



**MODELLO DI ORGANIZZAZIONE, GESTIONE E
CONTROLLO AI SENSI DELL' EX D.Lgs 231/2001**

Approvato dall'Amministratore unico in data 06/12/2023

Approvato dall' ODV in data 06/12/2023

Indice:

1. QUADRO NORMATIVO	4
1.1. IL DECRETO LEGISLATIVO N. 231 DEL 2001	4
1.2. FATTISPECIE DI REATO AI SENSI DEL D.LGS. 231/2001.....	4
1.3. APPARATO SANZIONATORIO	6
1.4. REATI COMMESSI ALL'ESTERO.....	7
1.5. MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO.....	7
1.6. LINEE GUIDA PER LA PREDISPOSIZIONE DEI MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO.....	9
2. DESCRIZIONE DELL'ENTE.....	9
2.1. MAJOR BIT: ORGANIZZAZIONE E REALTÀ OPERATIVA	9
3. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO E METODOLOGIA SEGUITA PER L'ADOZIONE	10
3.1. PREMESSA.....	10
3.2. IL PROGETTO DI MAJOR BIT PER L'AGGIORNAMENTO DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO.....	11
3.3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI MAJOR BIT	13
3.4. INDIVIDUAZIONE DELLE ATTIVITÀ SENSIBILI	15
3.5. DESTINATARI	15
3.6. IL CODICE ETICO.....	16
4. L'ORGANISMO DI VIGILANZA.....	16
4.1. PREMESSA.....	16
4.2. REQUISITI SOGGETTIVI DEI COMPONENTI	17
4.3. ISTITUZIONE, NOMINA E REVOCA DELL'ORGANISMO DI VIGILANZA.....	17
4.4. FUNZIONI E POTERI.....	18
4.5. REGOLE DI CONDOTTA.....	19
4.6. SEGNALAZIONI ALL'ODV.....	19
4.7. RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI	20
4.8. REPORTING DELL'ORGANISMO DI VIGILANZA VERSO GLI ORGANI DELLA SOCIETÀ.....	21
5. SEGNALAZIONI DI REATI O IRREGOLARITÀ NELL'AMBITO DEL RAPPORTO DI LAVORO (C.D. WHISTLEBLOWING).....	21
6. IL SISTEMA DISCIPLINARE.....	24
6.1. PREMESSA.....	24
6.2. MISURE NEI CONFRONTI DI LAVORATORI DIPENDENTI NON DIRIGENTI.....	25
6.3. MISURE NEI CONFRONTI DEI DIRIGENTI	26
6.4. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI	27
6.5. MISURE NEI CONFRONTI DEL REVISORE.....	27

6.6. MISURE NEI CONFRONTI DI COLLABORATORI, CONSULENTI E SOGGETTI TERZI	39
7. LA FORMAZIONE E L'INFORMAZIONE.....	27
8. ADOZIONE DEL MODELLO – CRITERI DI AGGIORNAMENTO E ADEGUAMENTO DEL MODELLO	28
9. PARTE SPECIALE.....	29
9.1. PREMESSA	29
9.2. LE ATTIVITÀ SENSIBILI.....	29
9.3. IL SISTEMA DEI CONTROLLI	31
9.3.1. PRINCIPI DI COMPORTAMENTO	31
9.3.2. PRINCIPI DI CONTROLLO	32
10. ATTIVITÀ SENSIBILI.....	34
10.1. ACQUISIZIONE DELLE COMMESSE	34
10.2. GESTIONE DELLA COMMESSA.....	37
10.3. GESTIONE DELLE ATTIVITÀ DI DELIVERY.....	40
10.4. GESTIONE DEGLI EVENTUALI CONTENZIOSI GIUDIZIALI O PROCEDIMENTI ARBITRALI	43
10.5. GESTIONE DELLE ATTIVITÀ PER L’OTTENIMENTO DI CONTRIBUTI/FINANZIAMENTI, ANCHE SOTTOFORMA DI CREDITO D’IMPOSTA.....	48
10.6. GESTIONE DELLE ISPEZIONI	47
10.7. GESTIONE DEGLI INVESTIMENTI.....	49
10.8. GESTIONE DEGLI ACQUISTI.....	50
10.9. SELEZIONE, ASSUNZIONE E GESTIONE DEL PERSONALE (COMPRESI I SOGGETTI APPARTENENTI A CATEGORIE PROTETTE O LA CUI ASSUNZIONE È AGEVOLATA).	53
10.10. GESTIONE DEI FLUSSI FINANZIARI (PAGAMENTI E INCASSI).....	56
10.11. GESTIONE DEI RAPPORTI INFRAGRUPPO	59
10.12 ELABORAZIONE DEL BILANCIO E DEL RENDICONTO FINANZIARIO E COMUNICAZIONE A STAKEHOLDERS E/O A TERZI DI DATI E INFORMAZIONI RELATIVI ALLA SITUAZIONE ECONOMICA, PATRIMONIALE E FINANZIARIA DELLA SOCIETÀ.....	61
10.13. PREDISPOSIZIONE DI DICHIARAZIONI DEI REDDITI O DI SOSTITUTI D’IMPOSTA O DI ALTRE DICHIARAZIONI FUNZIONALI ALLA LIQUIDAZIONE DI TRIBUTI IN GENERE.....	63
10.14. GESTIONE DELLE RISORSE INFORMATICHE.....	66
10.15. GESTIONE DEGLI ADEMPIMENTI IN MATERIA AMBIENTALE	68
10.16. GESTIONE DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO	69
Note.....	76

1. QUADRO NORMATIVO

1.1. IL DECRETO LEGISLATIVO N. 231 DEL 2001

Con il Decreto Legislativo 8 giugno 2001 n. 231 (di seguito, il “**D.Lgs. 231/2001**” o “**Decreto**”), emanato in attuazione della delega conferita al Governo con l’art. 11 della Legge 29 settembre 2000, n. 300¹, il Legislatore ha introdotto la disciplina della “*Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato*” che trova applicazione nei confronti degli enti forniti di personalità giuridica, società e associazioni anche prive di personalità giuridica.

Secondo quanto previsto dal Decreto, gli enti possono essere ritenuti “responsabili” per alcuni reati commessi o tentati nel loro interesse o a loro vantaggio, da parte di esponenti dei vertici aziendali (i c.d. soggetti “in posizione apicale” o, semplicemente, “apicali”) e di coloro che sono sottoposti alla direzione o vigilanza di questi ultimi (art. 5, comma 1, del D.Lgs. 231/2001)².

La responsabilità amministrativa delle Società è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato e, a determinate condizioni, si affianca a quest’ultima.

L’ampliamento di responsabilità introdotto con l’emanazione del D.Lgs. 231/2001 mira - sostanzialmente - a coinvolgere, nella punizione di determinati reati, il patrimonio delle società e, in ultima analisi, gli interessi economici dei soci, i quali, fino all’entrata in vigore del D.Lgs. 231/2001, non pativano dirette conseguenze dalla realizzazione di reati commessi, nell’interesse o a vantaggio della propria società.

Tuttavia, la responsabilità amministrativa è esclusa se l’ente ha, tra l’altro, adottato ed efficacemente attuato, prima della commissione dei reati, un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della stessa specie di quello verificatosi.

Aggiornamenti normativi recenti

Successivamente all’adozione del presente Modello, il quadro normativo di riferimento ha registrato ulteriori evoluzioni, tra cui in particolare:

- il D.Lgs. 10 marzo 2023 n. 24 in materia di whistleblowing, che ha rafforzato le tutele del segnalante e ampliato gli obblighi organizzativi a carico degli enti;
- gli sviluppi normativi in materia di digitalizzazione, sicurezza informatica e protezione dei dati, nonché le iniziative europee in tema di intelligenza artificiale (AI Act), che possono incidere sui profili di rischio rilevanti ai sensi del D.Lgs. 231/2001.

La Società si impegna a monitorare costantemente tali evoluzioni al fine di garantire l’adeguamento continuo del presente Modello.

1.2. FATTISPECIE DI REATO AI SENSI DEL D.LGS. 231/2001

In base al D.Lgs. 231/2001, l’ente può essere ritenuto responsabile soltanto per la commissione dei reati espressamente richiamati negli artt. da 23 a 25 *sexiesdecies* del D.Lgs. 231/2001 o da altri provvedimenti normativi (ad es. art. 10 L. 146/2006 in tema di “Reati transnazionali”), se commessi nel suo interesse o a suo vantaggio dai soggetti qualificati ex art. 5, comma 1, del Decreto stesso.

Le fattispecie di reato richiamate dal D.Lgs. 231/2001 possono essere comprese, per comodità espositiva, nelle seguenti categorie:

- delitti nei rapporti con la Pubblica Amministrazione (quali, ad esempio, corruzione, concussione,

peculato, abuso d'ufficio, malversazione ai danni dello Stato, truffa ai danni dello Stato, frode informatica ai danni dello Stato e induzione a dare o promettere utilità, richiamati dagli **artt. 24 e 25 del D.Lgs. 231/2001**)³;

- delitti informatici e trattamento illecito dei dati (quali ad esempio, accesso abusivo ad un sistema informatico o telematico, installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, danneggiamento di sistemi informatici o telematici richiamati all'art. 24 bis del D.Lgs. 231/2001)⁴;
- delitti di criminalità organizzata (art. 24 ter del D.Lgs. 231/2001)⁵;
- delitti contro la fede pubblica (art. 25 bis del D.Lgs. 231/2001)⁶;
- delitti contro l'industria ed il commercio (art. 25 bis.1 del D.Lgs. 231/2001)⁷;
- delitti in materia di sicurezza informatica e perimetro di sicurezza nazionale cibernetica (quali, ad esempio, violazioni delle misure di sicurezza, accesso abusivo a sistemi critici e compromissione dell'integrità dei dati, anche alla luce delle evoluzioni normative in materia di cybersecurity);
- • reati in materia di protezione dei dati personali (privacy), connessi al trattamento illecito di dati e alla violazione delle disposizioni del Regolamento UE 2016/679 (GDPR), laddove rilevanti anche ai fini dei reati informatici di cui all'art. 24-bis del D.Lgs. 231/2001;
- • delitti in materia di frode informatica e reati commessi mediante l'utilizzo di sistemi digitali, anche nell'ambito dello sviluppo, gestione e manutenzione di software e piattaforme tecnologiche;
- • delitti in materia di violazione del diritto d'autore connessi all'utilizzo, sviluppo o distribuzione di software, banche dati e contenuti digitali (art. 25-novies del D.Lgs. 231/2001);
- • delitti di riciclaggio, autoriciclaggio e impiego di denaro di provenienza illecita (art. 25-octies), con particolare riferimento alle transazioni digitali e ai flussi finanziari connessi a servizi informatici;
- • reati tributari (art. 25-quinquiesdecies), anche con riferimento alla gestione elettronica dei dati contabili e fiscali;
- • delitti connessi all'utilizzo improprio di tecnologie avanzate, incluse soluzioni basate su intelligenza artificiale, laddove possano determinare rischi rilevanti ai fini del D.Lgs. 231/2001.

