abilitati, quali le Banche, gli Istituti di moneta elettronica e Poste Italiane S.p.A;
- accettare denaro e titoli trasferiti attraverso l'utilizzo di dispositivi, materiali o immateriali, o una loro combinazione, diversa dalla moneta a corso legale;
- porre in essere 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;
- 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.
- commettere negozi commettere negozi simulati riguardanti non solo denaro contante su un conto corrente o beni immobili, ma beni della più diversa natura, quali a titolo esemplificativo la cessione di quote o azioni eseguita al fine di estraniarsi dalla compagine della società solo apparentemente, poiché chi si è spogliato formalmente della titolarità delle quote o azioni continua di fatto a determinarne l'attività come amministratore o socio occulto ed a partecipare alla gestione e agli utili derivanti dall'attività imprenditoriale;
- 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* coinvolti nella gestione delle attività di tesoreria devono garantire, ognuno per le parti di rispettiva competenza, l'esecuzione dei seguenti specifici controlli.

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

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

1. Il RAM deve predisporre un piano di pagamenti mensile, che verrà condiviso in una piattaforma digitale (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.
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.

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).

6.2 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.

6.3 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.*).
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*.

6.4 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.

6.5 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.

6.6 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.

7 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).

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

- A non eludere le disposizioni in materia di misure di prevenzione patrimoniali o di contrabbando o per agevolare la commissione dei delitti di ricettazione, riciclaggio e impiego di

denaro, beni o utilità di provenienza illecita, spogliandosi fittiziamente della titolarità di denaro, beni o altre utilità, attribuendola a terzi.

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.

8 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.

9 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.

10 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.

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 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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 02

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 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 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.

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..

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.

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..

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. 2626 c.c. - Indebita restituzione dei conferimenti

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

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

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

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.

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*.

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.

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.

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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.*).

7.7 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.

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:

DICHIARAZIONE FRAUDOLENTA MEDIANTE FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (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. 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. 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. 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. 8 D. LGS. 74/2000)

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

OCCULTAMENTO O DISTRUZIONE DI DOCUMENTI CONTABILI (ART. 10 D. LGS. 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.

INDEBITA COMPENSAZIONE (ART. 10-QUATER D. LGS. 74/2000)

Il reato di cui all'art. 10-quater del D. Lgs. 74/2000, che si realizza con la condotta di chi non versa le somme dovute utilizzando in compensazione crediti non spettanti o inesistenti. 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 indebita compensazione 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.

SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DI IMPOSTE (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.

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.

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.

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.

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.

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.

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 03

SOMMARIO

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.

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. 332 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.*

1 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

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..

2 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..

3 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 dovrà essere a conoscenza di tutti i procedimenti.
I relativi verbali dovranno essere sottoscritti dal Presidente o dal professionista e/o funzione all'uopo incaricato con apposita delega.

4 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.

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.

5 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 tutte le procedure che coinvolgano rapporti con la P.A.;
- 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.

6 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.

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;
- 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.

7 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, 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'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 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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 04

SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

Ai sensi del D. Lgs. 231/2001, il processo relativo alla gestione dei contenziosi giudiziali e stragiudiziali, nonchè delle dichiarazioni da rendere all'Autorità Giudiziaria, potrebbe presentare occasioni per la commissione dei reati di "*Corruzione contro la Pubblica Amministrazione*", "*Induzione indebita a dare o promettere utilità*", "*Traffico di influenze illecite*", e "*Truffa ai danni dello Stato o di altro Ente pubblico"* nonché del reato di "*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria".*

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

Dunque, la presente procedura definisce i ruoli, le responsabilità operative, le attività di controllo ed i principi di comportamento adottati dalla BITCONTROL S.r.l. nella gestione dei rapporti con l'Autorità Giudiziaria nel caso di procedimenti penali.

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.

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

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 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.

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.

5 RESPONSABILE DELLA PROCEDURA

Il responsabile della procedura è il PRES.

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.*).

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;

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.

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 05

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 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.

2 ACRONIMI AZIENDALI

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

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 E DESTINATARI DELLA PROCEDURA

Rientrano nel campo di applicazione della procedura le funzioni aziendali svolte dai soggetti che intrattengono rapporti con i fornitori di prodotti (come attrezzature elettroniche, prodotti di cancelleria, *software*, *etc.*), necessari allo svolgimento dell'attività di impresa nonché dei fornitori di servizi – intesi quali società di consulenza, studi di commercialisti/avvocati, *etc.* – i quali devono attenersi ai principi contenuti nel Modello e nel Codice Etico adottato da BITCONTROL s.r.l.

5 RESPONSABILE DELLA PROCEDURA

Il processo di acquisto è gestito dal RCOM/APVG e dal PRES, a seconda della tipologia di fornitura.

6 INDICAZIONI COMPORTAMENTALI

Il processo di selezione del *partner* dovrà essere condiviso tra i diversi responsabili, ovvero RCOM/APVG e PRES.

6.1 PRESIDI DA RISPETTARE

I *Destinatari* coinvolti nella selezione e gestione dei fornitori di beni, servizi e incarichi professionali devono garantire, ognuno per le parti di rispettiva competenza, l'esecuzione dei seguenti controlli:

- Garantire, per importi superiori ad euro 5.000,00, che la selezione del fornitore sia sempre effettuata sulla base della valutazione del miglior rapporto tra qualità e convenienza del servizio / prodotto offerto / *business*, prediligendo i fornitori inseriti nell'elenco *"Elenco dei Fornitori Qualificati"* (fornitori con i quali esiste un rapporto di lunga data – ovvero, di almeno due anni – e che hanno assicurato la conformità dei loro prodotti, nel prosieguo anche solo *"elenco fornitori"*);
- nell'ipotesi in cui il prodotto/servizio richiesto non sia reperibile presso i fornitori, il RCOM/APVG che, in relazione alla propria area di riferimento, debba selezionare un fornitore – anche ai fini dell'inserimento nel sopra citato *elenco* – deve sottoporre la scelta al PRES che siglerà il preventivo, solo per importi superiori ad euro 5.000,00;
- verifica da parte del RCOM/APVG, prima della selezione finale, che nessun rapporto sia iniziato con persone o enti che non abbiano intenzione di adeguarsi ai principi etici della Società.

6.2 LA SOTTOSCRIZIONE DEL CONTRATTO O L'ACCETTAZIONE DEL PREVENTIVO

I contratti con i fornitori/professionisti/consulenti devono essere sottoscritti dal PRES, il quale deve, peraltro, verificare che nei contratti siano riportate specifiche clausole di impegno a rispettare le leggi e i regolamenti applicabili, con particolare riferimento a quanto previsto dal D.lgs. 231/2001. Nel caso in cui con i fornitori/professionisti/consulenti non sia stipulato un contratto, ma si proceda tramite "accettazione di preventivo", lo stesso deve essere sottoscritto, con firma digitale o con firma olografa dal Presidente, nonchè conservato in apposito raccoglitore o apposito archivio informatico, all'uopo predisposto nell'apposita piattaforma digitale di condivisione; preventivi relativi a forniture di importi eccedenti euro 20.000,00, se accettati, devono essere comunicati all'OdV.

6.3 LA CONSEGNA DEI BENI O L'ESECUZIONE DELLA PRESTAZIONE

Il RCOM/APVG verifica, per acquisti di importo superiore ad euro 1.000,00; la corrispondenza della fornitura e/o del servizio con l'oggetto del preventivo/contratto. Per i pagamenti superiori, ad euro 15.000,00 dovrà essere acquisita apposita autorizzazione scritta dal PRES, così come previsto alla

voce "gestione pagamenti". Il RCOM/APVG si occuperà dell'archiviazione della fattura e della relativa quietanza di pagamento, che dovrà essere vistata dal PRES e trasmessa al REC.
I compensi stabiliti per l'affidamento di incarichi a professionisti devono essere verificati dal PRES, il quale dovrà assicurarsi che siano stabiliti nel rispetto dei tariffari previsti per ciascuna categoria professionale.
Le fatture che vengono emesse o ricevute e registrate nella contabilità aziendale, aventi ad oggetto prestazioni immateriali (consulenze esterne, pubblicità, pareri legali, corsi o eventi di formazione, partecipazione a fiere o eventi, *etc.*) devono essere corredate da elementi di riscontro della loro veridicità con riferimento all'oggetto, quali, a titolo esemplificativo: relazioni scritte, corrispondenza, fotografie, documenti, gadget, stampe di pubblicità, *etc.*
Per quanto concerne il pagamento della fornitura o l'esecuzione della prestazione, si rimanda alla PMOG 01 "Gestione tesoreria"; in ogni caso, si precisa che, eventuali anticipi dei compensi dovuti al REC possono essere erogati solo se previsto e alle condizioni stabilite nel relativo contratto, nonché, debitamente documentati.

6.4 LA GESTIONE DI ATTIVITÀ IN OUTSOURCING

Nei contratti che prevedono la gestione in *outsourcing* di attività aziendali presso la sede della società, il fornitore garantisce che, in caso di impiego di personale proveniente da paesi terzi, questo sia in possesso di regolare permesso di soggiorno e provvede, in caso di richiesta della Società, a comunicare i nominativi e copia dei relativi documenti in corso di validità.

7 LA GESTIONE DEI RAPPORTI CON SOGGETTI APPARTENENTI A SOCIETÀ TERZE

È fatto obbligo alle funzioni aziendali che interloquiscono con soggetti appartenenti a società terze di segnalare, per iscritto, ai superiori e all'OdV, ogni richiesta di denaro o di regalia non giustificata dai normali rapporti amministrativi, ricevuta da soggetti appartenenti ad altre aziende; sussiste tale obbligo anche laddove vengano a conoscenza di analoghe condotte effettuate da soggetti operanti in o per conto di BITCONTROL s.r.l. nei confronti di soggetti appartenenti a società terze.

8 LA GESTIONE DEGLI OMAGGI E DI QUALSIVOGLIA EROGAZIONE GRATUITA

Preliminarmente, si precisa che, ai fini della presente procedura, valgono le seguenti definizioni:
• **PER OMAGGI** si intendono le elargizioni di beni di modico valore offerte, nell'ambito delle ordinarie relazioni di affari, al fine di promuovere l'immagine di BITCONTROL;
•**PER SPESE DI RAPPRESENTANZA** si intendono le spese sostenute da BITCONTROL nell'espletamento delle relazioni commerciali, destinate a promuovere e migliorare l'immagine della Società (ad es. spese per rinfreschi, per forme di accoglienza ed ospitalità, ecc.);

• **PER INIZIATIVE DI BENEFICENZA** si intendono le elargizioni in denaro che BITCONTROL destina esclusivamente ad Enti senza fini di lucro;

• **PER SPONSORIZZAZIONI** si intendono la promozione, la valorizzazione ed il potenziamento dell'immagine della BITCONTROL attraverso la stipula di contratti atipici (in forma libera, di natura patrimoniale, a prestazioni corrispettive) con Enti esterni (ad es.: Enti senza fini di lucro, Enti territoriali ed organismi locali, ecc.).

Una gestione non trasparente dei processi relativi a omaggi, spese di rappresentanza, beneficenze e sponsorizzazioni potrebbe, infatti, consentire la commissione di tali reati, ad esempio attraverso il riconoscimento/concessione di vantaggi ad esponenti della Pubblica Amministrazione e/o ad esponenti apicali, e/o a persone loro subordinate, di società o enti controparti o in relazione con la Società, al fine di favorire interessi di BITCONTROL, ovvero la creazione di disponibilità utilizzabili per la realizzazione dei reati in questione.

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

È vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri nonché a soggetti appartenenti a *partner* privati (o a soggetti loro congiunti, affini, conviventi e soggetti ad essi in qualche modo collegati), che possano influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsivoglia vantaggio alla società. Gli omaggi consentiti si caratterizzano per l'esiguità del loro valore: ai fini della presente procedura e dell'intero Modello, si intendono omaggi di "modico valore", beni di valore unitario non superiore ad euro 50 (similarmente a quanto previsto dalla normativa fiscale sulla deduzione di beni acquistati per essere distribuiti gratuitamente *ex* art. 108 co. 2 D.P.R. 917/1986).

9 LE SPESE DI SPONSORIZZAZIONE

Non si possono effettuare donazioni o sponsorizzazioni se sono pendenti debiti con l'Agenzia delle Entrate o con altri Organismi Pubblici, dovendo, prima, destinare le somme al pagamento di tasse e imposte.

In ogni caso l'importo annuo non può eccedere euro 1.000,00.

Nella scelta del materiale visivo e sonoro per *sponsor*, materiale pubblicitario di qualsivoglia tipo, l'Organo amministrativo o i soggetti da lui incaricati, rispetteranno i principi di tolleranza, uguaglianza, parità che sono enunciati anche nel Codice Etico.

10 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.

11 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutti i *Destinatari* coinvolti nella selezione e gestione dei fornitori di beni, servizi e incarichi professionali informano tempestivamente l'Organismo di Vigilanza di situazioni anomale e/o in deroga alla presente procedura e comportamenti non uniformati a quanto previsto nel Modello e nel Codice Etico. In caso di dubbi sulla moralità dei *partner* commerciali, la funzione aziendale che ha chiesto la fornitura/consulenza dovrà informare tempestivamente l'Organismo di Vigilanza, nonché comunicare l'eventuale insorgenza di criticità nei rapporti con il *partner*.

I *Destinatari* devono garantire, ognuno per le parti di rispettiva competenza, la tracciabilità del processo seguito, tenendo a disposizione dell'Organismo di Vigilanza – in un archivio ordinato – tutta la documentazione all'uopo necessaria.