- reati societari (quali ad esempio, false comunicazioni sociali, impedito controllo, illecita influenza sull'assemblea, corruzione tra privati, istigazione alla corruzione richiamati dall'**art. 25 ter D.Lgs. 231/2001**)⁸;
- delitti in materia di terrorismo e di eversione dell'ordine democratico (richiamati dall'**art. 25 quater del D.Lgs. 231/2001**);
- delitti contro la personalità individuale (**art. 25 quater.1** e **art. 25 quinquies del D.Lgs. 231/2001**)⁹;
- delitti di abuso di mercato (abuso di informazioni privilegiate e manipolazione del mercato, richiamati dall'**art. 25 sexies del D.Lgs. 231/2001**)¹⁰;
- reati transnazionali¹¹;
- delitti in materia di salute e sicurezza sui luoghi di lavoro (omicidio colposo e lesioni personali gravi colpose richiamati dall'**art. 25 septies del D.Lgs. 231/2001**)¹²;
- delitti di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio introdotto dalla L. n. 186/2014 (richiamati dall'**art. 25 octies del D.Lgs. 231/2001**)¹³;
- delitti in materia di violazione del diritto d'autore (**art. 25 nonies del D.Lgs. 231/2001**)¹⁴;
- delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (**art. 25 decies del D.Lgs. 231/2001**)¹⁵;
- reati ambientali (**art. 25 undecies del D.Lgs. 231/2001**)¹⁶;
- delitto di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, procurato ingresso illecito e favoreggiamento dell'immigrazione clandestina (**art. 25 duodecies del D.Lgs. 231/2001**)¹⁷;
- propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (**art. 25 terdecies del D.Lgs. 231/2001**)¹⁸;
- frode in competizioni sportive ed esercizio abusivo di gioco o di scommessa e giochi d'azzardo (**art. 25 quaterdecies del D.Lgs. 231/2001**)¹⁹;
- reati tributari (**art. 25 quinquiesdecies del D.Lgs. 231/2001**)²⁰;
- reati di contrabbando (**art. 25 sexiesdecies del D.Lgs. 231/2001**)²¹.

L'articolo 23 del D. Lgs. 231/2001 "Inosservanza delle sanzioni interdittive" prevede inoltre la punibilità dell'ente qualora, nello svolgimento dell'attività dello stesso ente a cui è stata applicata una sanzione o una misura cautelare interdittiva, siano trasgrediti gli obblighi o i divieti inerenti a tali sanzioni e misure.

1.3. APPARATO SANZIONATORIO

Gli **artt. 9 - 23 del D.Lgs. n. 231/2001** prevedono a carico dell'ente, in conseguenza della commissione o tentata commissione dei reati sopra richiamati, le seguenti sanzioni:

- sanzione pecuniaria (e sequestro conservativo in sede cautelare);
- sanzioni interdittive (applicabili anche quali misure cautelari) di durata non inferiore a tre mesi e non superiore a due anni (con la precisazione che, ai sensi dell'art. 14, comma 1, D.Lgs. n.231/2001, *“Le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente”*) che, a loro volta, possono consistere in:
 - Interdizione dall'esercizio dell'attività;
 - Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla Commissione dell'illecito;
 - Divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
 - Esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
 - Divieto di pubblicizzare beni o servizi;
 - Confisca (e sequestro preventivo in sede cautelare);
 - Pubblicazione della sentenza (in caso di applicazione di una sanzione interdittiva).

La sanzione pecuniaria viene determinata da parte del Giudice attraverso un sistema basato su “quote” in numero non inferiore a cento e non superiore a mille e di importo variabile fra un minimo di Euro 258,22 ad un massimo di Euro 1.549,37.

Nella commisurazione della sanzione pecuniaria il Giudice determina:

- il numero delle quote, in considerazione della gravità del fatto, del grado della responsabilità dell'ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti;
- l'importo della singola quota, in base alle condizioni economiche e patrimoniali dell'ente.

Le sanzioni interdittive si applicano in relazione ai soli illeciti amministrativi per i quali siano espressamente previste e purché ricorra almeno una delle seguenti condizioni:

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

Il Giudice determina il tipo e la durata della sanzione interdittiva tenendo in considerazione l'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso e, se necessario, può applicarle congiuntamente (art. 14, comma 1 e comma 3, D.Lgs. 231/2001).

Le sanzioni dell'interdizione dall'esercizio dell'attività, del divieto di contrattare con la Pubblica Amministrazione e di pubblicizzare beni o servizi possono essere applicate - nei casi più gravi – in via definitiva²².

Inoltre, ai sensi e alle condizioni di cui all'art. 15 del D.Lgs. 231/2001²³, è possibile la prosecuzione dell'attività dell'ente (in luogo dell'irrogazione della sanzione) da parte di un commissario nominato dal Giudice ai sensi e alle condizioni di cui all'art. 15 del D.Lgs. n.231/2001.

Nei casi in cui i delitti puniti ai sensi del D.Lgs. 231/2001 vengano commessi in forma tentata, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di durata) vengono ridotte da un terzo alla metà (artt. 12 e 26 D.Lgs. 231/2001).

Non insorge alcuna responsabilità in capo all'ente qualora lo stesso impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 D. Lgs. 231/2001). In tal caso, l'esclusione di sanzioni si giustifica in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e per suo conto.

1.4. REATI COMMESSI ALL'ESTERO

Ai sensi dell'art. 4 del D.Lgs. 231/2001, l'ente può essere chiamato a rispondere in Italia in relazione a reati contemplati dal Decreto - commessi all'estero²⁴.

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

I. il reato deve essere commesso da un soggetto funzionalmente legato all'ente, ai sensi dell'art. 5, comma 1, del D.Lgs. 231/2001;

II. l'ente deve avere la propria sede principale nel territorio dello Stato italiano;

III. l'ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p. (nei casi in cui la legge prevede che il colpevole - persona fisica - sia punito a richiesta del Ministro della Giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti dell'ente stesso) e, anche in ossequio al principio di legalità di cui all'art. 2 del D.Lgs. 231/2001, solo a fronte dei reati per i quali la sua responsabilità sia prevista da una disposizione legislativa *ad hoc*;

IV. sussistendo i casi e le condizioni di cui ai predetti articoli del codice penale, nei confronti dell'ente non proceda lo Stato del luogo in cui è stato commesso il fatto.

1.5. MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Elemento caratteristico dell'apparato normativo dettato dal D.Lgs. 231/2001 è l'attribuzione di un valore esimente al Modello di Organizzazione, Gestione e Controllo adottato dall'ente.

In caso di reato commesso da un soggetto in posizione apicale, infatti, la società non risponde se prova che (art. 6, comma 1, del D.Lgs. 231/2001):

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del reato, modelli di organizzazione e gestione idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un organismo della società dotato di autonomi poteri di iniziativa e di controllo;
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza.

Nel caso di reato commesso da soggetti apicali sussiste in capo all'ente una presunzione di responsabilità dovuta al fatto che tali soggetti esprimono e rappresentano la politica e, quindi, la volontà dell'ente stesso.

Per essere esente da responsabilità, l'ente dovrà, dunque, dimostrare la sua estraneità ai fatti contestati al soggetto apicale provando la sussistenza dei sopra elencati requisiti tra loro concorrenti e, di riflesso, la circostanza che la commissione del reato non deriva da una propria "colpa organizzativa".

Nel caso, invece, di un reato commesso da soggetti sottoposti alla direzione o vigilanza di un apicale, la società risponde se la commissione del reato è stata resa possibile dalla violazione degli obblighi di direzione o vigilanza alla cui osservanza la società è tenuta.

In tal caso, dunque, si assisterà ad un'inversione dell'onere della prova. L'accusa sarà, pertanto, tenuta a provare la mancata adozione ed efficace attuazione di un modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello verificatosi.

L'art. 7, comma 4, del D.Lgs. 231/2001 definisce, inoltre, i requisiti dell'efficace attuazione dei modelli organizzativi:

- la verifica periodica e l'eventuale modifica del modello quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione e nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

I Modelli di Organizzazione, Gestione e Controllo adottati ai sensi del D.Lgs. 231/2001, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, devono:

- individuare le attività nel cui ambito possono essere commessi reati (cfr. Parte Speciale del presente Modello);
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire (cfr. Parte Speciale del presente Modello);
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati (cfr. Parte Speciale del presente Modello, cap. 9.13);
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Con riferimento ai reati in materia di salute e sicurezza sul lavoro, l'art. 30 del D.Lgs. 81/08 (cd. Testo Unico Sicurezza) prevede che il Modello di Organizzazione e Gestione deve essere adottato attuando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

- al rispetto degli *standard* tecnico - strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- alle attività di sorveglianza sanitaria;
- alle attività di informazione e formazione dei lavoratori;
- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

1.6. LINEE GUIDA PER LA PREDISPOSIZIONE DEI MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

L'art. 6, comma 3, del D.Lgs. 231/2001 prevede che *“I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati”*.

Nella predisposizione del presente Modello, la Società si è ispirata alle Linee Guida di Confindustria emanate il 7 marzo 2002, parzialmente modificate il 31 marzo 2008 e da ultimo aggiornate nel giugno 2021, approvate da parte del Ministero della Giustizia.

In particolare, le Linee Guida elaborate da Confindustria suggeriscono di utilizzare, nella costruzione dei Modelli di Organizzazione, Gestione e Controllo, le attività di *risk assessment* e *risk management*, prevedono le seguenti fasi:

- Individuazione delle attività cd. sensibili, ossia quelle nel cui ambito possono essere commessi i reati, e dei relativi rischi;
- Analisi del sistema di controllo esistente prima dell'adozione/aggiornamento del Modello Organizzativo;
- Valutazione dei rischi residui, non coperti dai presidi di controllo precedenti;
- Previsione di specifici protocolli diretti a prevenire i reati, al fine di adeguare il sistema di controllo preventivo.

2. DESCRIZIONE DELL'ENTE

2.1. MAJOR BIT, ORGANIZZAZIONE E REALTÀ OPERATIVA

Il gruppo Major Bit (di seguito anche “Major Bit” o la “Società”) ha un'esperienza trentennale nel campo della consulenza e formazione ICT.

Major Bit opera con successo su settori di mercato quali AEROSPAZIO, DIFESA, PROGETTI DI RICERCA EU, PA e GRANDI AZIENDE PRIVATE, esprimendo un knowhow nello sviluppo Software, Business Intelligence, Cartografia/GIS su piattaforma ESRI e Open Source, Intelligenza Artificiale, Ingegnerizzazione di Procedure Operative. Nello Specifico opera principalmente nel settore dell'Information Technology, supportando le aziende/clienti (medie e grandi imprese) e la Pubblica Amministrazione Centrale nelle fasi di sviluppo ed innovazione tecnologica orientando tali realtà alla scelta delle soluzioni, dei processi, dei prodotti e delle metodologie applicabili, oltre ai servizi canonici di consulenza specifica ed alla realizzazione di applicativi personalizzati.

Major Bit ha per oggetto:

- SVILUPPO APPLICATIVO: Ricerca e sperimentazione di moderne tecnologie di sviluppo web/mobile
- BUSINESS INTELLIGENCE: Ingegnerizzazione dell'ambiente Datawarehouse e relativi flussi di caricamento, produzione Dashboard e Reportistica mediante le principali tecnologie di BI oggi presenti sul mercato.
- PROCEDURE ORGANIZZATIVE: il Tool proprietario CyberGuide supporta l'operatività introducendo linee guida procedurali codificate secondo le normative vigenti.
- FORNITURA HARDWARE: Fornitura di Hardware per infrastrutture IT, gestione dati, networking, cybersecurity.
- RICERCA E SVILUPPO: metodologie nel campo dell'INTELLIGENZA ARTIFICIALE applicata ai processi manutentivi ed operativi.

Alla data di adozione del presente Modello, la Società è gestita da un Amministratore unico investito dei più ampi poteri per la gestione ordinaria e straordinaria della stessa essendo in quest'ambito ad esso demandato di compiere tutti gli atti che ritenga opportuni per l'attuazione dell'oggetto sociale, esclusi quelli che per legge o per statuto sono inderogabilmente riservati all'Assemblea ordinaria dei Soci.

La modifica o l'aggiornamento dell'organigramma della Società non implicano necessariamente la revisione del Modello di Organizzazione, Gestione e Controllo (di seguito anche solo "Modello"), salvo che tali modifiche comportino significativi mutamenti delle regole previste dal presente Modello.

I principali strumenti di governance di cui la Società si è dotata, possono essere così riassunti:

- lo Statuto che, oltre a descrivere l'attività svolta, contempla diverse previsioni relative al governo della Società;
- un Sistema di Gestione della Qualità che disciplina, secondo modelli e principi predefiniti, le principali attività di Major Bit;
- il Codice Etico;
- l'individuazione della figura datoriale in materia di salute e sicurezza, oltre che la nomina di un RSPP;
- la documentazione aziendale relativa al sistema di gestione della salute e sicurezza sul lavoro, tra cui il Documento di Valutazione dei rischi adottato.

L'insieme degli strumenti di governance adottati (qui sopra richiamati in estrema sintesi) e delle previsioni del presente Modello consente di individuare, rispetto a tutte le attività, come siano formate e attuate le decisioni dell'ente (cfr. art. 6, comma 2 lett. b, D. Lgs. 231/01).

3. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO E METODOLOGIA SEGUITA PER L'ADOZIONE

3.1. PREMESSA

La decisione della Società di dotarsi di un Modello di Organizzazione Gestione e Controllo adottato ai sensi D.Lgs. 231/2001, rappresenta non solo il mezzo per minimizzare il rischio di commissione delle tipologie di reato contemplate dal Decreto, ma altresì un atto di responsabilità sociale nei confronti di tutti i portatori di interessi (personale, clienti, fornitori, partner *etc.*) oltre che della collettività.

In particolare, l'adozione e la diffusione di un Modello Organizzativo mirano, da un lato, a determinare una consapevolezza nel potenziale autore del reato di realizzare un illecito la cui commissione è fermamente condannata da parte della Società, dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire a Major Bit stessa di prevenire e reagire tempestivamente allo scopo di impedire la commissione del reato o la realizzazione dell'evento.

La Società ha, quindi, inteso avviare un'attività (di seguito, "Progetto") di adozione del Modello per la prevenzione dei reati al fine di conformarsi a quanto previsto dalle *best practices*, dalla dottrina e dalla giurisprudenza esistente in materia.

3.2. IL PROGETTO DI MAJOR BIT PER L'AGGIORNAMENTO DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

La metodologia scelta per l'aggiornamento del Modello della Società, in termini di organizzazione, definizione delle modalità operative e strutturazione in fasi, è stata elaborata al fine di rispettare quanto delineato dalle *best practices* esistenti in materia e, comunque, tenendo in considerazione quanto previsto dalle linee guida applicabili.

Il Progetto di adozione del Modello si è articolato nelle fasi di seguito riportate:

Fase 1 - Risk Assessment:

Identificazione dei *Key Officer* da intervistare, ossia dei soggetti che svolgono i ruoli chiave nell'ambito delle attività di Major Bit in base a funzioni e responsabilità; raccolta ed analisi della documentazione rilevante; realizzazione delle interviste con i *Key Officer* individuati; rilevazione delle attività sensibili e relativa valutazione in merito al potenziale rischio di commissione dei reati richiamati dal D.Lgs. 231/2001; condivisione con i soggetti intervistati delle risultanze della prima fase.

La valutazione del livello di esposizione al rischio di commissione di reati è stata effettuata secondo la tabella che segue, considerando congiuntamente:

- incidenza attività: valutazione della frequenza e/o della rilevanza economica dell'attività;
- rischio astratto di reato: valutazione circa la possibilità, in astratto, di condotte illecite nell'interesse o a vantaggio dell'ente.

Valutazione del rischio totale dell'attività			
Incidenza attività			
Bassa	Medio	Basso	Basso
Media	Medio	Medio	Basso
Alta	Alto	Alto	Medio
	Alto	Medio	Basso
	Rischio astratto reato		

La valutazione del livello di rischio residuo di commissione di reati è stata effettuata secondo la tabella che segue, considerando il rischio totale dell'attività calcolato secondo quanto sopra e il livello degli *standard* di controllo esistenti.

Valutazione del rischio residuo dell'attività			
Rischio			
Basso	Basso	Basso	Medio
Medio	Basso	Medio	Alto
Alto	Medio	Alto	Alto
	Alto	Medio	Basso
	Livello di compliance		

Il risk assessment deve essere oggetto di revisione periodica, e comunque ogniqualvolta intervengano modifiche rilevanti nell'organizzazione aziendale, nei processi operativi, nei servizi offerti o nel contesto normativo di riferimento, con particolare attenzione ai rischi connessi alla sicurezza informatica, alla gestione dei dati e all'utilizzo di tecnologie avanzate.

Fase 2 - Gap Analysis/Definizione dei protocolli di controllo:

Analisi delle attività sensibili rilevate e dell'ambiente di controllo con riferimento ad un Modello "a tendere", ossia conforme a quanto previsto dal D. Lgs. 231/2001;

- predisposizione della *Gap Analysis* (sintesi delle differenze tra protocolli di controllo esistenti e Modello a tendere);
- individuazione delle proposte di adeguamento e delle azioni di miglioramento; condivisione del documento all'Amministrazione

In particolare, il documento di *Gap Analysis* è finalizzato a rilevare gli *standard* di controllo che devono essere necessariamente rispettati per consentire alla Società di instaurare un'organizzazione volta ad evitare la commissione di reati.

Gli *standard* di controllo sono fondati sui seguenti principi generali che devono essere rispettati nell'ambito di ogni attività sensibile individuata:

- *Esistenza di procedure/linee guida formalizzate:*

esistenza di regole formali o prassi consolidate idonee a fornire principi di comportamento e modalità operative per lo svolgimento delle attività sensibili;

- *Tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informativi:*

verificabilità *ex post* del processo di decisione, autorizzazione e svolgimento dell'attività sensibile, anche tramite apposite evidenze archiviate;

- *Regolamentazione del processo e segregazione dei compiti:*

identificazione delle attività poste in essere dalle varie funzioni e ripartizione delle stesse tra chi esegue, chi autorizza e chi controlla, in modo tale che nessuno possa gestire in autonomia l'intero svolgimento di un processo. Tale segregazione è garantita dall'intervento all'interno di un processo sensibile di più soggetti allo scopo di garantire indipendenza ed obiettività delle attività;

- *Esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate:*

formalizzazione di poteri di firma e di rappresentanza coerenti con le responsabilità organizzative e gestionali assegnate e chiaramente definiti e conosciuti all'interno della Società.

Il documento di *Gap Analysis* include, altresì, un *Action Plan*, contenente le priorità per l'esecuzione degli interventi per l'adeguamento dei sistemi di controllo a fronte dei dati raccolti e dei *gap* rilevati.

Fase 3 - Definizione del Modello 231 e attività successive:

Il progetto di aggiornamento del Modello ha consentito di individuare i miglioramenti necessari per portare il livello di *compliance* a livello "alto" per ogni attività sensibile e, quindi, mitigare il rischio di commissione di reati. Tali miglioramenti sono stati effettuati dalla Società per allinearsi a quanto richiesto dalla normativa vigente. Predisposizione della bozza del Modello di Organizzazione, Gestione e Controllo; condivisione della bozza predisposta con l'Amministratore; approvazione del Modello Organizzativo da parte dell'Amministrazione. Le stesse fasi di progetto, in quanto applicabili, saranno poste in essere in occasione degli ulteriori aggiornamenti del Modello.

3.3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI MAJOR BIT

L'aggiornamento del Modello di Organizzazione, Gestione e Controllo da parte della Società ha comportato, dunque, un'attività di adeguamento dei protocolli preesistenti ai principi di controllo introdotti con il D.Lgs. 231/2001, al fine di limitare il rischio di commissione dei reati richiamati dal Decreto.

Come già accennato, unitamente al verificarsi delle altre circostanze previste dagli artt. 6 e 7, il D.Lgs. 231/2001 attribuisce un valore esimente all'adozione ed efficace attuazione di modelli di organizzazione, gestione e controllo nella misura in cui questi ultimi risultino idonei a prevenire, la commissione, o la tentata commissione, degli illeciti richiamati.

In particolare, ai sensi del co. 2 dell'art. 6 del D.Lgs. 231/2001, un modello di organizzazione e gestione deve rispondere alle seguenti esigenze:

- I. individuare le attività nel cui ambito possono essere commessi reati;
- II. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- III. individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- IV. prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;
- V. introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Alla luce delle considerazioni che precedono, Major Bit ha predisposto un Modello che tiene conto della propria peculiare realtà, in coerenza con il proprio sistema di *governance* ed in grado di valorizzare i controlli e gli organismi esistenti.

Tale Modello, dunque, rappresenta un insieme coerente di principi, procedure e disposizioni che:

- 1- incidono sul funzionamento interno della Società e sulle modalità con le quali la stessa si rapporta con l'esterno
- 2- regolano la diligente gestione di un sistema di controllo delle attività sensibili, finalizzato a prevenire la commissione, o la tentata commissione, dei reati richiamati dal D.Lgs. 231/2001.