Si precisa che, deve, essere annualmente trasmesso all'Organismo di Vigilanza l'elenco degli omaggi erogati a soggetti appartenenti alla Pubblica Amministrazione e/o a soggetti privati.

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 06

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. in relazione alla gestione dell'esecuzione degli appalti e dei contratti a favore degli enti pubblici e privati al fine di prevenire, nell'esecuzione di tale attività, la commissione degli illeciti previsti dal D.lgs. 231/2001, ed in particolare dagli artt. 24, 24-ter, 25 e 25-ter del medesimo Decreto.

Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Codice Etico.

LA PRESENTE PROCEDURA TROVA APPLICAZIONE NELLA:

- Partecipazione a gare ed appalti pubblici;
- Partecipazione a richieste d'offerta private
- Regolare gestione ed esecuzione dei contratti d'appalto in osservanza alle disposizioni normative dettate in materia.

2 ACRONIMI AZIENDALI

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

- D.LGS. N. 36/2023;
- CODICE DISCIPLINARE DI BITCONTROL S.R.L.
- MODELLO DI GESTIONE, ORGANIZZAZIONE E CONTROLLO DI BITCONTROL S.R.L..

4 CAMPO DI APPLICAZIONE E DESTINATARI DELLA PROCEDURA

La presente procedura trova applicazione nei confronti delle funzioni aziendali che, sotto la supervisione del PRES e del RTEC, intrattengono rapporti con la P.A. nell'ambito della presentazione e gestione di pratiche finalizzate ad ottenere, per conto dei clienti della Società, agevolazioni finanziarie, intervengono nella gestione della partecipazione alle gare e dell'esecuzione degli appalti, nonché dei contratti a favore di enti pubblici e privati.

LA PRESENTE PROCEDURA RIGUARDA:

- partecipazione a tutti i tipi di gare ed appalti pubblici;
- partecipazione a richieste d'offerta private;
- partecipazione ed esecuzione dell'appalto come operatore economico singolo , in A.T.I., tramite contratto di Rete, in consorzio, ovvero in subappalto (a titolo esemplificativo, per l'attività di controllo della progettazione dei documenti e dei dati; provvedere all'approvvigionamento; esecuzione delle prove, dei controlli e dei collaudi; controllo delle apparecchiature per prova, misurazione e collaudo; controllo del prodotto; controllo delle registrazioni della qualità; esecuzione di audit; gestione dei documenti di gara, dei contratti e conservazione della relativa documentazione);
- partecipazione ed esecuzione dei contratti a favore di enti privati.

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 *audit*t; gestione dei documenti di gara, dei contratti e conservazione della relativa documentazione);
- partecipazione ed esecuzione dei contratti a favore di enti privati.

Il principale responsabile della procedura è l'Organo amministrativo e, in via sussidiaria, il RCOM/APVG e il RTEC.

5 LA DISCIPLINA DEL NUOVO CODICE DEGLI APPALTI PUBBLICI

Dall'esame del decreto di riforma del codice degli appalti ex D.Lgs. n. 36/2023, emerge che la contestazione o l'accertata commissione di una fattispecie di reato contemplata dal D.Lgs. 231/2001 potrà far scattare l'esclusione dell'operatore economico dalle gare indette dalla Pubblica Amministrazione.

In particolare, tra le novità di maggior interesse per le imprese private, si segnalano le interazioni con la disciplina della responsabilità da reato degli enti, nonché con le disposizioni del Titolo IV, ovvero con i requisiti di partecipazione e selezione dei partecipanti, di seguito sintetizzate e le relative cause di esclusione automatica e non automatica.

5.1 CAUSE DI ESCLUSIONE AUTOMATICA

L'articolo 94 della scheda di decreto legislativo afferma che è causa di esclusione di un operatore economico dalla partecipazione a una procedura d'appalto la condanna con sentenza definitiva o decreto penale di condanna divenuto irrevocabile o sentenza di applicazione della pena su richiesta, ai sensi dell'articolo 444 del codice di procedura penale, per uno dei seguenti reati:

a) delitti, consumati o tentati, di cui agli articoli 416, 416-bis del codice penale oppure delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis oppure al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché per i delitti, consumati o tentati, previsti dall' articolo 74, del DPR 9 ottobre 1990, n. 309, dall' articolo 291-quater del DPR 23 gennaio 1973, n. 43 e dall' articolo 452-quaterdieces del codice penale, in quanto riconducibili alla partecipazione a un'organizzazione criminale;

b) false comunicazioni sociali di cui agli articoli 2621 e 2622 del codice civile;

c) frode ai sensi dell'articolo 1, della convenzione relativa alla tutela degli interessi finanziari delle Comunità europee;

d) delitti, consumati o tentati, commessi con finalità di terrorismo, anche internazionale, e di eversione dell'ordine costituzionale, reati terroristici o reati connessi alle attività terroristiche;

e) delitti di cui agli articoli 648-bis, 648-ter e 648-ter.1 del codice penale, riciclaggio di proventi di attività criminose o finanziamento del terrorismo, quali definiti all' articolo 1 del decreto legislativo 22 giugno 2007, n. 109;

f) sfruttamento del lavoro minorile e altre forme di tratta di esseri umani definite con il decreto legislativo 4 marzo 2014, n. 24;

g) ogni altro delitto da cui derivi, quale pena accessoria, l'incapacità di contrattare con la pubblica amministrazione;

h) Corruzione e concussione, Truffa aggravata ai danni dello Stato e Reati in tema di erogazioni pubbliche;

i) turbata libertà d'incanti;

5. 2 CAUSE DI ESCLUSIONE NON AUTOMATICA

L'articolo 95, dello schema di decreto legislativo del Codice degli appalti, prevede che la stazione appaltante esclude dalla partecipazione alla procedura un operatore economico qualora accerti:

a) sussistere gravi infrazioni, debitamente accertate con qualunque mezzo adeguato, alle norme in materia di salute e di sicurezza sul lavoro nonché agli obblighi in materia ambientale, sociale e del lavoro stabiliti dalla normativa europea e nazionale, dai contratti collettivi o dalle disposizioni internazionali elencate nell'

allegato X alla direttiva 2014/24/UE del Parlamento europeo e del Consiglio del 26 febbraio 2014;

b) che la partecipazione dell'operatore economico determini una situazione di conflitto di interesse non diversamente risolvibile;

c) sussistere una distorsione della concorrenza derivante dal precedente coinvolgimento degli operatori economici nella preparazione della procedura d'appalto che non possa essere risolta con misure meno intrusive;

d) sussistere rilevanti indizi tali da far ritenere che le offerte degli operatori economici siano imputabili ad un unico centro decisionale a cagione di accordi intercorsi con altri operatori economici partecipanti alla stessa gara;

e) che l'offerente abbia commesso un illecito professionale grave, tale da rendere dubbia la sua integrità o affidabilità, dimostrato dalla stazione appaltante con mezzi adeguati;

f) violazioni (anche non accertate) degli obblighi fiscali o previdenziali, a meno che l'operatore abbia ottemperato o si sia impegnato in modo vincolante in tal senso;

g) rilevanti indizi sull'esistenza di un accordo tra gli operatori economici sulle offerte;

5.3 GLI ILLECITI PROFESSIONALI GRAVI

L'illecito professionale grave rileva solo se compiuto dall'operatore economico offerente.

L'esclusione di un operatore economico è disposta e comunicata dalla stazione appaltante quando ricorrono tutte le seguenti condizioni:

a) elementi sufficienti ad integrare il grave illecito professionale;

b) idoneità del grave illecito professionale ad incidere sull'affidabilità e integrità dell'operatore;

c) adeguati mezzi di prova.

L'ILLECITO PROFESSIONALE SI PUÒ DESUMERE AL VERIFICARSI DI ALMENO UNO DEI SEGUENTI ELEMENTI:

a) sanzione esecutiva irrogata dall'Autorità garante della concorrenza e del mercato o da altra autorità di settore, rilevante in relazione all'oggetto specifico dell'appalto;

b) condotta dell'operatore economico che abbia tentato di influenzare indebitamente il processo decisionale della stazione appaltante o di ottenere informazioni riservate a proprio vantaggio oppure che abbia fornito, anche per negligenza, informazioni false o fuorvianti suscettibili di influenzare le decisioni sull'esclusione, la selezione o l'aggiudicazione;

c) condotta dell'operatore economico che abbia dimostrato significative o persistenti carenze nell'esecuzione di un precedente contratto di appalto o di concessione che ne hanno causato la risoluzione per inadempimento oppure la condanna al risarcimento del danno o altre sanzioni comparabili, derivanti da inadempienze particolarmente gravi o la cui ripetizione sia indice di una persistente carenza professionale;

d) condotta dell'operatore economico che abbia commesso grave inadempimento nei confronti di uno o più subappaltatori;

e) condotta dell'operatore economico che abbia violato il divieto di intestazione fiduciaria di cui all'articolo 17, della legge 19 marzo 1990, n. 55, laddove la violazione non sia stata rimossa;

f) omessa denuncia all'autorità giudiziaria da parte dell'operatore economico persona offesa dei reati previsti e puniti dagli articoli 317 e 629 del codice penale aggravati ai sensi dell'articolo 416-bis.1 del medesimo codice salvo che ricorrano i casi previsti dall'articolo 4, primo comma, della legge 24 novembre 1981, n. 689. Tale circostanza deve emergere dagli indizi a base della richiesta di rinvio a giudizio formulata nei confronti dell'imputato per i reati nell'anno antecedente alla pubblicazione del bando e deve essere comunicata, unitamente alle generalità del soggetto che ha omesso la predetta denuncia, dal procuratore della Repubblica procedente all'ANAC, la quale ne cura la pubblicazione;

g) contestata commissione da parte dell'operatore economico, ovvero dei soggetti di cui al comma 3, dell'articolo 94, di taluno dei reati consumati o tentati di cui al comma 1, del medesimo articolo 94;

h) contestata o accertata commissione, da parte dell'operatore economico oppure dei soggetti di cui al comma 3, dell'articolo 94, di taluno dei seguenti reati consumati:

1) abusivo esercizio di una professione, ai sensi dell'articolo 348 del codice penale;

2) bancarotta semplice, bancarotta fraudolenta, omessa dichiarazione di beni da comprendere nell'inventario fallimentare o ricorso abusivo al credito, di cui agli articoli 216, 217, 218 e 220 del regio decreto 16 marzo 1942, n. 267;

3) i reati tributari ai sensi del decreto legislativo 10 marzo 2000, n. 74, i delitti societari di cui agli articoli 2621 e seguenti del codice civile o i delitti contro l'industria e il commercio di cui agli articoli da 513 a 517 del codice penale;

4) i reati urbanistici di cui all'articolo 44, comma 1, lettere b) e c), del DPR 6 giugno 2001, n. 380, con riferimento agli affidamenti aventi ad oggetto lavori o servizi di architettura e ingegneria;

5) i reati previsti dal decreto legislativo 8 giugno 2001, n. 231;

i) commissione, da parte dell'operatore economico, di condotte diverse da quelle di cui alle precedenti lettere, la cui gravità incida in modo evidente sull'affidabilità ed integrità del medesimo in misura tale da compromettere l'interesse pubblico.

5.4 LE INTERAZIONI CON IL MODELLO N. 231/2001

Le previsioni di cui sopra collegano espressamente l'esclusione degli operatori economici al sistema della responsabilità amministrativa degli enti.

IN PARTICOLARE:

• esclusione automatica nel caso di condanna dell'ente, ai sensi del D.Lgs. n. 231/2001, per uno dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti;

• esclusione automatica nel caso di condanna penale delle persone fisiche legate all'ente (art. 94, comma 3) per uno dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti;

• esclusione automatica degli enti già destinatari della sanzione interdittiva di cui all'art. 9, comma 2, lett. c), del D.Lgs. n. 231/2001 («il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio») o di altra sanzione che comporta il divieto di contrarre con la pubblica amministrazione (senza vincolo alcuno, in questo caso, all'elenco dei gravi reati-presupposto dell'art. 94, comma 1, del Codice degli appalti);

• esclusione non automatica dell'ente di cui si accerti la commissione di un illecito professionale grave, desumibile – fra gli altri motivi – dalla commissione o dalla mera contestazione di un qualsiasi reato-presupposto di cui al D.Lgs. n. 231/2001.

Quest'ultima previsione (art. 98, comma 3, lett. h), in particolare, consente l'esclusione dell'operatore economico a vario titolo coinvolto in una indagine per un reato che fonda la responsabilità amministrativa degli enti, ancorché in fase di indagini ovvero riferibile alle persone fisiche collegate all'ente. Il comma 6 dell'articolo, infatti, stabilisce che costituiscono mezzi di prova adeguati alla dimostrazione dell'illecito professionale legato alle violazioni 231 le sentenze e i decreti penali di condanna, nonché i provvedimenti cautelari personali o reali.

Come già segnalato da diverse organizzazioni (*in primis*, l'Unione delle Camere Penali Italiane e l'Associazione dei Componenti degli Organismi di Vigilanza – AODV231), la nuova disciplina si pone in frizione con i principi fondamentali della materia penale (presunzione di non colpevolezza ex art. 27, comma 2°, Cost.), con la libertà di iniziativa economica privata (art. 41 Cost.) e con taluni degli stessi principi ispiratori del Codice degli appalti.

Si consideri, inoltre, che il riferimento all'intero decalogo dei reati contemplati dal Decreto 231 non tiene conto della incessante moltiplicazione delle fattispecie suscettibili di dar luogo alla responsabilità da reato delle società, molte delle quali non costituiscono nemmeno espressione della c.d. criminalità d'impresa, men che meno della devianza "politico-amministrativa" cui si dovrebbero riferire le esclusioni dalle gare pubbliche.