Il Modello - così come approvato dalla Società - comprende i seguenti elementi costitutivi:

- nella parte generale, una descrizione relativa:
- al quadro normativo di riferimento;

- alla realtà e al sistema di *governance* di Major Bit;
- alla metodologia adottata per le attività di *risk assessment*, *gap analysis* e *action plan*;
- alla individuazione e nomina dell'Organismo di Vigilanza della Società, con specificazione di poteri e compiti che lo riguardano;
- alla funzione del sistema disciplinare e al relativo apparato sanzionatorio;
- al piano di formazione e informazione da adottare al fine di garantire la conoscenza delle misure e delle disposizioni contenute nel Modello;
- ai criteri di aggiornamento e adeguamento del Modello;
- nella parte speciale, una descrizione relativa ai processi/attività sensibili e relativi *standard* di controllo.

3.4 INDIVIDUAZIONE DELLE ATTIVITÀ SENSIBILI

A seguito dell'attività di *risk assessment* svolta, sono state individuate le attività sensibili indicate nella parte speciale del presente Modello.

Sulla base delle suddette attività sensibili - secondo differenti gradazioni di rischio – si sono ritenuti esistenti profili di rischio di commissione dei reati previsti dagli artt. 24, 24 *bis*, 24 *ter*, 25, 25 *bis*.1; 25 *ter*, 25 *quater*; 25 *quinquies*, 25 *septies*, 25 *octies*, 25 *novies*, 25 *decies*, 25 *undecies*, 25 *duodecies*, 25 *quaterdecies* e 25 *quinquiesdecies* del D.Lgs. 231/2001 (reati commessi nei rapporti con la Pubblica Amministrazione, reati informatici, delitti di criminalità organizzata, delitti contro l'industria e commercio, reati societari e corruzione tra privati, reati di terrorismo, delitti contro la personalità individuale, reati commessi in violazione delle norme a tutela della salute e sicurezza sul lavoro, reati di ricettazione, riciclaggio, reimpiego di denaro, beni o utilità di provenienza illecita e auto riciclaggio, delitti in violazione del diritto d'autore, induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria, reati ambientali e impiego di cittadini di paesi terzi il cui soggiorno è irregolare, frode in competizioni sportive).

Il rischio di commissione del reato di violazione delle norme in materia di perimetro di sicurezza nazionale cibernetica, inserito all'interno art. 24 *bis* D.Lgs. 231/2001 dal D.L. 105/2019, è stato considerato non applicabile in quanto la Società, ad oggi, non risulta ricompresa tra i soggetti obbligati al rispetto delle prescrizioni indicate dal suddetto Decreto.

Con riferimento alla fattispecie di "esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati" prevista dall'art. 25-*quaterdecies* D.Lgs. 231/2001 è stato rilevato che tale reato non è applicabile all'attività svolta dalla Società.

Per quanto concerne, invece, i reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, la mutilazione degli organi genitali femminili, i reati transnazionali, i delitti di razzismo e xenofobia e i reati contrabbando – vista l'attività svolta dalla Società – è stata ritenuta remota la possibilità di realizzazione degli stessi.

Tra le attività sensibili devono essere incluse, ove rilevanti:
 la gestione delle infrastrutture IT e dei sistemi informativi;
 la gestione dei dati personali e delle informazioni riservate;

l'utilizzo e lo sviluppo di sistemi basati su intelligenza artificiale;
la gestione della sicurezza informatica e dei rischi cyber.

3.5 DESTINATARI

Le disposizioni del presente Modello sono rivolte agli Amministratori, al Direttore Generale e a tutti coloro che rivestono all'interno della Società funzioni di rappresentanza, amministrazione e direzione (c.d. soggetti apicali), ai dipendenti (per tali intendendosi tutti coloro che sono legati alla Società da un rapporto di lavoro subordinato, incluso il personale dirigente); inoltre, ove applicabili, le regole e i principi di comportamento contenuti nel Modello devono essere rispettati anche da fornitori, consulenti e clienti nell'ambito dei rapporti intercorrenti con la Società (di seguito anche i "**Destinatari**").

3.6. IL CODICE ETICO

I principi e le regole contenuti nel presente Modello tengono conto anche di quelli previsti dal Codice Etico (di seguito anche il “**Codice**”) adottato dalla Società.

In termini generali, il Codice è un documento ufficiale di Major Bit, indirizzato a tutto il personale, ai consulenti, ai collaboratori, ai fornitori e ai terzi in genere, che esprime gli orientamenti dell’Ente e che richiede loro comportamenti improntati alla legalità, onestà, integrità morale, trasparenza e correttezza, obiettività e rispetto della personalità individuale prevedendo l’insieme dei principi di condotta rilevanti ai fini del buon funzionamento, dell’affidabilità, del rispetto di leggi e regolamenti nonché dell’immagine di Major Bit.

Il Codice è reso noto a tutti i destinatari e Major Bit ne richiede l’osservanza da parte di tutti i soggetti che operano per il conseguimento degli obiettivi aziendali.

Il Codice Etico, fra l’altro, richiama principi di comportamento che consentono di prevenire i reati di cui al D.Lgs. 231/2001, anche se non direttamente inseriti all’interno del Modello.

Il Codice deve, quindi, essere considerato come parte integrante del presente Modello e strumento fondamentale per il conseguimento degli obiettivi di quest’ultimo.

4. L'ORGANISMO DI VIGILANZA

4.1. PREMESSA

Come sopra anticipato - in ottemperanza all’art. 6, comma 1, lett. a) e b) del D.Lgs. 231/2001 l’ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti qualificati ex art. 5 del D.Lgs. 231/2001, se l’organo dirigente ha, fra l’altro:

- adottato ed efficacemente attuato Modelli di Organizzazione, Gestione e Controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e l’osservanza del Modello e di curarne l’aggiornamento ad un organismo dell’ente dotato di autonomi poteri di iniziativa e controllo.

L’affidamento dei suddetti compiti ad un Organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi rappresentano, quindi, presupposti indispensabili per l’esonero dalla responsabilità prevista dal D.Lgs. 231/2001.

I requisiti principali dell’Organismo di Vigilanza (di seguito anche solo “**OdV**”), così come proposti dalle Linee Guida per la predisposizione dei Modelli di Organizzazione e Gestione emanate da Confindustria, possono essere così identificati:

- **Autonomia ed Indipendenza:** l'Organismo di Vigilanza si inserisce "come unità di staff in massima posizione gerarchica con riporto diretto al massimo vertice dell'ente" ed è privo di poteri decisionali ed operativi in merito all'attività aziendale;
- **Professionalità:** l'OdV deve possedere specifiche competenze in ambito giuridico, economico, nell'ambito delle tecniche di analisi e di valutazione dei rischi;
- **Continuità di azione:** la continuità di azione ha la finalità di garantire il costante controllo dell'efficace, effettiva e costante attuazione del Modello Organizzativo adottato dalla Società ai sensi D.Lgs. 231/2001. Il D.Lgs. 231/2001 non fornisce indicazioni specifiche circa la composizione dell'Organismo di Vigilanza. La Società si è dotata di un Organismo collegiale che non riporta gerarchicamente ad alcuna funzione della Società ed è collocato in posizione di *staff* rispetto all'Amministrazione

4.2. REQUISITI SOGGETTIVI DEI COMPONENTI

Ogni componente dell'Organismo di Vigilanza possiede i requisiti di onorabilità²⁵, assenza di conflitto d'interessi, assenza di relazioni di parentela e/o di affari *etc.*

4.3. ISTITUZIONE, NOMINA E REVOCA DELL'ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza è composto da quattro membri nominati dall'organo amministrativo della Società. L'OdV resta in carica per 3 (tre) anni ed è rinnovabile alla scadenza. E' necessario che l'Organismo di Vigilanza possieda, oltre a competenze professionali adeguate, requisiti soggettivi che garantiscano l'autonomia, l'indipendenza e l'onorabilità richiesta dal compito e dovranno, altresì, godere dei requisiti di moralità cui all'art. 80 del D.lgs. n. 50/2016. In particolare, non possono essere nominati:

- coloro che versino in una delle cause di ineleggibilità o di decadenza previste dall'art. 2382 Codice Civile per gli amministratori;
- coloro che siano imputati per uno dei reati di cui al Decreto Legislativo n.231/2001;
- coloro che siano stati condannati alla reclusione a seguito di processo penale avente ad oggetto la commissione di un delitto;
- il coniuge, i parenti e gli affini entro il quarto grado dei consiglieri della società, i consiglieri, il coniuge, i parenti e gli affini entro il quarto grado dei membri degli organi associativi.

Qualora venisse a mancare l'Organismo di Vigilanza, l'Amministratore provvede alla sostituzione e contestualmente dispone il relativo aggiornamento del Modello.

La revoca dell'Organismo di Vigilanza può avvenire per i sotto elencati motivi:

- venir meno dei requisiti di cui sopra;
- gravi e accertati motivi di incompatibilità che ne vanifichino indipendenza e autonomia;
- grave negligenza nell'espletamento dei compiti connessi all'incarico;
- violazione degli obblighi di riservatezza previsti a carico dell'Organismo di Vigilanza;
- mancata o insufficiente attività di controllo.

La revoca dell'Organismo di Vigilanza compete all'Amministratore e provvede alla sua sostituzione.

4.4. FUNZIONI E POTERI

Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura della Società, posto però che l'organo amministrativo è in ogni caso chiamato a vigilare sull'adeguatezza del suo operato, in quanto lo stesso ha la responsabilità ultima del funzionamento e dell'efficacia del Modello.

Per lo svolgimento delle proprie attività, l'Organismo di Vigilanza adotta un regolamento di funzionamento interno in cui definisce le proprie modalità operative.

L'OdV ha poteri di iniziativa e controllo necessari per assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello secondo quanto stabilito dall'art. 6 del D.Lgs. 231/2001.

In particolare, l'Organismo di Vigilanza verifica:

- il funzionamento del Modello e l'osservanza delle prescrizioni in questo contenute da parte di tutti i destinatari;
- la reale efficacia e capacità del Modello della Società di prevenire la commissione di reati richiamati dal D.Lgs. 231/2001;
- l'opportunità di aggiornare il Modello, laddove vengano riscontrate esigenze di adeguamento dello stesso in relazione a mutate condizioni dell'Ente o a novità normative.

A tale fine, l'Organismo di Vigilanza può disporre di atti ispettivi e di controllo, di accesso ad atti di Major Bit, riservati e non, ad informazione o dati, a procedure, dati contabili o ad ogni altro dato, atto o informazione ritenuti utili. Per garantire una vigilanza quanto più efficace possibile sul funzionamento e il rispetto del Modello, rientrano fra i compiti dell'OdV, a titolo meramente esemplificativo e non tassativo:

- attivare un piano di verifica volto ad accertare la concreta attuazione del Modello Organizzativo da parte di tutti i destinatari;
- monitorare la necessità di un aggiornamento della mappatura dei rischi e del Modello, in caso di significative variazioni organizzative o di estensione della tipologia di reati presi in considerazione dal D.Lgs. 231/2001, informandone l'Amministratore;
- eseguire periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle aree di rischio;
- monitorare, in collaborazione con l'Amministratore, le iniziative di informazione/formazione finalizzate alla diffusione della conoscenza e della comprensione del Modello nell'Ente;
- accogliere, elaborare e conservare le informazioni rilevanti (comprese le eventuali segnalazioni) in ordine al rispetto del Modello;
- coordinarsi con le funzioni dell'Ente per un migliore monitoraggio delle aree a rischio;
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del Modello;
- segnalare prontamente ogni criticità relativa all'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto, proponendo le opportune soluzioni operative;
- segnalare all'Amministratore eventuali violazioni di regole contenute nel Modello o le carenze rilevate in occasione delle verifiche svolte, affinché questi possa adottare i necessari interventi di adeguamento;

- vigilare sull'applicazione coerente delle sanzioni previste dalle normative interne nei casi di violazione del Modello, ferma restando la competenza dell'organo deputato per l'applicazione dei provvedimenti sanzionatori;
- rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni.