6 IL RUOLO DELLA RESTORATIVE COMPLIANCE

D'altra parte, il comma 4 dell'art. 98 prevede che, ai fini della valutazione di gravità dell'illecito professionale, si tenga conto del bene giuridico e dell'entità della lesione inferta dalla condotta e del tempo trascorso dalla violazione, «anche in relazione a modifiche intervenute nel frattempo nell'organizzazione dell'impresa». Ciò significa che le stazioni appaltanti, pur in presenza degli elementi che integrano, sul piano oggettivo, un illecito professionale, potranno valutare – nell'esercizio della discrezionalità amministrativa – le azioni correttive intraprese dall'operatore economico in un tempo successivo alla contestazione o alla condanna per un illecito 231, al fine di stabilire se la riorganizzazione aziendale è tale da elidere la gravità dell'illecito e/o da riabilitare l'affidabilità dell'ente.

Il riferimento, anche se non espresso, è, dunque, alla restorative compliance, ossia alla riorganizzazione intrapresa dall'ente successivamente alla commissione dell'illecito. L'adozione, l'effettiva attuazione e la "correzione" di un Modello di organizzazione, gestione e controllo, già rilevanti sul fronte "premiale" delle condotte riparatorie ex D.Lgs. n. 231/2001, divengono dunque strumenti di riabilitazione dell'ente, anche ai fini della partecipazione alle gare pubbliche, ovvero per rimediare alla sua potenziale esclusione.

La previsione conferma, in definitiva, il ruolo sempre più centrale della compliance (non solo ex ante, ma anche ex post) nel sistema in senso lato sanzionatorio delle persone giuridiche, nell'ambito del quale spiccano le previsioni del D.Lgs. n. 231/2001 e le misure interdittive e di prevenzione di cui D.Lgs. n. 159/2011 (c.d. codice antimafia), in ispecie per le ripercussioni che determinano sulla "vita" pubblica e sociale dell'ente e nei rapporti con la p.a.

7 TURBATA LIBERTA' DEGLI INCANTI (EX ART. 353 C.P.) E TURBATA LIBERTA' DEL PROCEDIMENTO DI SCELTA DEL CONTRAENTE (EX ART. 353 BIS C.P.)

Il 9 Ottobre del 2023 è stata pubblicata in Gazzetta Ufficiale la Legge n. 137/2023 che ha convertito in legge, con modificazioni, il D.L. 10 agosto 2023 n. 105 (cd. Decreto Giustizia).

La citata Legge di conversione ha introdotto importanti modifiche al testo originario del Decreto Giustizia e le principali novità riguardano proprio l'introduzione di nuovi delitti nel catalogo dei reati presupposto ex D.Lgs. n. 231/2001 intervenendo sugli artt. 24 e 25-octies.

In particolare, La Legge di conversione ha introdotto all'art. 24 le fattispecie di reato di turbata libertà degli incanti (art. 353 c.p.) e turbata libertà del procedimento di scelta del contraente (art. 353-bis c.p.).

L'art. 353 c.p. punisce chiunque, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, impedisca o turbi una gara nei pubblici incanti o nelle licitazioni private per conto della Pubblica Amministrazione, ovvero ne allontani gli offerenti.

La disposizione si applica anche nel caso di licitazioni private per conto di privati, è dirette da un pubblico ufficiale o da persona legalmente autorizzata.

L'art. 353-bis c.p. sanziona, invece, chiunque, con violenza o minaccia, o con doni, promesse, collusioni o altri mezzi fraudolenti, turbi il procedimento amministrativo diretto a stabilire il contenuto del bando o di altro atto equipollente al fine di condizionare le modalità di scelta del contraente da parte della Pubblica Amministrazione.

Entrambe le fattispecie, quindi, sono volte a tutelare il buon andamento della P.A. rispetto a condotte fraudolente che impediscano o alterino la regolare procedura di una gara (art. 353 c.p.), o, ancor prima, il procedimento che porta alla realizzazione di un bando (art. 353-bis c.p.).

PERTANTO, TITOLO ESEMPLIFICATIVO, I DESTINATARI DELLA PRESENTE PROCEDURA SI DEVONO ASTENERE:

- ✓ dal promettere ad un proprio concorrente lavori futuri, al fine di impedirne la partecipazione a una gara di appalto, poiché ciò configurerebbe il reato di cui all'art. 353-bis c.p.;
- ✓ dal firmare un accordo clandestino con un pubblico ufficiale finalizzato a redigere un bando di gara con requisiti talmente stringenti da predeterminare l'aggiudicazione poiché ciò integrerebbe il reato di cui all'art. 353 c.p.;
- ✓ dal porre in essere qualsiasi atto idoneo ad influenzare l'andamento della gara.

All'uopo, si evidenzia come la recentissima Cass., VI, ord. n. 41379/2023, ha rimesso alle SS.UU. la questione se sia configurabile, oltre al reato di cui all'art. 353 c.p., anche quello di estorsione nella condotta di chi, con violenza o minaccia, allontani gli offerenti da una gara nei pubblici incanti o nelle licitazioni private. Con la citata sentenza la Corte di Cassazione ha precisato che "*il delitto da cui derivi, quale pena accessoria, l'incapacità di turbata libertà della gara si configura sia nel caso di danno effettivo sia nel caso di danno mediato e potenziale, non occorrendo l'effettivo conseguimento del risultato, perseguito dagli autori dell'illecito, ma la semplice idoneità degli atti ad influenzare l'andamento della gara (…) Si è precisato che, ai fini dell'integrazione del reato di cui all'art. 353 cod. pen., occorre che tale idoneità si sia in qualche modo manifestata, nel senso che le condotte dell'agente devono essersi tradotte in una concreta minaccia, ossia che abbiano in qualche modo cagionato la verificazione del citato evento di pericolo, determinando un rischio di alterazione di quello che, diversamente, sarebbe stato il corso degli incanti*".

L'Ente nel cui interesse e/o a cui vantaggio risulti commesso uno dei reati appena descritti potrà essere condannato a pagare una sanzione amministrativa pecuniaria fino a 500 quote (da un minimo di 25.800 euro ad un massimo di 774.500 euro).

L'art. 24, comma 2, D.Lgs. n. 231/2001 prevede inoltre la sanzione pecuniaria da 200 a 600 quote (da 51.600 a 929.400 euro) nel caso in cui l'ente abbia conseguito un profitto di rilevante entità o sia derivato un danno di particolare gravità.

In aggiunta alle sanzioni pecuniarie, troveranno applicazione le seguenti sanzioni interdittive (art. 9, comma 2, lett. c), d) ed e), D.Lgs. n. 231/2001)

- ✓ divieto di contrattare con la Pubblica Amministrazione;

- ✓ esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- ✓ divieto di pubblicizzare beni o servizi;
- ✓ in generale, al fine di evitare la configurazione del reato di cui all'art. 353 bis c.p. è vietata la commissione di comportamenti fraudolenti volti a falsare il risultato di una procedura ad evidenza pubblica; tali comportamenti possono realizzarsi mediante l'uso di violenza, minaccia, doni, promesse, collusione od altri mezzi fraudolenti, impedendo o turbando la gara espletata da Pubbliche Amministrazioni o allontanando gli offerenti.

Dunque, sia il reato di "Turbata libertà degli incanti" (art. 353 c.p.) sia il reato di "Turbata libertà del procedimento di scelta del contraente" (art. 353 bis c.p) sono volti a tutelare il corretto espletamento delle procedure ad evidenza pubblica, nelle varie fasi, i procedurali (dalla predisposizione del bando fino allo svolgimento della procedura ad evidenza pubblica).

8 PRINCIPI GENERALI DI COMPORTAMENTO E PRESIDI DI CONTROLLO

Le principali attività disciplinate dalla presente procedura, riguardano essenzialmente le fasi di definizione del processo di acquisizione dei lavori acquisiti mediante la partecipazione di BitControl alle gare ed in particolare alla:

- Valutazione dell'opportunità a partecipare alla gara pubblica;
- Valutazione dell'opportunità di aderire all'offerta privata;
- Predisposizione della documentazione;
- Riesame dell'offerta;
- Aggiudicazione e stipula del contratto;
- Avvio di commessa ed esecuzione dei lavori:
- Emissione SAL attivi e Certificati di pagamento;
- Fatturazione attiva, incasso e contabilizzazione.

Tutti i contratti stipulati con la P.A., le comunicazioni, le richieste e le autorizzazioni devono essere gestite e firmate da soggetti dotati dei relativi poteri e capacità professionali e tecniche, nel rispetto dell'organizzazione aziendale. Deve essere, altresì, assicurata la tracciabilità della documentazione di ogni contratto o negoziazione.

Tutti coloro che, per ragioni 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.

A TAL PROPOSITO, AI DESTINATARI INTERESSATI È 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 o influenzare detti funzionari ad agire secondo modalità che possano agevolare la Società ad ottenere, promuovere, mantenere le proprie attività o ad assicurarsi vantaggi illegittimi o indebiti nello

svolgimento delle stesse. 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), neppure al verificarsi di particolari ricorrenze, 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 o asserite con pubblici ufficiali, incaricati di pubblici servizi, ovvero con uno degli altri soggetti di cui all'art. 322 bis c.p., consegnando 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;
- ✓ nella scelta di eventuali 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;
- ✓ 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 l'Azienda.

9 INDICAZIONI COMPORTAMENTALI PER LA GESTIONE DELLA PARTECIPAZIONE ALLE GARE

IL PROCESSO DI PARTECIPAZIONE A GARE PUBBLICHE SI ARTICOLA NELLE SEGUENTI FASI:

1. VALUTAZIONE DEL BANDO PUBBLICO;
2. PREDISPOSIZIONE DELLA DOCUMENTAZIONE NECESSARIA PER LA PARTECIPAZIONE ALLA GARA;
3. AGGIUDICAZIONE DELLA GARA.

9.1 VALUTAZIONE DEL BANDO PUBBLICO

L'ufficio gare procede a rivenire e studiare i bandi, a selezionare quelli più inerenti il core business di BITCONTROL S.R.L., nonché a sottoporli all'attenzione del CDA, che di concerto con l'ufficio

tecnico e l'ufficio gare, valuta la preliminare sussistenza dei requisiti di economicità ed interesse alla partecipazione alla gara e le motivazioni che rendono opportuna la partecipazione al bando.
In caso di valutazione positiva, il CDA, qualora non vi sia una funzione aziendale espressamente delegata alla gestione delle gare/appalti pubblici, provvederà a nominare un responsabile di gara che curerà la predisposizione della domanda di partecipazione al bando nel rispetto della tempistica prescritta per il deposito della stessa e delle previsioni del bando di gara.

9.2 PREDISPOSIZIONE DELLA DOCUMENTAZIONE NECESSARIA PER LA PARTECIPAZIONE ALLA GARA

IL DL, TRAMITE IL RAM ED IL RESPONSABILE DI GARA, HA IL COMPITO DI:

- stimare in modo appropriato il valore da indicare nell'offerta;
- individuare i costi relativi alla sicurezza, secondo quanto stabilito dalla Legge n. 123/07 e dal D. Lgs. 81/2008, successivamente modificato dalla Legge 106/09, ove non già predeterminati dal bando di gara;
- predisporre la documentazione di supporto richiesta dal bando gara, anche tramite la raccolta delle informazioni da altre funzioni per quanto di competenza;
- chiedere all'Ente che ha emesso il bando eventuali chiarimenti in merito ai requisiti/contenuti del bando, nel rispetto dei termini di cui al d.lgs. 163/2006;
- predisporre la domanda di partecipazione in tutti i suoi elementi, firmarla, curandone altresì l'invio nei termini previsti dal bando.

9.3 AGGIUDICAZIONE DELLA GARA

In caso di aggiudicazione della gara, il DL sarà responsabile di attivare il processo interno finalizzato a dare la corretta esecuzione al contratto concluso con la Pubblica Amministrazione.
Alla comunicazione dell'aggiudicazione definitiva della procedura di gara, il DL, il RAM ed il Responsabile dell'Ufficio Gare procedono a tutti gli adempimenti amministrativi prodromici alla sottoscrizione del contratto di appalto e successivamente – in base alle tempistiche previste ed alla disponibilità del committente – il DL firmerà il contratto monitorando la presa in consegna dei lavori.
Successivamente all'avvio dei lavori, verrà definito il "budget di commessa" – riesame del computo metrico da un punto di vista "realizzativo", con il programma degli approvvigionamenti di commessa (forniture e subappalti) – dal quale discenderanno le richieste di acquisto.

10 INDICAZIONI COMPORTAMENTALI PER LA GESTIONE DELL'ESECCUZIONE DEGLI APPALTI

Ai fini della prevenzione dei reati di cui al D.lgs. 231/2001, indipendentemente dalla circostanza che gli appalti siano eseguiti direttamente o in A.T.I., tramite Rete, consorzio o subappalto o con enti privati, è obbligatorio rispettare le seguenti prescrizioni:

a. eseguire la fornitura a regola d'arte, secondo l'ordinaria diligenza, astenendosi da condotte illecite o lesive dell'interesse del committente lecito e contrattualmente pattuito;

b. approntare e mantenere, per ogni commessa, un fascicolo digitale caricato nell'apposito archivio informatico all'uopo predisposto nell'apposita piattaforma digitale di condivisione, contenente una "scheda di apertura commessa", l'indicazione del responsabile della commessa, il contratto, la documentazione inerente l'acquisto dei materiali, il piano di fornitura, la documentazione concernente la costituzione dell'A.T.I., o la partecipazione tramite contratto di Rete o consorzio, ovvero gli eventuali documenti relativi al subappalto diversi dal contratto, con le rispettive competenze delle partecipanti, la documentazione concernente le comunicazioni tra le aziende partecipanti all'A.T.I. o al consorzio o al contratto di Rete, ovvero con l'appaltatore principale;

c. i contatti con funzionari di enti pubblici potranno avvenire solo per motivi inerenti alle gare cui la società partecipa o intende partecipare e solo attraverso il PRES, o il soggetto da quest'ultimo incaricato: dovrà essere predisposto un elenco con indicazione di data, motivazione del contatto e soggetto interlocutore; il suddetto elenco, relativo ai contatti intercorsi con i funzionari degli enti pubblici, verrà caricato e tenuto nell'archivio informatico all'uopo predisposto nella piattaforma digitale di condivisione.