4.5. REGOLE DI CONDOTTA

L'attività dell'OdV deve essere improntata ai principi di integrità, obiettività, riservatezza.

Tali regole di condotta possono esplicitarsi nei termini che seguono:

- integrità: l'OdV deve operare con onestà, diligenza e senso di responsabilità, nonché rispettare e favorire il conseguimento degli obiettivi della Società;
- obiettività: l'OdV non deve partecipare ad alcuna attività che possa pregiudicare l'imparzialità della propria valutazione. Deve riportare tutti i fatti significativi di cui sia venuto a conoscenza e la cui omissione possa dare un quadro alterato e/o incompleto delle attività analizzate;
- riservatezza: i componenti dell'OdV devono esercitare tutte le opportune cautele nell'uso e nella protezione delle informazioni acquisite. Non deve usare le informazioni ottenute né per vantaggio personale né secondo modalità che siano contrarie alla legge o che possano arrecare danno agli obiettivi della Società. Tutti i dati di cui sia titolare Major Bit devono essere trattati nel pieno rispetto delle disposizioni di cui al d.lgs. n. 196/2003 e s.m.i.

La divulgazione di tali informazioni potrà essere effettuata solo ai soggetti e con le modalità previste dal presente Modello.

4.6. SEGNALAZIONI ALL'ODV

L'Organismo di Vigilanza deve essere tempestivamente informato, mediante apposito sistema di comunicazione interna, in merito a condotte illecite, fondate su elementi di fatto precisi e concordanti, che possano determinare una violazione del Modello o che, più in generale, siano rilevanti ai fini del D.Lgs. 231/2001 o in merito a violazioni del modello di organizzazione e gestione dell'ente.

Le segnalazioni possono avvenire per iscritto, anche in forma anonima, attraverso appositi canali di informazione riservata con le seguenti modalità:

- e-mail: ***segnalazioni@majorbit.com***
- lettera raccomandata indirizzata a: **Major Bit, Viale Luigi Schiavonetti 278, 00173 Roma (RM)**

In particolare, devono essere segnalati senza ritardo:

- le notizie relative alla commissione, o alla ragionevole convinzione di commissione, degli illeciti ai quali è applicabile il D.Lgs. 231/2001, compreso l'avvio di procedimento giudiziario a carico di personale della Società per reati previsti nel D.Lgs. 231/2001;
- le violazioni delle regole di comportamento o procedurali contenute nel presente Modello e tutti i comportamenti che possano determinare una violazione del Modello.

L'Organismo di Vigilanza valuta le segnalazioni ricevute e propone all'Amministratore i provvedimenti conseguenti, 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.

I segnalanti in buona fede sono garantiti contro qualsiasi forma di ritorsione, discriminazione, diretta o indiretta, o penalizzazione per motivi collegati, direttamente o indirettamente, alla segnalazione così come previsto dall'art. 6 del D.Lgs. 231/2001.

È assicurata la riservatezza della identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate in mala fede.

Oltre alle segnalazioni relative alle violazioni sopra descritte, devono essere obbligatoriamente ed immediatamente trasmesse all'OdV le informazioni concernenti:

- eventuali modifiche all'assetto interno o alla struttura organizzativa della Società o alla variazione delle aree di attività;
- le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- 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 ai quali è applicabile il D.Lgs. 231/2001, qualora tali indagini coinvolgano la Società o il suo personale od organi dell'ente;
- i procedimenti relativi all'applicazione di misure di prevenzione previste dalla legge vigente e i procedimenti da parte dell'Autorità Nazionale Anticorruzione;
- gli esiti delle attività di controllo periodico (rapporti, monitoraggi, consuntivi, etc.);
- le richieste di assistenza legale inoltrate dall'amministratore, dal personale in caso di avvio di procedimento giudiziario nei loro confronti ed in relazione ai reati di cui al D.Lgs. 231/2001 o alla normativa in materia di salute e sicurezza sul lavoro o ambientale;
- le notizie relative alla effettiva attuazione del Modello Organizzativo, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- reportistica periodica in materia di salute e sicurezza sui luoghi di lavoro e sulle tematiche ambientali;
- i procedimenti disciplinari promossi e la relativa definizione.

L'Organismo di Vigilanza definisce la tempistica di trasmissione con apposita comunicazione ai responsabili delle attività sensibili individuate.

L'Organismo di Vigilanza verifica periodicamente anche l'adeguatezza delle misure adottate dalla Società in materia di sicurezza informatica, protezione dei dati e gestione dei rischi tecnologici emergenti.

4.7. RACCOLTA E CONSERVAZIONE DELLE INFORMAZIONI

Ogni informazione in possesso dell'OdV è trattata in conformità al D.Lgs. 30 giugno 2003, n.196, come modificato dal D.Lgs. 10 settembre 2018 n. 101, e al Regolamento Europeo n.2016/679 (General Data Protection Regulation, in breve "GDPR").

A tal proposito, in forza del parere espresso dall'Autorità Garante per la Protezione dei Dati Personali in data 12 maggio 2020 circa la qualificazione soggettiva ai fini privacy dei componenti dell'Organismo di Vigilanza, in ragione del trattamento dei dati personali che l'esercizio dei compiti e delle funzioni affidate all'OdV comporta nell'ambito delle misure organizzative da porre in essere in attuazione del principio di accountability, in qualità

del Titolare del Trattamento (art. 24 del GDPR) designa ogni componente dell'OdV quale soggetto autorizzato al trattamento dei dati personali (artt. 29 GDPR ed art. 2 *quaterdecies* D.Lgs.196/2003).

Tutte le informazioni, la documentazione, ivi compresa la reportistica prevista dal Modello, e le segnalazioni raccolte dall'Organismo di Vigilanza – e allo stesso pervenute - nell'espletamento dei propri compiti istituzionali, vengono custodite a cura dell'OdV in un apposito archivio e conservate, in ottemperanza ai principi di cui all'art. 5 del GDPR, per il tempo necessario rispetto agli scopi per i quali è stato effettuato il trattamento e comunque per un periodo non superiore a dieci anni.

L'Organismo di Vigilanza provvede affinché il passaggio della gestione dell'archivio avvenga correttamente nel caso di nomina di un nuovo OdV.

4.8. REPORTING DELL'ORGANISMO DI VIGILANZA VERSO GLI ORGANI DELLA SOCIETÀ

L'Organismo di Vigilanza riferisce in merito all'efficacia e osservanza del Modello, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi. A tal fine, l'Organismo di Vigilanza predispone:

- con cadenza annuale, una relazione informativa, relativa all'attività svolta, da presentare all'Amministratore, al Collegio Sindacale e al Revisore della Società;
- immediatamente, al verificarsi di violazioni accertate del Modello, con presunta commissione di reati, una comunicazione da presentare all'Amministratore, informandone anche il Collegio Sindacale ed il Revisore della Società.

Nell'ambito del *reporting* annuale vengono affrontati i seguenti aspetti:

- controlli e verifiche svolti dall'Organismo di Vigilanza ed esito degli stessi;
- stato di avanzamento di eventuali progetti di implementazione/revisione di processi sensibili;
- eventuali innovazioni legislative o modifiche organizzative che richiedono aggiornamenti;
- eventuali sanzioni disciplinari irrogate dagli organi competenti a seguito di violazioni del Modello;
- altre informazioni ritenute significative;
- valutazione di sintesi sull'adeguatezza del Modello rispetto alle previsioni del D.Lgs.231/2001.

Gli incontri con gli organi della Società cui l'Organismo di Vigilanza riferisce sono documentati. L'OdV cura l'archiviazione della relativa documentazione.

5. SEGNALAZIONI DI REATI O IRREGOLARITÀ NELL'AMBITO DEL RAPPORTO DI LAVORO (C.D. WHISTLEBLOWING)

La legge n. 179/2017 ha introdotto l'obbligo per tutte le Società di aggiornare ed implementare il Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D.lgs. 231/01, istituendo e regolando un sistema che consenta ai propri lavoratori la possibilità di segnalare eventuali attività illecite di cui gli stessi siano venuti a conoscenza per ragioni di lavoro (c.d. *whistleblowing*).

In particolare, la sopra citata Legge è intervenuta inserendo all'art.6 del D.lgs. 231/2001 il comma 2 bis a norma del quale il Modello Organizzativo deve prevedere:

- a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1 lettere *a* e *b*, di presentare, a tutela dell'integrità dell'Ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'Ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione e segnalazione;
- b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- d) nel sistema disciplinare adottato ai sensi del comma 2 lettera e, sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Tale norma, che mira ad incentivare la collaborazione dei lavoratori nella rilevazione di possibili frodi, pericoli o altri seri rischi che possano danneggiare clienti, colleghi o la stessa reputazione ed integrità dell'impresa, introducendo specifiche tutele a favore del segnalante, interviene su un duplice piano:

I- imponendo a enti e imprese di creare una procedura organizzativa che consenta a chi ritenga di dover segnalare o denunciare un illecito di agire senza mettere a repentaglio la propria posizione sul piano personale e lavorativo per effetto della segnalazione stessa

II- prevedendo un sistema di garanzie sostanziali e processuali volte a impedire che dalla segnalazione o denuncia possano derivare forme di ritorsione da parte del datore di lavoro.

Destinatario designato alle segnalazioni sopra citate è l'Organismo di Vigilanza, nella persona del Presidente, in considerazione del fatto che è un professionista esterno.

I canali interni adibiti alla trasmissione di tali comunicazioni sono:

- a) *e-mail* alla casella di posta elettronica ***segnalazioni@majorbit.com***, il cui accesso è consentito esclusivamente al Presidente dell'Organismo di Vigilanza;
- b) lettera cartacea inviata mediante posta ordinaria o raccomandata al *Presidente dell'Organismo di Vigilanza*, all'indirizzo **Major Bit, Viale Luigi Schiavonetti 278, 00173 Roma (RM)**.

In ottemperanza al D.Lgs 24/2023 attuativo della *Direttiva (UE) 2019/1937* del Parlamento Europeo e del Consiglio, del 23 ottobre 2019 e in riferimento all'articolo 4 comma 3 del Decreto Legislativo, la segnalazione interna potrebbe avvenire anche in forma orale, le quali *“sono effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole”*.