LOTTA ALLA CORRUZIONE

i) NEI RAPPORTI CON LA P.A.:

- la Società vieta qualsivoglia forma di corruzione, sia attiva, sia passiva;
- ai soggetti che agiscono per conto della Società, è fatto divieto di autorizzare, sollecitare, offrire, promettere di concedere, offrire, direttamente o indirettamente, pagamenti o oggetti di valore a funzionari pubblici con l'intento di persuadere o influenzare detti funzionari ad agire secondo modalità che possano agevolare la Società ad ottenere, promuovere, mantenere le proprie attività o ad assicurarsi vantaggi illegittimi o indebiti nello svolgimento delle stesse;
- le violazioni delle fattispecie di cui sopra, dovranno essere tempestivamente segnalate all'OdV;
- i soggetti ai quali i funzionari pubblici propongono una tangente, monetaria e non, direttamente o indirettamente, devono rifiutare ed informare tempestivamente l'OdV, secondo le modalità prescritte;

ii) NEI RAPPORTI CON I PRIVATI:

- è vietato offrire, promettere, concedere, sollecitare o accettare, sia direttamente che indirettamente, qualsivoglia vantaggio indebito monetario o di altra natura, a/da qualsiasi soggetto che dirige o lavora, indipendentemente dalla posizione ricoperta, per un altro ente privato al fine di indurlo ad agire o ad astenersi dall'agire in violazione dei suoi doveri; nelle ipotesi di realizzazione di tali fattispecie di reato, i soggetti che ne abbiano conoscenza devono informare tempestivamente l'OdV;
- nessun soggetto della Società, o che agisca per conto e nell'interesse della stessa, è autorizzato, anche al verificarsi di particolari ricorrenze, ad offrire o corrispondere a soggetti terzi, omaggi, trattamenti di favore e/o regalie di valore più che simbolico e, comunque, estranei alle normali relazioni di cortesia, nell'intento di favorire in modo illecito la Società; i medesimi soggetti non possono accettare da terzi omaggi, trattamenti di favore e/o regalie di valore più che simbolico.

11 DISCRASIA TRA PRESTAZIONE PREVISTA E PRESTAZIONE EFFETTIVAMENTE ESEGUITA

In caso di discrasia (di qualsivoglia genere e specie) tra prestazione contrattualmente prevista e prestazione concretamente eseguita:

1. ciascun *Destinatario* è tenuto a farne comunicazione al responsabile della commessa/fornitura;
2. il processo di fatturazione è sospeso sino al superamento della problematica;
3. ove ritenuto opportuno, il committente può essere coinvolto nel processo di superamento della discrasia, anche attraverso la concordata revisione del prezzo;
4. deve essere concordata la rimozione della discrasia, ovvero la revisione del prezzo; nel caso di decisione di rimozione della discrasia, il RCOM/APVG è tenuto a darne attuazione e comunicarne per iscritto il buon esito.
5. sottoposizione a liquidazione giudiziale o allo stato di liquidazione coatta o concordato preventivo (ferme restando, però, le disposizioni volte ad assicurare la continuità aziendale e altri strumenti di regolazione della crisi).

Infine, sono esclusi in via automatica gli operatori economici iscritti nel casellario informatico dell'ANAC per aver presentato false dichiarazioni o falsa documentazione nelle procedure di gara e negli affidamenti aventi ad oggetto lavori o servizi di architettura e ingegneria, subappalti o ai fini del rilascio dell'attestazione di qualificazione (per il periodo durante il quale perdura l'iscrizione), nonché gli operatori che abbiano commesso violazioni gravi, definitivamente accertate, degli obblighi fiscali o previdenziali, a meno che l'operatore abbia ottemperato o si sia impegnato in modo vincolante in tal senso.

12 FATTURAZIONE DELLE OPERAZIONI

Una volta conclusa la prestazione indicata nel contratto ed eseguita la fatturazione dei corrispettivi, secondo quanto previsto dalla normativa fiscale, il RCOM/APVG, o la funzione all'uopo incaricata, dovrà verificare che l'importo complessivamente fatturato corrisponda a quanto stabilito nel contratto; eventuali differenze dovranno essere segnalate al PRES. L'emissione di note di credito dovrà essere autorizzata dal PRES o da altro soggetto all'uopo incaricato.

13 ARCHIVIAZIONE

Tutta la documentazione suddetta deve essere inserita nel fascicolo di commessa a cura delle Funzioni responsabili.

14 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

L'OdV ha facoltà di visionare i fascicoli di cui sopra a semplice richiesta.

Ciascun *Destinatario* – e in particolare ciascun responsabile della commessa – è tenuto a segnalare tempestivamente all'OdV a mezzo di apposito *report* ovvero in forma libera purché scritta:

1. qualunque evento e/o comportamento anomalo rilevato nell'esecuzione degli appalti;
2. qualsiasi violazione della presente procedura;
3. qualunque altra anomalia riscontrata in fase di contrattualizzazione ed esecuzione degli appalti;
4. qualunque violazione del Modello e del Codice Etico.

Tutte le funzioni aziendali coinvolte hanno la responsabilità di osservare e far osservare il contenuto della presente procedura.

L'ODV, IN PARTICOLARE, PUÒ:

- visionare tutta la documentazione;
- verificare il puntuale rispetto delle disposizioni previste dalla presente procedura, dal Codice Etico, dal Modello e da tutte le disposizioni in materia.

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'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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 07

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.

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.

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.

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.

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.

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.

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.

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.

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.

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 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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 08

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.

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, 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., 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*.

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

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* 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.

5 RESPONSABILE DELLA PROCEDURA

Sono responsabili della procedura le funzioni responsabili delle diverse aree: il PRES, il RSPP, il RSGQ, il RTEC, il RPROG, il RFAM, ed il RAM/RUU.

Tutti i dipendenti, per quanto di propria competenza, utilizzano ed hanno accesso ai sistemi informatici della Società.

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.)

"*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede si procede d'ufficio."

Il reato 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.

6.2 DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615-QUATER C.P.)

"*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."

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 DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-QUINQUIES C.P.)

"*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."*

L'art. 615 quinquies punisce chiunque abusivamente si procura, detiene, produce, riproduce importa, diffonde, comunica consegna o mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi allo scopo di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero di favorire l'interruzione o l'alterazione del suo funzionamento.

Tali fattispecie perseguibili d'ufficio, intendono reprimere anche la sola abusiva detenzione o diffusione di credenziali d'accesso o di programmi (virus, spyware) o dispositivi potenzialmente dannosi indipendentemente dalla messa in atto degli altri crimini informatici sopra illustrati, rispetto ai quali le condotte in parola possono risultare propedeutiche.

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.)

"*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."

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..

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.

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.

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

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.

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 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.

8.1 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.

8.2 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.

8.3 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.

9 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.

10 ARCHIVIAZIONE

Tutta la documentazione prodotta nell'ambito della presente procedura deve essere trasmessa al RGAD, che procederà all'archiviazione.

11 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;
- 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.

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 09

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 10

SOMMARIO

1 OBIETTIVI DELLA PROCEDURA

La presente procedura, uniformemente e ad integrazione del sistema di sicurezza sul lavoro adottato dalla BITCONTROL S.r.l., individua una serie di procedure, in conformità all'art. 30 D.lgs 81/2008 e decreto del 13 febbraio 2014 emanato dal Ministero del Lavoro e Politiche Sociali, atte a verificare e controllare la corretta applicazione degli adempimenti previsti dalla vigente legislazione nazionale in materia di tutela della salute e della sicurezza negli ambienti di lavoro.

Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Modello e nel Codice Etico.

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 dei lavoratori, così come definiti dal D.lgs. 81/2008 ss.mm.ii., sulla gestione delle attività in materia di sicurezza e salute della Società e sulle conseguenze derivanti da un mancato rispetto delle norme di legge e delle regole di comportamento e controllo definite dalla Società. In particolare, ciascun lavoratore dovrà ricevere formazione sufficiente ed adeguata con particolare riferimento al proprio posto di lavoro ed alle proprie mansioni. La suddetta formazione deve essere fatta in occasione dell'assunzione, del trasferimento o cambiamento di mansioni o dell'introduzione di nuove attrezzature di lavoro o di nuove tecnologie, di nuove sostanze e preparati pericolosi;
- la definizione e l'aggiornamento (in base ai cambiamenti nella struttura organizzativa ed operativa dalla Società nonché l'evolversi del panorama normativo) di procedure specifiche per la prevenzione di infortuni e malattie, in cui siano, tra l'altro, disciplinate le modalità di gestione degli incidenti e delle emergenze;
- l'idoneità delle risorse umane – in termini di numero e qualifiche professionali, formazione – e materiali, necessarie al raggiungimento degli obiettivi prefissati dalla Società per la sicurezza e la salute dei lavoratori.

I lavoratori devono comunicare tempestivamente, alle funzioni individuate e con le modalità definite nelle procedure operative, situazioni di pericolo, quasi infortuni, infortuni (indipendentemente dalla loro gravità) e violazioni alle regole di comportamento e alle procedure operative.

È fatto esplicito divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 25 septies del D.lgs. 231/2001);
- porre in essere o dare causa a violazioni dei principi di comportamento, dei protocolli e delle procedure aziendali;
- fruire di servizi in "appalto" con consulenti, *partner* ed in generale fornitori, in assenza dei requisiti di idoneità tecnico-professionale.

2 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 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 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 riguarderà anche la scelta delle attrezzature di lavoro e delle sostanze e dei preparati chimici impiegati, la sistemazione dei luoghi di lavoro, i rischi dei gruppi di lavoro esposti a rischi particolari (stress lavoro-correlato, lavoratrici in stato di gravidanza, minori, ect.), nonché quelli connessi alle differenze di genere, di età, di provenienza.
Ai sensi dell'art. 28, infatti, il documento redatto a conclusione della valutazione deve avere data certa e contenere:
a) Una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;
b) l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati, a seguito della valutazione di cui all'articolo 17, comma 1, lettera a);
c) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
d) l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
e) l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio;
f) l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.
Il documento sarà utilizzato come guida da tutti i soggetti facenti parte del sistema organizzativo della sicurezza, al fine di applicare tutte le misure da adottare in relazione ai rischi presenti.
Tutti saranno soggetti alla piena osservanza e applicazione delle misure di sicurezza riportate nel presente documento.
Le misure, i DPI e le cautele di sicurezza sono:

- 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 – 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 per poter operare all'interno o in collaborazione con la Società devono dare evidenza del rispetto e adempienza di tutte le norme vigenti applicabili, nonché dei parametri definiti dalla Società all'interno delle proprie procedure.

Il Datore di Lavoro, attraverso la propria struttura organizzativa, secondo quanto previsto dall'art. 26 del D. Lgs 81/2008, qualora siano presenti interferenze, promuove la cooperazione ed il coordinamento di cui ai punti precedenti, elaborando un Documento Unico di Valutazione dei Rischi per le Interferenze, nel quale siano indicate le misure adottate per eliminare o, laddove non sia possibile, per ridurre al minimo le interferenze. Tale documento deve allegarsi al contratto di appalto o d'opera, già in fase di procedura di affidamento. Il documento può essere, eventualmente, aggiornato all'atto della consegna delle aree.

È, peraltro, obbligatorio attivare le procedure di cui al TITOLO IV del D. Lgs. 81/2008 nel caso si tratti di cantieri temporanei e mobili.

Durante l'effettuazione dei lavori, il DL o un suo incaricato direttamente o tramite il soggetto identificato per il controllo, deve verificare che gli appaltatori operino ed agiscano in maniera compatibile e congruente con le indicazioni di SSL stabilite in sede di contratto, con la Politica dell'azienda, e con il DUVRI ~~(se presente)~~.

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 DL ha la responsabilità di fornire i mezzi e le risorse adeguate allo svolgimento delle attività di addestramento, formazione ed informazione, incluse le competenze esterne o interne necessarie per la loro esecuzione; a questi spetta il compito di approvare il "Programma di formazione, informazione ed addestramento" proposto dal RSPP in collaborazione col RLS ed il Medico Competente; detto programma deve essere aggiornato in occasione della revisione ed eventuale rielaborazione della valutazione dei rischi, nel caso di modifiche legislative, di nuove assunzioni, di cambiamenti nelle mansioni, nei cambiamenti di attività o processi (nuove macchine, attrezzature, impianti, nuove modalità operative, *etc.*), dell'evoluzione tecnica.

Il RSPP ha il dovere di compilare il registro personale della formazione/informazione/addestramento per ciascun lavoratore e per i neo assunti e ha la responsabilità di conservare, nell'archivio delle registrazioni, la documentazione comprovante la formazione, l'informazione e l'addestramento effettuato (verbali di addestramento, copie di attestati di partecipazione, diplomi, *etc.*), i risultati relativi alla verifica delle qualifiche e all'efficacia delle azioni formative eseguite.

Al termine degli interventi formativi, deve essere verificato il grado di apprendimento secondo le modalità previste dall'Accordo Stato Regioni in materia di Formazione alla salute e sicurezza nei luoghi di lavoro, sia per i corsi organizzati dal DL stesso che per quelli erogati presso soggetti esterni.

Nell'ambito del programma di formazione è obbligatorio, inoltre, formare i lavoratori sugli aspetti principali del MOG e su ruoli, compiti e responsabilità di ciascuna figura in esso coinvolta.

Come si evince dalla conferenza stato regioni di giugno 2022 sono state individuate le durate, contenuti minimi e modalità della formazione obbligatoria e aggiornamento periodico a carico del datore di lavoro. Inoltre sono state individuate le modalità di verifica finale di apprendimento obbligatoria per i discenti di tutti i percorsi formativi e di aggiornamento obbligatoria in materia di salute e sicurezza sul lavoro e anche le modalità delle verifiche dell'efficacia durante lo svolgimento delle prestazioni lavorative.

Viene inoltre indicato che l'addestramento consiste nello svolgimento di prova pratica, per l'uso corretto e in sicurezza di attrezzature, macchine, impianti, sostanze, dispositivi, anche di protezione individuale, anche in relazione all'applicazione delle procedure di lavoro

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;
- 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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 11

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 processo di gestione ed utilizzo di opere dell'ingegno per le attività a rischio connesse alle fattispecie di reato previste dall'art. 25 novies *"Reati in materia di violazione del diritto di autore"*, nel rispetto dei principi di massima trasparenza, tempestività e collaborazione, nonché tracciabilità delle attività.
Le prescrizioni della presente procedura integrano, altresì, i principi di comportamento contenuti nel Codice Etico.

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

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* coinvolti nelle attività di gestione ed utilizzo di opere dell'ingegno all'interno 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.

5 RESPONSABILE DELLA PROCEDURA

Per la presente procedura è responsabile il PRES.

6 INDICAZIONI COMPORTAMENTALI

I Destinatari che, per ragione del proprio incarico o della propria funzione, siano coinvolti nella gestione ed utilizzo di opere dell'ingegno e dei sistemi informatici aziendali devono rispettare le norme in materia di proprietà intellettuale e impiegare beni aziendali per adottare condotte che non violino la tutela dei diritti d'autore.

Inoltre, è fatto divieto di utilizzare o installare programmi diversi da quelli autorizzati.

La presente procedura è strettamente correlata con la PMOG 08 "Gestione delle risorse informatiche" e con la PMOG 01 "Gestione tesoreria".

I DESTINATARI DEVONO ATTENERSI, OGNUNO PER LE PARTI DI COMPETENZA, AI SEGUENTI DIVIETI:

- è vietato violare le condizioni di licenza di un software;
- è vietato acquistare software "pirati" per l'azienda;
- è vietato utilizzare banche dati senza la relativa autorizzazione;
- è vietato distribuire e installare dispositivi di decodificazione per l'accesso a un servizio criptato, senza pagamento del canone;
- è vietato l'impiego per finalità aziendali di beni tutelati da diritti acquisiti in elusione dei relativi obblighi o, comunque, con modalità difformi da quelle previste dal titolare;
- è vietata la condivisione o scambio di file in violazione della normativa del diritto d'autore e, comunque, al di fuori degli ordinari e leciti circuiti commerciali dei beni oggetto di proprietà intellettuale (File sharing);
- è vietata l'immissione o condivisione, senza averne diritto, di contenuti protetti da diritti d'autore in un sistema di reti telematiche (upload/download);
- è vietato l'utilizzo di apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere reati riguardanti gli strumenti di pagamento diversi dai contanti o sono specificamente adattati al medesimo scopo;
- è vietato l'utilizzo e l'installazione abusiva di apparecchiature ed altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche, nonché le condotte atte a danneggiare o interrompere un sistema informatico o telematico.

All'atto dell'assunzione, qualsiasi dipendente interessato dalla presente procedura, deve essere adeguatamente formato e di tale attività deve essere redatto un verbale.

7 IL SISTEMA DEI CONTROLLI E I PRESIDI A MITIGAZIONE DEI RISCHI REATO

Per ognuna delle attività sensibili identificate sono stati individuati i sistemi dei controlli e i presidi in essere a mitigazione dei rischi reato in riferimento ai reati di delitti in materia di violazione del diritto di autore,

IN PARTICOLARE:

- Adozione di regole comportamentali all'interno del Codice Etico che prevedono il divieto a tutte le funzioni aziendali, nell'ambito delle proprie attività lavorative e/o mediante utilizzo delle risorse di 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;
- 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:**

  - 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 di terzi utilizzati per lo svolgimento delle attività aziendali, siano opportunamente identificati e che il pagamento delle licenze ai rispettivi fornitori, sia oggetto di un controllo periodico.

8 ARCHIVIAZIONE

Tutta la documentazione prodotta nell'ambito della presente procedura deve essere archiviata da ciascuna funzione, anche attraverso la trasmissione della stessa al RGAD.

9 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Tutti i *Destinatari* coinvolti nelle attività di gestione ed utilizzo delle opere di ingegno sono tenuti a comunicare tempestivamente all'Organismo di Vigilanza qualsiasi violazione ai principi di comportamento adottati o qualsiasi situazione non conforme alla normativa, nonché violazioni 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'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.

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 12

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.

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;

• le attività siano svolte in modo da garantire la veridicità, la completezza, la congruità e la tempestività nella predisposizione dei dati e delle informazioni a supporto dell'istanza di autorizzazione o forniti in esecuzione degli adempimenti prevedendo specifici controlli in contraddittorio;

• 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.

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

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 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.

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:

- richiesta e gestione di agevolazioni, contributi, finanziamenti pubblici, licenze, permessi e autorizzazioni;
- avvio e gestione di procedimenti finalizzati ad accertare il valore catastale di immobili ai fini della determinazione delle relative imposte.

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. il pagamento effettuato su conti correnti di banche appartenenti od operanti in Paesi elencati tra i c.d. "paradisi fiscali", o in favore di società "*off shore*", deve essere eseguito nel rispetto di leggi vigenti in materia;
7. garantire la tracciabilità del pagamento, ovvero stampare e/o archiviare digitalmente la contabile del bonifico eseguito;
8. la documentazione relativa ai pagamenti deve essere inserita nel fascicolo di riferimento;
9. le relative registrazioni contabili – o le schede contabili che dovranno essere richieste al professionista incaricato della tenuta della contabilità se esterna alla Società - devono essere controllate, a campione, dal PRES ed essere conformi alla tipologia di acquisto.

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 di
fondi 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
15
MODELLO ORGANIZZATIVO EX D.LGS.
231/01 – PARTE SPECIALE REV. 5
17 LUGLIO 2023
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.

8 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.

9 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.

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231
PARTE SPECIALE 13

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 733-bis c.p., alcuni dei reati di cui al D.Lgs. 152/06 (Testo Unico Ambientale), nonché alcuni reati di cui alle leggi 150/92, 549/97 e D.Lgs. 202/07. Successivamente, con la Legge 22 maggio 2015 n. 68, il novero dei reati è stato integrato con le fattispecie di cui agli artt. 452-bis, 452-quater, 452-quinquies, 452-sexies e 452-octies c.p. (c.d. "ecoreati").

Infine, il D. Lgs 1° marzo 2018, n. 21, ha abrogato l'art. 260 del D. Lgs. 156/06 introducendo l'art. 452-quaterdecies c.p.

IN PARTICOLARE, L'ART. ART. 25-UNDECIES, D.LGS. 231/01, DISCIPLINA I SEGUENTI REATI:

− inquinamento ambientale (art. 452-bis c.p.);

– disastro ambientale (art. 452-quater c.p.);
– delitti colposi contro l'ambiente (art. 452-quinquies c.p.);
– traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.);
– circostanze aggravanti (art. 452-octies c.p.);
– uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.);
– distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.);
– scarichi di acque reflue industriali senza autorizzazione (art. 137, commi 2, 3 e 5, d. lgs. n.152/2006);
– scarichi nel sottosuolo e nelle acque sotterranee (art. 137, comma 11, d. lgs. n. 152/2006);
– traffico illecito di rifiuti (d. lgs n.152/2006, art. 259);
– scarichi nelle acque del mare di sostanze o materiali vietati da parte di navi o aero-mobili (art. 137, comma 13, D.lgs. 152/06);
– attività di gestione di rifiuti non autorizzata (art. 256, commi 1, 3, 5, 6, primo periodo, D.lgs. 152/06);
– bonifica dei siti (art. 257, commi 1 e 2, D.Lgs. 152/06);
– violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258, comma 4, secondo periodo, D.Lgs. 152/06);
– traffico illecito di rifiuti (art. 259, comma 1, D.Lgs. 152/06);
– attività organizzate per il traffico illecito di rifiuti (art. 260, commi 1 e 2, D.Lgs. 152/06);
– sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis, commi 6 e 7, secondo e terzo periodo, D.Lgs. 152/06);
– sistema informatico di controllo della tracciabilità dei rifiuti (art. 260-bis, comma 8, D.Lgs. 152/06);
– superamento dei valori limite di emissione e dei valori limite di qualità dell'aria (art. 279, comma 5, D.Lgs. 152/06);
– commercio internazionale di specie animali e vegetali in via di estinzione (art. 1, commi 1 e 2, Legge 150/1992);
– commercio internazionale di specie animali e vegetali in via di estinzione (art. 2, commi 1 e 2, Legge 150/1992);
– commercio internazionale di specie animali e vegetali in via di estinzione (art. 3-bis, comma 1, Legge 150/1992);
– commercio internazionale di specie animali e vegetali in via di estinzione (art. 6, comma 4, Legge 150/1992);

− cessazione e riduzione dell'impiego delle sostanze lesive dell'ozono (art. 3, comma 6, Legge 549/1993);

− inquinamento doloso (art. 8, commi 1 e 2, D.Lgs. 202/2007);

− inquinamento colposo (art. 9, commi 1 e 2, D.Lgs. 202/2007).

Pertanto, sono state analizzate, le fattispecie di illeciti presupposto per le quali si applica il Decreto e con riferimento a ciascuna categoria dei medesimi sono state identificate in 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.

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)

Tale ipotesi di reato punisce chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico- fisiche dei rifiuti, nonché chi fa uso di un certificato falso durante il trasporto.

• 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.

•FALSITÀ NELLA TRACCIABILITÀ DEI RIFIUTI MEDIANTE IL SISTRI (ART. 260 BIS, COMMA 6 – COMMA 7, 2° E 3° PERIODO - COMMA 8, C. A.)85

Al sistema informatico di controllo della tracciabilità dei rifiuti, denominato SISTRI, partecipano obbligatoriamente o su base volontaria, secondo i criteri di cui all'art. 188 ter C.A., i produttori di rifiuti e gli altri soggetti che intervengono nella loro gestione (commercianti, intermediari, consorzi di recupero o riciclaggio, soggetti che compiono operazioni di recupero o di smaltimento, trasportatori). In tale contesto sono puniti i delitti consistenti nel fornire false indicazioni sulla natura e sulle caratteristiche di rifiuti al fine della predisposizione di un certificato di analisi dei rifiuti da inserire in SISTRI, nell'inserire nel sistema un certificato falso o nell'utilizzare tale certificato per il trasporto dei rifiuti.

È altresì punito il trasportatore che accompagna il trasporto con una copia cartacea fraudolentemente alterata della scheda SISTRI compilata per la movimentazione dei rifiuti.

NELLO SPECIFICO, LA PRESENTE PROCEDURA HA LO SCOPO DI:

a) indicare le procedure che i collaboratori di BITCONTROL sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, e ai responsabili delle funzioni aziendali che cooperano con lo stesso, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

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

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.

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.

Le disposizioni della presente Parte Speciale hanno per Destinatari tutti i soggetti coinvolti nei processi sopra identificati, affinché gli stessi adottino regole di condotta conformi a quanto prescritto al fine di prevenire il verificarsi dei delitti ivi considerati.

NELLO SPECIFICO LA PRESENTE PARTE SPECIALE HA LO SCOPO DI:

a) indicare i principi che i destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;

b) fornire all'Organismo di Vigilanza, ed ai Responsabili delle funzioni aziendali che con lo stesso cooperano, gli strumenti operativi per esercitare le attività di controllo, monitoraggio e verifica necessarie.

Il principale responsabile della presente procedura è l'Organo Amministrativo.

5. 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 della salute e sicurezza è stato completamente realizzato e se è sufficiente alla realizzazione della politica e degli obiettivi dell'azienda.

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 regolamentazione e gli obblighi legislativi vigenti in materia di tracciabilità dei rifiuti, inclusi, quando in vigore, i nuovi obblighi derivanti dall'adesione al Sistema elettronico di rintracciabilità dei rifiuti (SISTRI).

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.

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.

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.

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

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

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.

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

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.

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.

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 delladiminuzioni 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.

Le misure preventive immaginabili sono legate, in primo luogo, alla diffusione più ampia possibile della filosofia di impresa perseguita dalla Società, ribadendo a chiunque operi al suo interno che il perseguimento di vantaggi per la Società, ottenuti attraverso il compimento di attività penalmente vietate, non è mai consentito e che la Società adotterà ogni misura, anche radicale, ritenuta utile a garantire immediatamente in quel settore organizzativo la situazione di legalità e trasparenza, nell'ipotesi in cui emerga il fondato sospetto che soggetti operanti nella Società siano dediti alla commissione di fatti delittuosi, seppure a vantaggio della Società stessa.