Inoltre, con riferimento all'articolo 5 comma 1 del D.Lgs 24/2023, nell'ambito della gestione del canale di segnalazione interna, il gestore del canale nella persona del Presidente dell'Organismo di Vigilanza si impegna a svolgere le seguenti attività:

- a) rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
- b) mantiene le interlocuzioni con la persona segnalante e può richiedere a quest'ultima, se necessario, integrazioni;
- c) dà diligente seguito alle segnalazioni ricevute;
- d) fornisce riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione;
- e) mette a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne; in riferimento all'articolo 5 comma 1 lettera e del D.Lgs 24/2023 *“le suddette informazioni sono esposte e rese facilmente visibili nei luoghi di lavoro, nonché accessibili alle persone che pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico in una delle forme di cui all'articolo 3, commi 3 o 4. Se dotati di un proprio sito internet, i soggetti del settore pubblico e del settore privato pubblicano le informazioni di cui alla presente lettera anche in una sezione dedicata del suddetto sito”*.

La segnalazione viene ricevuta dal Presidente dell'Organismo di Vigilanza (di seguito inteso “destinatario della segnalazione”) che, svolta una valutazione iniziale, informa gli altri componenti dell'Organismo.

L'Organismo di Vigilanza agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione, penalizzazione o qualsivoglia conseguenza derivante dalle stesse, assicurando loro la riservatezza circa l'identità, fatti comunque salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

In particolare, in ottemperanza al D.Lgs 24/2023 attuativo della *Direttiva (UE) 2019/1937* del Parlamento europeo e del Consiglio, del 23 ottobre 2019 e in riferimento all'articolo 4 comma 1 del Decreto Legislativo citato, l'organizzazione si impegna ad attivare *“propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione”*.

Gli obblighi di riservatezza non possono essere opposti quando le informazioni richieste sono necessarie per le indagini o i procedimenti avviati dall'autorità giudiziaria in seguito alla segnalazione.

Si rammenta che i prestatori di lavoro hanno comunque il dovere di diligenza e l'obbligo di fedeltà al datore di lavoro ai sensi degli artt. 2104 e 2105 del Codice Civile e, pertanto, il corretto adempimento all'obbligo d'informazione da parte del prestatore di lavoro non potrà di per sé dar luogo all'applicazione di sanzioni disciplinari.

È espressamente prevista la nullità di qualsiasi misura ritorsiva nei confronti del segnalante, attuata, ad esempio, con provvedimenti di licenziamento ritorsivi o discriminatori, ovvero con mutamenti di mansione.

Le segnalazioni fornite all'OdV non impongono allo stesso una verifica sistematica e puntuale di tutti i fenomeni rappresentati.

È, quindi, rimesso alla responsabilità dell'OdV stabilire in quali casi e come attivarsi in base alla rilevanza delle segnalazioni stesse.

A tal fine, è comunque necessario che le segnalazioni siano fondate su elementi di fatto precisi e concordanti, proprio per permettere al destinatario delle stesse di valutarne la rilevanza.

La Società ha adottato apposita procedura in tema di c.d. *whistleblowing*, sulla base della quale gestisce e analizza le segnalazioni ricevute tramite le modalità sopra descritte ed effettua le conseguenti indagini interne al fine di verificarne la fondatezza e di comunicare l'esito delle stesse al segnalante.

6. IL SISTEMA DISCIPLINARE

6.1. PREMESSA

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

Tale sistema disciplinare deve rivolgersi tanto al personale quanto ai terzi che operino per conto della Società, prevedendo idonee sanzioni di carattere disciplinare in un caso e di carattere contrattuale/negoziale (ad es. risoluzione del contratto, cancellazione dall'elenco fornitori *etc.*) nell'altro caso.

Con particolare riguardo ai lavoratori dipendenti, il sistema disciplinare deve rispettare i limiti connessi al potere sanzionatorio imposti dall'art. 7 della Legge n. 300 del 1970 (c.d. "Statuto dei lavoratori") e dal Contratto Collettivo Nazionale di Lavoro per i dipendenti delle industrie metalmeccaniche private e della installazione di impianti, sia per quanto riguarda le sanzioni irrogabili sia per quanto riguarda le forme di esercizio del potere sanzionatorio.

In ogni caso, l'applicazione delle sanzioni disciplinari prescinde dall'avvio o dall'esito di un eventuale procedimento penale, in quanto i modelli di organizzazione e le procedure interne costituiscono regole vincolanti per i Destinatari, la violazione delle quali deve, al fine di ottemperare ai dettami del citato Decreto Legislativo, essere sanzionata indipendentemente dall'effettiva realizzazione di un reato o dalla punibilità dello stesso.

Al fine di promuovere l'efficacia dei canali di segnalazione di cui al par.5 la Società pone il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi che siano collegati, direttamente o indirettamente, alla segnalazione stessa e prevede sanzioni nei confronti di chi viola le misure di tutela del segnalante.

La Società inoltre intende favorire un clima di collaborazione trasparente e costruttivo ed evitare strumentalizzazioni delle segnalazioni che ne minerebbero la credibilità: a questo fine sono previste sanzioni disciplinari per chi effettuasse con dolo o colpa grave segnalazioni che si rivelano infondate.

È affidato all'OdV il compito di monitorare l'osservanza e la corretta applicazione del Sistema Disciplinare in caso di violazioni rilevanti ai fini del Decreto, nonché di informare l'Amministrazione affinché curi l'aggiornamento, la modifica e/o l'integrazione del Sistema Disciplinare stesso, qualora lo ritenesse necessario ai fini della migliore efficacia del Modello.

Il sistema disciplinare di seguito delineato si applica anche nei confronti di coloro che violino le misure di tutela adottate nei confronti dei lavoratori che abbiano effettuato segnalazioni, nonché nei confronti di coloro che effettuino con dolo o colpa grave segnalazioni che si rivelino totalmente infondate.

6.2. MISURE NEI CONFRONTI DI LAVORATORI DIPENDENTI NON DIRIGENTI

Con riguardo ai lavoratori dipendenti non dirigenti, il sistema disciplinare applicato da Major Bit è regolato dal Contratto Collettivo Nazionale di Lavoro per i dipendenti delle industrie metalmeccaniche private e della installazione di impianti.

La violazione delle singole disposizioni e regole comportamentali di cui al Modello e al Codice Etico da parte dei dipendenti costituisce illecito disciplinare.

In particolare, le infrazioni delle disposizioni contenute nel Modello Organizzativo e del Codice Etico potranno essere punite – a seconda della gravità della violazione e tenuto conto dell'eventuale recidiva – con:

- richiamo verbale;
- ammonizione scritta;
- multa in misura non superiore a tre ore di retribuzione oraria calcolata sul minimo tabellare;
- sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni;
- licenziamento.

Nell'ottica del Modello:

1. incorre nel provvedimento del **richiamo verbale** il lavoratore che commetta lievi violazioni, anche con condotte omissive, che non abbiano rilevanza esterna, delle disposizioni contenute nel Modello o nel Codice Etico, ovvero non comunichi all'OdV le informazioni previste dal Modello;

2. incorre nel provvedimento dell'**ammonizione scritta** il lavoratore che commetta violazioni, anche con condotte omissive, delle disposizioni contenute nel Modello o nel Codice Etico, ovvero non comunichi all'OdV le informazioni previste dal Modello nonché il lavoratore che violi in modo reiterato le disposizioni indicate al punto 1;

3. incorre nel provvedimento della **multa in misura non superiore a tre ore di retribuzione oraria calcolata sul minimo tabellare** chi:

- a)** violi più volte i principi e i protocolli previsti dal presente Modello o nel Codice Etico
- b)** adottati, nell'espletamento di attività a rischio, un comportamento reiteratamente non conforme alle prescrizioni del Modello stesso, ove in tali comportamenti sia ravvisabile un rifiuto di eseguire ordini concernenti obblighi derivanti dal Modello
- c)** violi in modo reiterato le disposizioni indicate al punto 2;

4. incorre nel provvedimento della **sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni** il lavoratore che:

- a)** violi colposamente le prescrizioni del Modello o del Codice Etico, arrecando un danno alla Società o esponendola a una situazione di pericolo in ordine alle sanzioni previste nel D.Lgs. 231/2001
- b)** violi l'obbligo di comunicare all'OdV la commissione di uno o più reati previsti dal Decreto di cui sia in

qualsiasi modo a conoscenza

c) violi in modo reiterato le disposizioni indicate al punto 3;

5. incorre nel provvedimento del **licenziamento** il lavoratore che:

a) eluda fraudolentemente il Modello, determinando la concreta applicazione a carico della Società di sanzioni previste dal Decreto

b) ponga in essere un comportamento inequivocabilmente diretto alla commissione di un reato previsto dal D.Lgs. 231/2001

c) violi in modo reiterato le disposizioni indicate al punto 4 o d) effettui con dolo o colpa grave segnalazioni di violazioni del Modello e di commissione dei reati previsti dal D.Lgs. 231/2001 che si rivelino infondate e di chi compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di chi abbia effettuato segnalazioni di violazioni del Modello e di commissione dei reati previsti dal D.Lgs. 231/2001.

Al fine di ottemperare alle previsioni del D.Lgs. 231/2001 con riguardo all'adozione di un sistema disciplinare idoneo a sanzionare il mancato rispetto da parte dei dipendenti non dirigenti delle misure previste nei modelli di organizzazione, gestione e controllo, la Società si avvale quindi del sistema disciplinare sopra brevemente descritto.

Inoltre, il mancato rispetto e/o la violazione delle regole di comportamento imposte dal Modello Organizzativo, dal Codice Etico e dalle prassi esistenti in Major Bit, ad opera dei dipendenti, costituisce inadempimento alle obbligazioni derivanti dal rapporto di lavoro e illecito disciplinare (art. 2106 c.c.) e, in quanto tali, possono comportare la comminazione delle sanzioni previste dalla normativa vigente e dal CCNL applicabile.

Conformemente all'art. 7 della legge 20 maggio 1970, n. 300, e alle previsioni del Contratto Collettivo Nazionale di Lavoro, le disposizioni in materia di sanzioni disciplinari devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti.

L'accertamento delle suddette infrazioni, eventualmente su segnalazione dell'Organismo di Vigilanza, la gestione dei procedimenti disciplinari e l'irrogazione delle sanzioni restano di competenza dell'Amministratore.

6.3. MISURE NEI CONFRONTI DEI DIRIGENTI

Con riguardo ai dirigenti, in assenza di un sistema disciplinare applicabile agli stessi ed in considerazione del particolare rapporto fiduciario con il Datore di Lavoro, in caso di violazione dei principi generali del Modello adottato e delle regole di comportamento imposte dal Codice Etico, l'Amministratore assume nei confronti dei responsabili i provvedimenti ritenuti idonei in funzione delle violazioni commesse quali la revoca di deleghe e procure e, fino al licenziamento, tenuto conto che le stesse costituiscono inadempimento alle obbligazioni derivanti dal rapporto di lavoro.