Tuttavia, al solo fine di scongiurare il pur remoto rischio che per la devianza di singoli soggetti operanti all'interno della Società, si possano in qualche modo agevolare dall'esterno, mediante il perfezionamento di rapporti contrattuali, organizzazioni di tipo criminale, si è ritenuto utile richiamare i principi di base e le regole della libera concorrenza - che hanno, peraltro, ispirato da sempre la filosofia di impresa della Società – per esigerne il rispetto.

Poiché i delitti di criminalità organizzata possono essere finalizzati anche alla commissione dei reati già analizzati nelle singole Parti Speciali, si ritiene opportuno specificare che le aree a rischio sopra menzionate devono intendersi integrate con le altre specificatamente individuate in relazione a ciascuna fattispecie oggetto di trattazione nelle altre Parti Speciali del presente Modello.

Tale precisazione si ritiene necessaria per ragioni strettamente legate alla formazione di un Modello quanto più efficace e in linea con il dettato normativo del Decreto.

In considerazione di tale natura peculiare dei reati associativi, non si ritiene possibile localizzare a specifiche aree aziendali il rischio della loro commissione.

LA PRESENTE PARTE SPECIALE HA LA FUNZIONE DI:

- fornire un elenco dei principi cui i destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- fornire all'OdV e ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica allo stesso demandato.

Tali regole di condotta si applicano a tutti i destinatari del Modello e, in particolare, ai soggetti esterni alla Società, nonché a tutti coloro che svolgono le proprie mansioni nelle aree di rischio segnalate nel paragrafo che precede e in quelle delle altre Parti Speciali.

Occorre preliminarmente evidenziare che, in tutte le aree "a rischio reato" qui considerate, occorre osservare i seguenti Presidi di Controllo Generali (a cui si aggiungono Presidi di Controllo Specifici in relazione a singole attività sensibili o categorie di attività sensibili):

1) rispetto del Codice Etico;

2) formazione in ordine al Modello e alle tematiche di cui al D. Lgs. n. 231/2001, rivolta alle risorse operanti nell'ambito delle aree a rischio, con modalità di formazione appositamente pianificate in considerazione del ruolo svolto;

3) diffusione del Modello tra le risorse aziendali, mediante consegna di copia su supporto documentale o telematico e pubblicazione del Modello e dei protocolli maggiormente significativi (ad es., Codice Etico, Sistema Disciplinare, Procedure rilevanti, ecc.) sulla intranet della Società;

4) diffusione del Modello tra i Terzi Destinatari tenuti al rispetto delle relative previsioni (ad es., fornitori, appaltatori, consulenti) mediante pubblicazione dello stesso sul sito intranet della Società o messa a disposizione in formato cartaceo o telematico;

5) dichiarazione con cui i Destinatari del Modello, inclusi i Terzi Destinatari si impegnano a rispettare le previsioni del Decreto;

6) previsione e attuazione del Sistema Disciplinare volto a sanzionare la violazione del Modello e dei Protocolli ad esso connessi;

7) acquisizione di una dichiarazione, sottoscritta da ciascun destinatario del Modello della Società, di impegno al rispetto dello stesso, incluso il Codice Etico;

8) implementazione di un sistema di dichiarazioni periodiche (almeno semestrali) da parte dei Responsabili Interni con le quali si fornisce evidenza del rispetto e/o della inosservanza del Modello (o, ancora di circostanze che possono influire sull'adeguatezza ed effettività del Modello);

9) creazione di una "Sezione 231" all'interno della intranet aziendale, presso cui pubblicare tutti i documenti rilevanti nell'ambito del Modello della Società (ad es., Modello, Codice Etico, Protocolli aziendali in esso richiamati);

10) rispetto dell'organigramma aziendale.

Inoltre, si intendono qui richiamati i presidi di controllo adottati nelle altre Parti Speciali del Modello, in ragione del pericolo di commistione delle fattispecie di reato trattate, unitamente al fenomeno della criminalità organizzata.

Infine, l'Organo amministrativo della Società potrà prevedere ulteriori misure a maggiore tutela delle aree di rischio individuate e a integrazione dei comportamenti sopra elencati.

AREA A RISCHIO N. 1: ADEMPIMENTI IN MATERIA DI PERSONALE

ATTIVITÀ SENSIBILI:

A) GESTIONE DEL PROCESSO DI SELEZIONE, VALUTAZIONE, SCELTA E GESTIONE DEI CANDIDATI.

La selezione, assunzione e gestione del personale è tra le aree più sensibili al rischio di criminalità organizzata, poiché le condotte di associazione per delinquere o associazione di tipo mafioso potrebbero concretizzarsi, quantomeno nelle forme del concorso esterno, in un sistema di reclutamento del personale imposto o caldeggiato da gruppi criminali attraverso un sodalizio criminoso tra soggetti apicali, risorse umane ed esponenti della criminalità organizzata, in cambio di altri vantaggi illeciti conseguibili dalla società.

Reati ipotizzabili:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).

ULTERIORI PRESIDI DI CONTROLLO:

1) osservanza delle procedure e dei principi applicativi per la selezione e per la gestione del personale;

2) divieto per tutti i destinatari e collaboratori esterni alla Società - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di delitti di criminalità organizzata;

3) in relazione alle procedure per la selezione del personale i Destinatati sono tenuti ad applicare i seguenti criteri per scelta:

• professionalità rispetto all'incarico o le mansioni da ricoprire;

• parità di trattamento;

• esibizione del casellario giudiziario e dei carichi pendenti;

• assunzione di informazioni sulla professionalità, sulle competenze e sui ruoli precedentemente ricoperti dalla risorsa;

4) obbligo, per coloro che ricoprono posizioni apicali, limitatamente alle funzioni a loro affidate, di:

• non sottostare a qualsivoglia richiesta contraria alla legge o ai precetti contenuti nel presente Modello;

• informare tempestivamente l'Organo Amministrativo e l'Autorità Giudiziaria ove vengano a conoscenza di fatti o eventi che possano favorire infiltrazioni della criminalità organizzata, ovvero se sottoposti a ricatti o minacce, avvertendo altresì le Autorità competenti.

In ultimo, al fine di prevenire la commissione dei delitti di criminalità organizzata nella selezione, assunzione e gestione del personale, è necessario adottare i seguenti ed ulteriori presidi di controllo:

1. Esistenza di un'idonea segregazione di ruoli e funzioni coinvolti nel sistema di selezione del personale, alfine di assicurare un efficiente sistema di controlli e differenziazione tra chi segnala la necessità di assumere personale, chi seleziona il candidato, chi lo esamina e chi decide di assumerlo.

2. La selezione del personale deve essere effettuata sulla base di criteri selettivi che garantiscono la trasparenza della scelta e che prendono in considerazione la professionalità, le competenze e l'affidabilità del candidato dal rischio di infiltrazione criminale dello stesso

AREA A RISCHIO N. 2: STIPULA E GESTIONE DI CONTRATTI

ATTIVITÀ SENSIBILI:

a) gestione dei contratti di consulenza e di prestazione professionale;

b) gestione dell'anagrafica Consulenti;

c) selezione dei consulenti;

d) gestione degli acquisti e monitoraggio dei beni/servizi ricevuti.

Reati ipotizzabili:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).

ULTERIORI PRESIDI DI CONTROLLO:

1) osservanza delle procedure e dei principi applicativi per la selezione dei consulenti, dei fornitori, di partners o altri professionisti con cui la Società intenda intrattenere rapporti lavorativi;

2) divieto per tutti i destinatari e per i collaboratori esterni alla Società - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di delitti di criminalità organizzata;

3) in relazione alle procedure per la selezione di eventuali partners e/o fornitori e/o consulenti i Destinatati sono tenuti ad applicare i seguenti criteri per scelta:

• professionalità rispetto all'incarico o le mansioni da ricoprire;

• parità di trattamento;

• assunzione di informazioni sulla professionalità, sulle competenze e sui ruoli precedentemente ricoperti dalla risorsa.

4) con riferimento alla gestione di rapporti economici con i consulenti e/o altri partners esterni è imposto di:

• utilizzare specifici conti correnti bancari e/o postali sui quali effettuare i relativi pagamenti;

• imporre, quale unico metodo di pagamento, lo strumento del bonifico bancario o postale, nonché qualsiasi altro metodo che assicuri la piena tracciabilità;

5) obbligo per coloro che ricoprono posizioni apicali, limitatamente alle funzioni a loro affidate di:

• non sottostare a qualsivoglia richiesta contraria alla legge o ai precetti contenuti nel presente Modello;

• informare tempestivamente l'Organo Amministrativo e l'Autorità Giudiziaria ove vengano a conoscenza di fatti o eventi che possano favorire infiltrazioni della criminalità organizzata, ovvero se sottoposti a ricatti o minacce, avvertendo altresì le Autorità competenti;

6) creazione dell'anagrafica Consulenti, nella quale inserire i consulenti della Società, assicurandone la previa qualificazione mediante l'accertamento dei requisiti di professionalità ed onorabilità;

7) formalizzazione dei requisiti da richiedere ai consulenti e dei criteri da utilizzare nella relativa selezione, nonché delle ragioni che giustificano eventuali deroghe dai requisiti e criteri suddetti;

8) individuazione delle risorse deputate: a) a selezionare i potenziali nuovi consulenti b) a formalizzare l'accordo negoziale; c) a gestire l'anagrafica Consulenti; d) a gestire i pagamenti delle fatture emesse dai consulenti;

9) richiesta, ove possibile, di almeno due preventivi in sede di selezione dei consulenti;

10) archiviazione della documentazione inviata dai potenziali candidati e concernente il rispetto dei requisiti richiesti;

11) inserimento negli accordi con i consulenti di una clausola volta ad assicurare il rispetto del Modello e del Codice Etico della Società.

AREA A RISCHIO N. 3: CONTABILITÀ

ATTIVITÀ SENSIBILI:

a) contabilità generale, bilancio e altre comunicazioni sociali;

ULTERIORI PRESIDI DI CONTROLLO:

1) osservanza delle procedure e dei principi applicativi aziendali;

2) divieto per tutti i Destinatari e per i collaboratori esterni alla Società - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di delitti di criminalità organizzata;

3) obbligo per coloro che ricoprono posizioni apicali, limitatamente alle funzioni a loro affidate di:

• non sottostare a qualsivoglia richiesta contraria alla legge o ai precetti contenuti nel presente Modello;

• informare tempestivamente l'Organo Amministrativo e l'Autorità Giudiziaria ove vengano a conoscenza di fatti o eventi che possano favorire infiltrazioni della criminalità organizzata, ovvero se sottoposti a ricatti o minacce, avvertendo altresì le Autorità competenti.

AREA A RISCHIO N. 4: APPROVVIGIONAMENTO

ATTIVITÀ SENSIBILI:

a) approvvigionamento di beni, lavori e servizi;

b) selezione e scelta di fornitori e di vettori con cui intrattenere rapporti di natura contrattuale;

c) individuazione dei partners con cui la Società decida di intrattenere rapporti professionali per lo svolgimento della sua attività.

Reati ipotizzabili:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).

ULTERIORI PRESIDI DI CONTROLLO:

1) osservanza delle procedure e dei principi applicativi per la selezione dei consulenti, dei fornitori, di partners o altri professionisti con cui la Società intenda intrattenere rapporti lavorativi;

2) divieto per tutti i Destinatari e per i collaboratori esterni alla Società - debitamente informati mediante apposite clausole contrattuali - di tenere condotte di qualsiasi natura che possano favorire la commissione di delitti di criminalità organizzata;

3) in relazione alle procedure per la selezione di eventuali partners e/o fornitori e/o consulenti i Destinatati sono tenuti ad applicare i seguenti criteri per scelta:

• professionalità rispetto all'incarico o le mansioni da ricoprire;

• parità di trattamento;

• assunzione di informazioni sulla professionalità, sulle competenze e sui ruoli precedentemente ricoperti dalla risorsa.

4) con riferimento alla gestione di rapporti economici con i consulenti, e/o altri partners esterni è imposto di:

• utilizzare specifici conti correnti bancari e/o postali sui quali effettuare i relativi pagamenti;

• imporre, quale unico metodo di pagamento, lo strumento del bonifico bancario o postale, nonché qualsiasi altro metodo che assicuri la piena tracciabilità;

5) obbligo per coloro che ricoprono posizioni apicali, limitatamente alle funzioni a loro affidate di:

• non sottostare a qualsivoglia richiesta contraria alla legge o ai precetti contenuti nel presente Modello;

• informare tempestivamente l'Organo Amministrativo e l'Autorità Giudiziaria ove vengano a conoscenza di fatti o eventi che possano favorire infiltrazioni della criminalità organizzata, ovvero se sottoposti a ricatti o minacce, avvertendo altresì le Autorità competenti;

6) creazione dell'anagrafica Fornitori, nella quale inserire i fornitori della Società, assicurandone la previa qualificazione mediante l'accertamento dei requisiti di professionalità ed onorabilità;

7) formalizzazione dei requisiti da richiedere ai fornitori e dei criteri da utilizzare nella relativa selezione, nonché delle ragioni che giustificano eventuali deroghe dai requisiti e criteri suddetti;

8) individuazione delle risorse deputate: a) a selezionare i potenziali nuovi fornitori b) a formalizzare l'accordo negoziale; c) a gestire l'anagrafica Fornitori; d) a gestire i pagamenti delle fatture emesse dai fornitori;

9) richiesta, ove possibile, di almeno due preventivi in sede di selezione dei fornitori;

10) archiviazione della documentazione inviata dai potenziali candidati e concernente il rispetto dei requisiti richiesti;

11) sottoscrizione di un contratto con tutti i fornitori, con previsione, per quelli per i quali si prevede di procedere con l'Ordine di Acquisto, della previa consultazione ed accettazione delle proprie Condizioni Generali di Contratto;

12) inserimento nei contratti di fornitura di una clausola volta ad assicurare il rispetto del Modello e del Codice Etico della Società.

In ultimo, al fine di prevenire la commissione dei delitti di criminalità organizzata nella gestione degli acquisti di beni e servizi e per l'affidamento degli incarichi di consulenza, è necessario adottare i seguenti ed ulteriori presidi di controllo:

1. Definire i criteri qualitativi e quantitative di selezione dei fornitori;
2. Verificare, preventivamente, i requisiti di onorabilità e professionalità dei fornitori di beni e/o servizi, laddove si tratti di fornitori non già conosciuti da 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).

AREA A RISCHIO N. 6: GESTIONE DEI SERVIZI FORNITI DALLA SOCIETÀ

ATTIVITÀ SENSIBILI:

a) gestione della clientela;

b) rapporti con eventuali intermediari, procacciatori di affari e simili;

c) offerta dei servizi forniti dalla Società.

Reati ipotizzabili:

- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso anche straniera (art. 416-bis c.p.)
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).

ULTERIORI PRESIDI (SPECIFICI) DI CONTROLLO:

Poiché i delitti di criminalità organizzata possono essere finalizzati anche alla commissione dei reati già analizzati nelle singole Parti Speciali, si ritiene opportuno specificare che le aree a rischio sopra menzionate andranno integrate con le altre precedentemente individuate in relazione a ciascuna fattispecie oggetto di trattazione nelle altre Parti del presente Modello.

Tale precisazione si ritiene necessaria per ragioni strettamente legate alla formazione di un Modello quanto più efficace e in linea con il dettato normativo del Decreto.

Le aree indicate assumono rilevanza anche nell'ipotesi in cui le attività sopra elencate siano eseguite, in tutto o in parte, da persone fisiche o giuridiche in nome o per conto della Società, in virtù di apposite deleghe o per la sottoscrizione di specifici rapporti contrattuali, dei quali deve essere tempestivamente informato l'OdV.

7 PRINCIPI GENERALI DI COMPORTAMENTO E REGOLE DI CONDOTTA

I Destinatari del Modello sono tenuti ad osservare, nella fattispecie delle attività sensibili individuate nella presente procedura, nonché nella sfera dei rapporti con ogni stackeholder esterno, le seguenti regole di condotta:

- Garantire il rispetto dello Statuto e delle norme di legge applicabili nelle operazioni societarie;
- Interdire l'ingresso nella compagine societaria di soggetti (sia essi persone fisiche che giuridiche) dei quali sia conosciuta o sospetta l'appartenenza ad operazioni criminali o comunque operanti al di fuori della liceità quali, a titolo meramente esemplificativo ma non esaustivo, persone legate alla camorra, alla mafia, al traffico di sostanze stupefacenti, all'usura, al riciclaggio ecc.;

- Non utilizzare strumenti e conti anonimi o contanti per il compimento di operazioni di trasferimento di importi rilevanti;
- Rispettare tutti i requisiti relativi alla selezione dei fornitori, con particolare attenzione all'incensuratezza degli stessi e alla valutazione preventiva in ordine congruità dei prezzi richiesti rispetto ai valori di mercato
- Divieto di prestare qualsivoglia forma di collaborazione o anche solo semplice contatto con soggetti colpiti o indiziati da provvedimenti giudiziari legati alla criminalità organizzata;
- Divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti effettivi e/o potenziali che possano, in maniera diretta ed indiretta, favorire le condizioni per reati di criminalità organizzata;
- Divieto di porre in essere qualsiasi situazione e/o tenere qualsiasi comportamento in conflitto di interessi con la Pubblica Sicurezza;

IN PARTICOLARE È FATTO DIVIETO DI:

- Promuovere, costituire, organizzare, dirigere partecipare ovvero finanziare in alcuna forma le associazioni di cui agli artt. 416 e 416 bis c.p.;
- Effettuare donazioni o altra forma di erogazione di fondi, anche indirette, nei confronti di simili associazioni;
- Fornire supporto logistico e/o qualsivoglia altro tipo a persone che partecipano alle predette associazioni;
- Stipulare qualsiasi tipo di contratto o avere rapporti commerciali, di collaborazione o di diverso tipo con controparti che abbiano precedenti penali o carichi pendenti noti alla Società in materia di reati di criminalità organizzata, ovvero dei quali si presume il vincolo associativo e la finalità criminale, anche se non si ha la certezza tanto del vincolo quanto dello scopo illecito, purchè si disponga di elementi sufficienti a farne desumere l'esistenza e ciononostante non si desista dall'instaurazione dei predetti rapporti.

8 COMUNICAZIONI ALL'ODV E POTERI DI CONTROLLO

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

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

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

L'Organismo di Vigilanza può anche intervenire a seguito di informazioni e segnalazioni ricevute.

L'ODV DOVRÀ EFFETTUARE:

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

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

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

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

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

ELENCO ALLEGATI

Allegato 1: Codice Etico

Allegato 2: Clausola contrattuale

Allegato 3: Elenco reati sanzionati dal Decreto

Allegato 4: Composizione dell'Organismo di Vigilanza

Allegato 5: Compensi, cause di (in)eleggibilità, decadenza e sospensione dei componenti dell'Organismo di Vigilanza

Allegato 6: procedura WHISTLEBLOWING

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

- ALLEGATO 1 -

CODICE ETICO

Il presente Codice Etico è stato approvato 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

7 LINEE GUIDA DEL SISTEMA SANZIONATORIO

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.

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.

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 superiore gerarchico, al Consiglio di Amministrazione, restando valide le norme specifiche previste dal Codice Civile.

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

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

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

(ai sensi del D. Lgs. 8 giugno 2001 n. 231)

- ALLEGATO 3 -

ELENCOREATI SANZIONATI DAL DECRETO

1. Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24, D.Lgs. n. 231/2001) [articolo modificato dalla L. 161/2017 e dal D.Lgs. n. 75/2020]

- Malversazione di erogazioni pubbliche (art. 316-bis c.p.) [articolo modificato dal D.L. n. 13/2022]
- Indebita percezione di erogazioni pubbliche (art. 316-ter c.p.) [articolo modificato dalla L. n. 3/2019 e dal D.L. n. 13/2022]
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art.640, comma 2, n.1, c.p.)
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.) [articolo modificato dal D.L. n. 13/2022]
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.)
- Frode nelle pubbliche forniture (art. 356 c.p.) [introdotto dal D.Lgs. n. 75/2020]

- Frode ai danni del Fondo europeo agricolo (art. 2. L. 23/12/1986, n.898) [introdotto dalla Legge 9 Ottobre 2023 n. 137]
- Turbata libertà degli incanti (Art. 353 c.p.) [introdotto dal D.Lgs. n. 75/2020]
- Turbata libertà del procedimento di scelta del contraente (Art. 353-bis c.p.) [introdotto dalla Legge 9 Ottobre 2023 n. 137]

2. Delitti informatici e trattamento illecito di dati (Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019]

- Documenti informatici (art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
- Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.) [articolo modificato dalla Legge n. 238/2021]
- Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) [articolo modificato dalla Legge n. 238/2021]
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) [articolo modificato dalla Legge n. 238/2021]
- Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) [articolo modificato dalla Legge n. 238/2021]
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)
- Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)
- Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)

3. Delitti di criminalità organizzata (Art. 24-ter, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009 e modificato dalla L. 69/2015]

- Associazione di tipo mafioso anche straniere (art. 416-bis c.p.) [articolo modificato dalla L. n. 69/2015]
- Associazione per delinquere (art. 416 c.p.)

- Scambio elettorale politico-mafioso (art. 416-ter c.p.) [così sostituito dall´art. 1, comma 1, L. 17 aprile 2014, n. 62, a decorrere dal 18 aprile 2014, ai sensi di quanto disposto dall´art. 2, comma 1 della medesima L. 62/2014)
- Sequestro di persona a scopo di estorsione (art. 630 c.p.)
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 DPR 9 ottobre 1990, n. 309) [comma 7-bis aggiunto dal D.Lgs. n. 202/2016]
- Tutti i delitti se commessi avvalendosi delle condizioni previste dall´art. 416-bis c.p. per agevolare l´attività delle associazioni previste dallo stesso articolo (L. 203/91)
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110 (art. 407, co. 2, lett. a), numero 5), c.p.p.)

4. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (Art. 25, D.Lgs. n. 231/2001) [modificato dalla L. n. 190/2012, dalla L. 3/2019 e dal D.Lgs. n. 75/2020]

- Concussione (art. 317 c.p.) [articolo modificato dalla L. n. 69/2015]
- Corruzione per l'esercizio della funzione (art. 318 c.p.) [modificato dalla L. n. 190/2012, L. n. 69/2015 e L. n. 3/2019]
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.) [articolo modificato dalla L. n. 69/2015]
- Circostanze aggravanti (art. 319-bis c.p.)
- Corruzione in atti giudiziari (art. 319-ter c.p.) [articolo modificato dalla L. n. 69/2015]
- Induzione indebita a dare o promettere utilità (art. 319-quater) [articolo aggiunto dalla L. n. 190/2012 e modificato dalla L. n. 69/2015]
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)
- Pene per il corruttore (art. 321 c.p.)
- Istigazione alla corruzione (art. 322 c.p.)
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.) [modificato dalla L. n. 190/2012 e dalla L. n. 3/2019]
- Traffico di influenze illecite (art. 346-bis c.p.) [modificato dalla L. 3/2019]
- Peculato (limitatamente al primo comma) (art. 314 c.p.) [introdotto dal D.Lgs. n. 75/2020]
- Peculato mediante profitto dell'errore altrui (art. 316 c.p.) [introdotto dal D.Lgs. n. 75/2020]
- Abuso d'ufficio (art. 323 c.p.) [introdotto dal D.Lgs. n. 75/2020]

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

- Alterazione di monete (art. 454 c.p.)
- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.)
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.)
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.)
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.)
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.)
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.)
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.)
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.)
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.)

6. Delitti contro l'industria e il commercio (Art. 25-bis.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

- Illecita concorrenza con minaccia o violenza" (art. 513-bis c.p.)
- Turbata libertà dell'industria o del commercio (art. 513 c.p.)
- Frodi contro le industrie nazionali (art. 514 c.p.)
- Frode nell'esercizio del commercio (art. 515 c.p.)
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.)
- Vendita di prodotti industriali con segni mendaci (art. 517 c.p.)
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.)
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater c.p.)

7. Reati societari (Art. 25-ter, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. 69/2015, dal D.Lgs. n.38/2017 e dal D.Lgs. n. 19/2023]

- False comunicazioni sociali (art. 2621 c.c.) [articolo modificato dalla L. n. 69/2015]
- Fatti di lieve entità (art. 2621-bis c.c.)
- False comunicazioni sociali delle società quotate (art. 2622 c.c.) [articolo modificato dalla L n. 69/2015]
- Impedito controllo (art. 2625, comma 2, c.c.)
- Indebita restituzione di conferimenti (art. 2626 c.c.)
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.) [aggiunto dalla legge n. 262/2005]
- Formazione fittizia del capitale (art. 2632 c.c.)
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
- Corruzione tra privati (art. 2635 c.c.) [aggiunto dalla legge n. 190/2012; modificato dal D.Lgs. n. 38/2017 e dalla L. n. 3/2019]
- Istigazione alla corruzione tra privati (art. 2635-bis c.c.) [aggiunto dal D.Lgs. n. 38/2017 e modificato dalla L. n. 3/2019]
- Illecita influenza sull'assemblea (art. 2636 c.c.)
- Aggiotaggio (art. 2637 c.c.)
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.)
- False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023) [aggiunto dal D.Lgs. n. 19/2023]

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

- Associazioni sovversive (art. 270 c.p.)
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270 bis c.p.)
- Circostanze aggravanti e attenuanti (art. 270-bis.1 c.p.) [introdotto dal D.Lgs. n. 21/2018]
- Assistenza agli associati (art. 270 ter c.p.)
- Arruolamento con finalità di terrorismo anche internazionale (art. 270 quater c.p.)