È passibile di licenziamento il dirigente che compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di chi abbia effettuato segnalazioni di violazioni del Modello o di commissione dei reati previsti dal D.Lgs. 231/2001 per motivi che siano collegati, direttamente o indirettamente, alla segnalazione stessa.

Analoga sanzione è prevista per il dirigente che effettui con dolo o colpa grave segnalazioni di violazioni del Modello o di commissione dei reati previsti dal D.Lgs. 231/2001 che si rivelano infondate.

6.4. MISURE NEI CONFRONTI DEGLI AMMINISTRATORI

La Società valuta con particolare rigore le infrazioni a quanto previsto dal Modello poste in essere da coloro che rappresentano il vertice della Società e che ne manifestano, dunque, l'immagine verso i terzi.

In caso di violazione della normativa vigente, del Modello Organizzativo o del Codice Etico da parte degli Amministratori, l'Organismo di Vigilanza informa il Collegio Sindacale, il Revisore della Società e i Soci, che assumeranno le opportune iniziative ai sensi di legge.

I soggetti destinatari dell'informativa dell'Organismo di Vigilanza, valutata la fondatezza della segnalazione ed effettuati i necessari accertamenti, potranno assumere gli opportuni provvedimenti al fine di adottare le misure più idonee previste dalla legge.

Inoltre, salva ogni altra azione a tutela della Società, è passibile di revoca del mandato l'Amministratore che compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di chi abbia effettuato segnalazioni di violazioni del Modello o di commissione dei reati previsti dal D.Lgs. 231/2001 per motivi che siano collegati, direttamente o indirettamente, alla segnalazione stessa.

Analogha sanzione è prevista per l'Amministratore che effettui con dolo o colpa grave segnalazioni di violazioni del Modello o di commissione dei reati previsti dal D.Lgs. 231/2001 che si rivelano infondate.

6.5. MISURE NEI CONFRONTI DEL REVISORE

L'Organismo di Vigilanza, ricevuta la notizia di violazione delle disposizioni e delle regole di comportamento del Modello e/o del Codice Etico da parte del Revisore, dovrà tempestivamente informare dell'accaduto l'Amministratore Unico che, valutata la fondatezza della segnalazione ed effettuati i necessari accertamenti, ne informeranno l'Assemblea al fine di assumere gli opportuni provvedimenti previsti dalla legge.

6.6. MISURE NEI CONFRONTI DI COLLABORATORI, CONSULENTI E SOGGETTI TERZI

Ogni comportamento posto in essere da collaboratori, consulenti o altri terzi legati alla Società da un rapporto contrattuale non di lavoro dipendente, in violazione delle previsioni del Decreto, del Modello e/o del Codice di Etico Deontologico per le parti di loro competenza, potrà determinare l'applicazione di penali o la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla Società, anche indipendentemente dalla risoluzione del rapporto contrattuale.

7. LA FORMAZIONE E L'INFORMAZIONE

Pur in mancanza di una specifica previsione all'interno del D.Lgs. 231/2001, le Linee Guida sulla predisposizione dei modelli 231, precisano che la comunicazione al personale e la sua formazione sono due fondamentali requisiti del Modello ai fini del suo corretto funzionamento.

Infatti, al fine di dotare il Modello Organizzativo di efficacia discriminante, la Società assicura una corretta divulgazione dei contenuti e dei principi dello stesso sia all'interno che all'esterno della propria organizzazione.

L'attività di comunicazione e formazione è diversificata a seconda dei destinatari cui essa si rivolge, ma deve essere, in ogni caso, improntata a principi di tempestività, efficienza (completezza, chiarezza, accessibilità) e

continuità, al fine di consentire ai diversi destinatari la piena consapevolezza di quelle disposizioni dell'Ente che sono tenuti a rispettare e delle norme etiche che devono ispirare i loro comportamenti.

Il personale è tenuto a:

I - acquisire consapevolezza dei contenuti del Modello messi a sua disposizione;

II - conoscere le modalità operative con le quali deve essere realizzata la propria attività.

Deve essere garantita al personale la possibilità di accedere e consultare la documentazione costituente il Modello, i protocolli di controllo e le procedure ad esso riferibili. Inoltre, al fine di agevolare la comprensione del Modello, il personale, con modalità diversificate secondo il loro grado di coinvolgimento nelle attività individuate come sensibili ai sensi del D.Lgs. 231/2001, è tenuto a partecipare alle specifiche attività formative che saranno promosse dalla Società.

Major Bit provvede ad adottare idonei strumenti di comunicazione per aggiornare il personale circa le eventuali modifiche apportate al presente Modello, nonché ogni rilevante cambiamento procedurale, normativo o organizzativo.

La partecipazione ai programmi di formazione è obbligatoria per il personale ed è oggetto di documentazione ed archiviazione.

La formazione del personale include anche tematiche relative alla sicurezza informatica, alla protezione dei dati personali, all'utilizzo corretto delle tecnologie digitali e ai rischi connessi all'impiego di sistemi di intelligenza artificiale.

8. ADOZIONE DEL MODELLO – CRITERI DI AGGIORNAMENTO E ADEGUAMENTO DEL MODELLO

L'Amministratore che delibera - gli aggiornamenti del Modello ed il suo adeguamento in conseguenza di:

- modifiche dell'assetto interno della Società e/o delle modalità di svolgimento delle attività;
- cambiamenti delle aree di *business*;
- notizie di tentativi o di commissione dei reati considerati dal Modello;
- notizie di nuove possibili modalità di commissione dei reati considerati dal Modello;
- modifiche normative;
- risultanze dei controlli;
- significative violazioni delle prescrizioni del Modello.

Il Modello sarà, in ogni caso, sottoposto a procedimento di revisione periodica e, comunque, tutte le volte intervengano modifiche legislative che necessitino un tempestivo intervento di modifica.

Le attività di revisione effettuate sono formali e delle stesse vengono conservate le rispettive registrazioni.

L'Organismo di Vigilanza viene informato tempestivamente in merito a qualsiasi modifica del Modello di Organizzazione, Gestione e Controllo.

Il Modello è oggetto di aggiornamento periodico, almeno annuale, nonché ogniqualvolta intervengano:
modifiche normative rilevanti;

cambiamenti organizzativi significativi;

introduzione di nuove tecnologie o servizi;

emersione di nuovi rischi, in particolare in ambito digitale e informatico.

L'Organismo di Vigilanza propone gli aggiornamenti all'organo amministrativo, che ne cura l'approvazione.

9. PARTE SPECIALE

9.1. PREMESSA

L'attività svolta nel corso del progetto di adozione del Modello ha consentito di individuare le attività sensibili (d'ora in avanti anche "processi sensibili") nel cui ambito potrebbero astrattamente essere commessi i reati presupposto previsti dal D.Lgs. 231/2001.

La presente Parte Speciale contiene, per ciascuno dei processi sensibili individuati, i protocolli di controllo previsti dall'art. 6 comma 2 lett. b) del D.Lgs. 231/2001.

Nella redazione della Parte Speciale è stata seguita la metodologia descritta nel Paragrafo 3.2 della Parte Generale del presente documento.

In particolare, sono qui previsti e disciplinati gli *standard* di controllo generali e specifici in relazione ai processi sensibili individuati.

Per le violazioni dei protocolli e delle procedure richiamate si applica quanto previsto nel Capitolo 6 della Parte Generale.

Per l'aggiornamento/adeguamento della Parte Speciale si applica quanto previsto nel Capitolo 8 della Parte Generale.

9.2. LE ATTIVITÀ SENSIBILI

Le attività sensibili individuate, con indicazione della valutazione del livello di esposizione al rischio di commissione di reati effettuata incrociando l'incidenza dell'attività con il rischio astratto di reato, senza quindi considerare la mitigazione del rischio dovuta ai controlli in essere e al Modello adottato sono i seguenti:

Attività sensibili	Esposizione potenziale al rischio (senza considerazione dei controlli)
Acquisizione delle commesse	Alta
Gestione della commessa	Alta
Gestione delle attività di Delivery	Alta
Gestione eventuali contenziosi giudiziali o procedimenti arbitrali	Bassa
Gestione delle attività per l'ottenimento di contributi/finanziamenti, anche sotto forma di credito d'imposta	Media
Gestione delle ispezioni	Media

Gestione degli investimenti	Media
Gestione degli acquisti (beni, servizi, consulenze prestazioni professionali e soluzioni software specialistiche)	Alta
Selezione, assunzione e gestione del personale (compresi i soggetti appartenenti a categorie protette o la cui assunzione è agevolata)	Alta
Gestione dei flussi finanziari (pagamenti e incassi)	Alta
Gestione dei rapporti infragruppo	Media
Elaborazione del bilancio e comunicazione a stakeholders e/o a terzi di dati e informazioni relativi alla situazione economica, patrimoniale e finanziaria della società	Alta
Predisposizione di dichiarazioni dei redditi o di sostituti d'imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere	Alta
Gestione delle risorse informatiche e del sito internet	Alta
Gestione degli adempimenti in materia ambientale	Bassa
Salute e sicurezza nei luoghi di lavoro	Media

9.3. IL SISTEMA DEI CONTROLLI

Il sistema dei controlli adottato dalla Società, costruito anche sulla base delle Linee Guida emanate da Confindustria nei limiti precedentemente indicati (documento cui si fa riferimento nella Parte Generale del presente Modello), prevede:

1. **Principi di comportamento**, applicabili indistintamente a tutti i processi sensibili, in quanto pongono regole e divieti che devono essere rispettati nello svolgimento di qualsiasi attività;
2. **Principi di controllo**, applicati ai singoli processi sensibili e contenenti l'indicazione delle regole e dei comportamenti richiesti nello svolgimento delle rispettive attività.