- Organizzazione di trasferimento per finalità di terrorismo (art. 270-quater.1) [introdotto dal D.L. n. 7/2015, convertito, con modificazioni, dalla L. n. 43/2015]
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies c.p.)
- Finanziamento di condotte con finalità di terrorismo (L. n. 153/2016, art. 270 quinquies.1 c.p.)
- Sottrazione di beni o denaro sottoposti a sequestro (art. 270 quinquies.2 c.p.)
- Condotte con finalità di terrorismo (art. 270 sexies c.p.)
- Attentato per finalità terroristiche o di eversione (art. 280 c.p.)
- Atto di terrorismo con ordigni micidiali o esplosivi (art. 280 bis c.p.)
- Atti di terrorismo nucleare (art. 280 ter c.p.)
- Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.)
- Sequestro a scopo di coazione (art. 289-ter c.p.) [introdotto dal D.Lgs. 21/2018]
- Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo (art. 302 c.p.)
- Cospirazione politica mediante accordo (art. 304 c.p.)
- Cospirazione politica mediante associazione (art. 305 c.p.)
- Banda armata: formazione e partecipazione (art. 306 c.p.)
- Assistenza ai partecipi di cospirazione o di banda armata (art. 307 c.p.)
- Impossessamento, dirottamento e distruzione di un aereo (L. n. 342/1976, art. 1)
- Danneggiamento delle installazioni a terra (L. n. 342/1976, art. 2)
- Sanzioni (L. n. 422/1989, art. 3)
- Pentimento operoso (D.Lgs. n. 625/1979, art. 5)
- Convenzione di New York del 9 dicembre 1999 (art. 2)

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

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

10. Delitti contro la personalità individuale (Art. 25-quinquies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003; modificato dalla L. n. 199/2016]

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.)
- Prostituzione minorile (art. 600-bis c.p.)
- Pornografia minorile (art. 600-ter c.p.)
- Detenzione o accesso a materiale pornografico (art. 600-quater) [articolo modificato dalla Legge n. 238/2021]
- Pornografia virtuale (art. 600-quater.1 c.p.) [aggiunto dall'art. 10, L. 6 febbraio 2006 n. 38]

- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.)
- Tratta di persone (art. 601 c.p.) [modificato dal D.Lgs. 21/2018]
- Acquisto e alienazione di schiavi (art. 602 c.p.)
- Intermediazione illecita e sfruttamento del lavoro (art. 603-bis c.p.)
- Adescamento di minorenni (art. 609-undecies c.p.) [articolo modificato dalla Legge n. 238/2021]

11. Reati di abuso di mercato (Art. 25-sexies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005]

- Manipolazione del mercato (art. 185 D.Lgs. n. 58/1998) [articolo modificato dal D.Lgs. 107/2018 e dalla Legge n. 238/2021]
- Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 D.Lgs. n. 58/1998) [articolo modificato dalla Legge n. 238/2021]

12. Altre fattispecie in materia di abusi di mercato (Art. 187-quinquies TUF) [articolo modificato dal D.Lgs. n. 107/2018]

- Divieto di manipolazione del mercato (art. 15 Reg. UE n. 596/2014)
- Divieto di abuso di informazioni privilegiate e di comunicazione illecita di informazioni privilegiate (art. 14 Reg. UE n. 596/2014)

13. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (Art. 25-septies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007; modificato L. n. 3/2018]

- Lesioni personali colpose (art. 590 c.p.)
- Omicidio colposo (art. 589 c.p.)

14. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonchè autoriciclaggio (Art. 25-octies, D.Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014 e dal D.Lgs. n. 195/2021]

- Ricettazione (art. 648 c.p.) [articolo modificato dal D.Lgs. 195/2021]
- Riciclaggio (art. 648-bis c.p.) [articolo modificato dal D.Lgs. 195/2021]

- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.) [articolo modificato dal D.Lgs. 195/2021]
- Autoriciclaggio (art. 648-ter.1 c.p.) [articolo modificato dal D.Lgs. 195/2021]
- Trasferimento fraudolento di valori (Art.512-bis c.p.) [introdotto dalla Legge 9 Ottobre 2023 n. 137]

15. 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]

- 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.)

16. Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1 comma 2, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. 184/2021]

Altre fattispecie

17. Delitti in materia di violazione del diritto d'autore (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]

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

scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter legge n.633/1941)

- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies legge n.633/1941)
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies legge n.633/1941).

18. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 116/2009]

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

19. Reati ambientali (Art. 25-undecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 121/2011, modificato dalla L. n. 68/2015, modificato dal D.Lgs. n. 21/2018]

- Disastro ambientale (art. 452-quater c.p.)
- Inquinamento ambientale (art. 452-bis c.p.)
- Delitti colposi contro l´ambiente (art. 452-quinquies c.p.)
- Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)
- Circostanze aggravanti (art. 452-octies c.p.)
- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.)
- Distruzione o deterioramento di habitat all´interno di un sito protetto (art. 733-bis c.p.)
- Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n.150/1992, art. 1, art. 2, art. 3-bis e art. 6)
- Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D. Lgs n.152/2006, art. 137)
- Attività di gestione di rifiuti non autorizzata (D. Lgs n.152/2006, art. 256)
- Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D. Lgs n. 152/2006, art. 257)

- Traffico illecito di rifiuti (D. Lgs n.152/2006, art. 259)
- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D. Lgs n.152/2006, art. 258)
- Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.) [introdotto dal D.Lgs. n. 21/2018]
- False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (D. Lgs n.152/2006, art. 260-bis)
- Sanzioni (D.Lgs. n. 152/2006, art. 279)
- Inquinamento doloso provocato da navi (D. Lgs. n.202/2007, art. 8)
- Inquinamento colposo provocato da navi (D. Lgs. n.202/2007, art. 9)
- Cessazione e riduzione dell´impiego delle sostanze lesive (L. n. 549/1993 art. 3)

20. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 109/2012, modificato dalla Legge 17 ottobre 2017 n. 161]

- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22, comma 12 bis, D.Lgs. n. 286/1998)
- Disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3 bis, 3 ter e comma 5, D.Lgs. n. 286/1998)

21. Razzismo e xenofobia (Art. 25-terdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla Legge 20 novembre 2017 n. 167, modificato dal D.Lgs. n. 21/2018]

- Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (art. 604-bis c.p.) [aggiunto dal D.Lgs. n. 21/2018]

22. Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 39/2019]

- Esercizio abusivo di attività di giuoco o di scommessa (art. 4, L. n. 401/1989)
- Frodi in competizioni sportive (art. 1, L. n. 401/1989)

23. Reati Tributari (Art. 25-quinquesdecies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 157/2019 e dal D.Lgs. n. 75/2020]

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000)

- Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)
- Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000)
- Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000)
- Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)
- Dichiarazione infedele (art. 4 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]
- Omessa dichiarazione (art. 5 D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]
- Indebita compensazione (art. 10-quater D.Lgs. n. 74/2000) [introdotto dal D.Lgs. n. 75/2020]

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

- Contrabbando nel movimento delle merci attraverso i confini di terra e gli spazi doganali (art. 282 DPR n. 43/1973)
- Contrabbando nel movimento delle merci nei laghi di confine (art. 283 DPR n. 43/1973)
- Contrabbando nel movimento marittimo delle merci (art. 284 DPR n. 43/1973)
- Contrabbando nel movimento delle merci per via aerea (art. 285 DPR n. 43/1973)
- Contrabbando nelle zone extra-doganali (art. 286 DPR n. 43/1973)
- Contrabbando per indebito uso di merci importate con agevolazioni doganali (art. 287 DPR n. 43/1973)
- Contrabbando nei depositi doganali (art. 288 DPR n. 43/1973)
- Contrabbando nel cabotaggio e nella circolazione (art. 289 DPR n. 43/1973)
- Contrabbando nell'esportazione di merci ammesse a restituzione di diritti (art. 290 DPR n. 43/1973)
- Contrabbando nell'importazione od esportazione temporanea (art. 291 DPR n. 43/1973)
- Contrabbando di tabacchi lavorati esteri (art. 291-bis DPR n. 43/1973)
- Circostanze aggravanti del delitto di contrabbando di tabacchi lavorati esteri (art. 291-ter DPR n. 43/1973)
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater DPR n. 43/1973)
- Altri casi di contrabbando (art. 292 DPR n. 43/1973)
- Circostanze aggravanti del contrabbando (art. 295 DPR n. 43/1973)

25. Delitti contro il patrimonio culturale (Art. 25-septiesdecies, D.Lgs. n. 231/2001) [Articolo aggiunto dalla L. n. 22/2022]

- Furto di beni culturali (art. 518-bis c.p.)
- Appropriazione indebita di beni culturali (art. 518-ter c.p.)
- Ricettazione di beni culturali (art. 518-quater c.p.)
- Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.)

- Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.)
- Importazione illecita di beni culturali (art. 518-decies c.p.)
- Uscita o esportazione illecite di beni culturali (art. 518-undecies c.p.)
- Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies c.p.)
- Contraffazione di opere d'arte (art. 518-quaterdecies c.p.)

26. Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (Art. 25-duodevicies, D.Lgs. n. 231/2001) [Articolo aggiunto dalla L. n. 22/2022]

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

27. Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013) [Costituiscono presupposto per gli enti che operano nell´ambito della filiera degli oli vergini di oliva]

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

28. Reati transnazionali (L. n. 146/2006) [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]

- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al D.P.R. 9 ottobre 1990, n. 309)
- Disposizioni contro le immigrazioni clandestine (art. 12, commi 3, 3-bis, 3-ter e 5, del testo unico di cui al D. Lgs. 25 luglio 1998, n. 286)

- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al D.P.R. 23 gennaio 1973, n. 43)
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)
- Favoreggiamento personale (art. 378 c.p.)
- Associazione per delinquere (art. 416 c.p.)
- Associazione di tipo mafioso (art. 416-bis c.p.)

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

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

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

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

INDICE

*

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.

3 Ambito di applicazione

La presente Procedura si applica alle Funzioni aziendali della BitControl S.r.l. ed a tutto il personale coinvolto nel processo di Whistleblowing.

La Procedura disciplina le seguenti attività:

➢ modalità di Segnalazione del dipendente e/o del terzo avente ad oggetto la violazione del Modello 231/01 o del Codice Etico della BitControl S.r.l.;

➢ istruttoria dell'Organismo di Vigilanza relativamente alla Segnalazione ricevuta;

➢ attività dell'Organismo di Vigilanza successiva all'istruttoria.

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*".

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" ha 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 SCOPO E DESTINATARI

La presente Procedura, che costituisce parte integrante del Modello 231/01 di BitControl S.r.l., ha una duplice finalità:

• regolamentare il processo di "Whistleblowing";

• definire i ruoli, compiti e responsabilità dei soggetti coinvolti nel suddetto processo.

II Whistleblowing è il sistema di segnalazione con il quale un soggetto che opera per conto della BitControl contribuisce a segnalare comportamenti contrari al Codice Etico, al Modello Organizzativo, alla Politica Anticorruzione, alle procedure aziendali anticorruzione adottate dalla Società, nonché a far emergere rischi e/o situazioni potenzialmente pregiudizievoli per la stessa Società. Lo scopo principale del Whistleblowing è quindi quello di gestire eventuali Segnalazioni, al fine di individuare eventuali problematiche, che potrebbero derivare da un illecito aziendale, rilevanti ai sensi del D.lgs. 231/01.

La presente Procedura, approvata dal Consiglio di Amministrazione della Società con verbale del 14.11.2022, regola quindi, anche attraverso indicazioni operative, il processo di invio, ricezione, analisi, trattamento e gestione delle Segnalazioni di condotte illecite, rilevanti ai sensi D.lgs. 231/01, nonché delle violazioni del relativo Modello 231/01, trasmesse dal Segnalante (Whistleblower) all'ODV della BitControl S.r.l.. Il presente documento disciplina, inoltre, le forme di tutela della riservatezza del Segnalante per evitare possibili ritorsioni nei suoi confronti.

La presente Procedura si applica a qualsiasi Segnalazione effettuata dai soggetti apicali, dalle persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali, nonché dai soggetti terzi meglio individuati al successivo paragrafo 6, attraverso gli appositi canali di comunicazione, riservati e messi a disposizione dalla Società.

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.

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 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.

Le Segnalazioni anonime verranno prese in considerazione per ulteriori verifiche solo se aventi un contenuto che risulti adeguatamente dettagliato e circostanziato.

Il perseguimento dell'interesse all'idoneità al Modello 231, che con la presente Procedura la Società intende perseguire, costituisce ai sensi dell'art. 3 della L. 179/2017 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.. 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

Il destinatario della Segnalazione è l'Organismo di Vigilanza della Società.

Pertanto, tutte le Segnalazioni inviate a soggetti diversi dall'OdV potranno non essere trattate alla stregua della presente Procedura e ciò in ragione della competenza esclusiva attribuita dalla medesima Procedura all'Organismo di Vigilanza della BitControl S.r.l.

Invero, sul punto si precisa che, qualora la Segnalazione non sia correttamente inviata all'Organismo di Vigilanza, la stessa dovrà essere tempestivamente inoltrata dall'erroneo destinatario al medesimo OdV, affinché esso possa valutare le Segnalazioni ricevute e determinare le eventuali iniziative.

L'OdV 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.

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 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) 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 G.B. Nicolosi n. 334, 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

L'OdV 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; l'OdV, 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.

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 l'OdV 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, l'Organismo di Vigilanza 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 invece all'esito dell'istruttoria medesima la Segnalazione dovesse apparire infondata o irrilevante, l'OdV provvederà ad archiviarla precisandone le relative motivazioni e 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. L'OdV 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.

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 la sua autorizzazione e 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 discriminatorie si intendono le azioni disciplinari ingiustificate, le molestie sul luogo di lavoro e ogni altra forma di ritorsione e/o reazione sfavorevole al Segnalante.

Il Segnalante qualora ritenga che lo stesso abbia subito o stia subendo una misura discriminatoria, provvede a dare notizia circostanziata dell'avvenuta discriminazione all'Organismo di Vigilanza affinché provveda a valutarne la fondatezza nonché all'Ispettorato Nazionale del lavoro 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.

In ogni caso la violazione dell'obbligo di riservatezza e/o del divieto di discriminazione 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, 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. In caso di abuso o falsità della Segnalazione, resta ferma quindi ogni eventuale responsabilità del Segnalante per calunnia, diffamazione, danno morale o altro danno civilmente o penalmente rilevante.

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, anche secondo quanto previsto dal sistema sanzionatorio adottato ai sensi del Modello 231/01 e del D.lgs. 231/01 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

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 all'Organismo di Vigilanza.

Per maggiori dettagli sul sistema di rilevamento degli illeciti e segnalazioni all'Organismo di Vigilanza si rimanda a quanto definito nel Modello 231/01.

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 condotte illecite o violazioni del Modello di cui al D.lgs. 231/01

1 Dati del segnalante

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):	

3 Descrizione del fatto:

4 La condotta è illecita perché:

Altro da Specificare:	