9.3.1. PRINCIPI DI COMPORTAMENTO

I Destinatari del Modello – nell'espletamento di tutti i processi sensibili e più in generale nell'esercizio della propria attività lavorativa - devono rispettare i seguenti principi generali:

- osservare tutte le leggi vigenti;
- comportarsi in modo corretto, trasparente e conforme ai principi generalmente riconosciuti in ambito amministrativo contabile, in tutte le attività finalizzate alla redazione del bilancio, per fornire informazioni veritiere e corrette sulla situazione economica, patrimoniale e finanziaria della Società;
- assicurare il corretto funzionamento della Società e dei suoi organi, garantendo e agevolando ogni forma di controllo sulla gestione da parte del Revisore;
- non frapporre alcun ostacolo allo svolgimento delle attività ispettive e di controllo da parte degli enti preposti effettuando con correttezza, tempestività e buona fede tutte le eventuali comunicazioni richieste;
- utilizzare le risorse finanziarie della Società esclusivamente secondo le modalità di gestione previste dalle norme interne e dalle leggi vigenti in tema di transazioni finanziarie e di limitazione all'uso del contante,
- instaurare e mantenere qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza, in considerazione dell'imparzialità che deve ispirare l'attività amministrativa;
- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza o la vicinanza a organizzazioni criminali o comunque illecite;
- non realizzare operazioni finanziarie e/o commerciali con controparti che utilizzano strutture societarie opache e/o che impediscono l'identificazione univoca dell'assetto societario (proprietà) e/o dei reali beneficiari dell'operazione;

È espressamente vietato:

- sfruttare o vantare relazioni esistenti o asserite con un rappresentante della Pubblica Amministrazione al fine di farsi dare o far dare ad altri denaro o altra utilità, come prezzo della mediazione illecita o per remunerare il rappresentante della PA in relazione all'esercizio della funzione o dei suoi poteri o in relazione ad un atto contrario alla propria funzione o dei suoi poteri;
- offrire denaro o altra utilità ad un soggetto terzo (anche consulente o fornitore della Società) che sfrutta o vanta relazioni esistenti o asserite con un rappresentante della Pubblica Amministrazione, come prezzo della mediazione illecita o per remunerare il rappresentante della PA in relazione all'esercizio della funzione o dei suoi poteri o in relazione ad un atto contrario alla propria funzione o dei suoi poteri.

Per ciascuna attività sensibile individuata sono stati indicati principi comportamentali generali volti a limitare la possibilità di realizzazione dei reati rilevanti ai fini 231.

9.3.2. PRINCIPI DI CONTROLLO

I principi di controllo sono indicati di seguito e sono descritti nell'ambito di ciascuna attività sensibile prevista al capitolo 10:

- **Regolamentazione del processo e segregazione dei compiti:**

identificazione delle attività poste in essere dalle varie funzioni e ripartizione delle stesse tra chi esegue, chi autorizza e chi controlla, in modo tale che nessuno possa gestire in autonomia l'intero processo; tale segregazione è garantita dall'intervento all'interno di un processo sensibile di più soggetti, al fine di assicurare indipendenza ed obiettività nella gestione dell'attività.

La descrizione delle attività sensibili, in alcuni casi, costituisce la formalizzazione delle prassi operative seguite da coloro che intervengono nel processo.

- **Esistenza di procedure/linee guida/prassi operative consolidate:**

esistenza di disposizioni, procedure formalizzate o prassi operative idonee a fornire principi di comportamento e modalità operative per lo svolgimento delle attività sensibili. Ove esistenti, sono riportate le procedure della Società, applicabili all'attività sensibile, vigenti al momento dell'aggiornamento del Modello, o l'indicazione delle prassi operative consolidate e formalizzate nel Modello.

- **Tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informatici:**

verificabilità *ex post* del processo di decisione, autorizzazione e svolgimento dell'attività sensibile, anche tramite apposite evidenze archiviate.

Rispetto ai processi sensibili indicati, è stata valutata l'esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate.

- **Esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate:**

formalizzazione di poteri di firma e di rappresentanza coerenti con le responsabilità organizzative e gestionali assegnate e chiaramente definiti e conosciuti all'interno della Società.

Le attività sono svolte nel rispetto di quanto previsto dal sistema interno di procure che attribuiscono poteri di rappresentanza di Major Bit verso l'esterno e dal sistema interno di deleghe per lo svolgimento dell'attività di competenza.

- **Famiglie di reato associabili:**

vengono enumerate le fattispecie di reato, aggregate per famiglie, delle quali, nell'ambito delle attività di *risk assessment*, si è rilevato il potenziale rischio di commissione. A prescindere dai reati indicati, nello svolgimento dei processi sensibili devono essere sempre applicati tutti i protocolli di controllo e di comportamento in quanto utili alla prevenzione di attività illecite.

- **Flussi informativi verso l'O.d.V.:**

sono indicati gli elementi informativi che dovranno essere sistematicamente assicurati all'Organismo di Vigilanza con le cadenze e modalità da questo precisate.

Oltre ai sopra elencati principi generali, in relazione alle singole attività, sono indicati protocolli di controllo specifici volti a mitigare rischi tipici del processo sensibile considerato. Le deroghe ai controlli generali e specifici previsti dal presente Modello e dal Codice Etico devono essere motivate ed autorizzate dall'Amministrazione.

10. ATTIVITÀ SENSIBILI

10.1. ACQUISIZIONE DELLE COMMESSE

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- non è ammesso riconoscere o promettere denaro o altra utilità (ad es. assunzione in Società) a soggetti legati alla Pubblica Amministrazione da vincoli di parentela, amicizia o segnalati dai Funzionari Pubblici, al fine di ottenere indebiti vantaggi per la Società;
- è vietato offrire omaggi e regalie, eccedenti le normali pratiche commerciali o di cortesia, a soggetti privati o a funzionari pubblici, o a loro familiari o a soggetti da loro indicati, che possano influenzarne l'indipendenza di giudizio o indurli ad assicurare un qualsiasi vantaggio indebito alla Società;
- è fatto espresso divieto di indurre in errore il funzionario pubblico della stazione appaltante circa la sussistenza dei requisiti previsti dal bando di gara o dalla trattativa privata, allo scopo di ottenere l'indebita assegnazione dell'appalto o del contratto, pur non possedendo i requisiti a tal fine richiesti;
- è vietato dare o promettere denaro o altra utilità aderendo ad una richiesta illecita da parte di Pubblico Ufficiale o di un Incaricato di Pubblico Servizio, per ottenere indebiti vantaggi per la Società (ad es. aggiudicazione della gara d'appalto);
- è vietato, in occasione di visite ispettive, indurre il privato o il funzionario pubblico ad omettere la contestazione di eventuali irregolarità o inadempimenti commessi dalla Società;
- è vietato alterare o falsificare il contenuto della documentazione richiesta dall'Ente Pubblico (ad es. falsa dichiarazione o falsa autocertificazione);
- è vietato omettere fraudolentemente dati o informazioni relativi alla documentazione da presentare alla Pubblica Amministrazione;
- non è ammesso riconoscere o promettere denaro o altra utilità (ad es. assunzione in Società) a soggetti privati, al fine di ottenere indebiti vantaggi per la Società;
- ogni attività relativa alla partecipazione alla gara viene opportunamente registrata e adeguatamente supportata da documentazione scritta, al fine di garantirne la tracciabilità e di verificare, in qualsiasi momento, la correttezza e completezza dei documenti prodotti;
- nell'esecuzione di lavori, qualora la società dovesse utilizzare aziende terze provvederà alla verifica del rispetto della normativa in materia di subappalto, in tema di salute e sicurezza e della regolarità del personale impiegato;
- è fatto obbligo di verificare il rispetto di quanto previsto nel CCNL di riferimento rispetto a straordinari, riposi, ferie, permessi etc.

I medesimi principi, in quanto applicabili, devono essere osservati anche in caso di appalti privati.

Regolamentazione del processo e segregazione dei compiti

Il processo di “**Acquisizione delle commesse**” si svolge secondo le seguenti macro attività:

- definizione delle esigenze della clientela ed analisi di mercato e delle attività dei *competitors* da parte della funzione Account Manager
- instaurazione e sviluppo dei rapporti con il cliente da parte dell'Account Manager;
- valutazione dell'esigenza del cliente da parte del Business Support e comunicazione alla Delivery competente;
- apertura di una request ad opera del Business Support ;
- analisi delle richieste del cliente e definizione delle specifiche del prodotto/servizio da parte del Business Support e del Client Manager;
- stima di costi e ricavi del progetto da parte del Business Support e della Delivery competente;
- definizione di un Business Case da parte del Business Support sulla base delle stime fornite dalla Delivery competente;
- eventuale fase di trattativa con il cliente gestita dal Business Support con il supporto delle Funzioni interessate, a seconda del prodotto/servizio da fornire;
- definizione del prezzo del servizio e predisposizione dell'offerta da parte del Business Support;
- verifica dell'offerta e sottoscrizione da parte dell'amministratore;
- inserimento dell'offerta nei sistemi interni da parte del Business Support e invio dell'offerta al cliente;
- ricezione dell'ordine del cliente da parte del Business Support;
- richiesta di apertura della commessa da parte del Business Support su input della Delivery competente;
- attività di verifica del Controller, nell'ambito della Funzione Finance, Controlling & Legal;
- interazione con il cliente da parte del Client Manager competente in corso di esecuzione ed eventuale coinvolgimento del Business Support in caso di criticità;
- avvio delle attività di gestione della commessa, secondo il processo descritto nella scheda “Gestione della commessa”;
- archiviazione di tutta la documentazione rilevante da parte delle Funzioni interessate mediante l'utilizzo del sistema informatico adottato dalla Società.

Il processo di “**Gestione delle attività di partecipazione a gare, anche ad evidenza pubblica**” si sviluppa secondo le seguenti macro attività:

- comunicazione all'Amministratore dei bandi di gara ad evidenza pubblica ai quali la Società intende partecipare, da parte del Business Support ovvero invito da parte della Stazione Appaltante; la comunicazione deve indicare i requisiti previsti dal bando, i motivi della scelta e i costi presunti;
- verifica del possesso dei requisiti necessari alla partecipazione da parte dell'Ufficio Gare
- predisposizione della documentazione necessaria da parte dell'Ufficio Gare
- predisposizione dell'offerta tecnica ed economica da parte dell'Ufficio Gad autorizzazione da parte del Business Support;
- approvazione dell'offerta da parte dell'Amministratore, che provvede alla sottoscrizione;
- monitoraggio dell'avanzamento della procedura di gara da parte del Business Support ed Ufficio Gare
- ricezione della comunicazione di aggiudicazione provvisoria da parte dell'Ufficio Gare;
- sottoscrizione del contratto da parte dell'Amministratore;

- esecuzione della commessa secondo quanto previsto dai processi “Gestione della commessa” e “Gestione delle attività di Delivery”.

Esistenza di procedure/linee guida/prassi operative consolidate

Si seguono le fasi indicate paragrafo precedente.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

Le attività sono tracciate mediante la registrazione ed archiviazione di tutti gli step di processo e della documentazione rilevante da parte delle Funzioni competenti, nonché mediante l'utilizzo di un sistema informatico per l'inserimento di dati e documenti

Principi di controllo specifici

Nel processo in oggetto, tutti i Destinatari devono attenersi alle regole di seguito indicate:

- i rapporti con i clienti sono improntati a correttezza, trasparenza e imparzialità e vengono tenuti da soggetti chiaramente identificati;
- nell'ambito dei rapporti commerciali con i clienti è fatto divieto di tenere condotte che possano ledere la concorrenza;
- per le operazioni riguardanti l'attività di valutazione, qualifica e selezione dei clienti, i protocolli prevedono che siano individuate situazioni di anomalia che consentano di rilevare eventuali transazioni a “rischio” o “sospette” con clienti sulla base del:
 - esistenza della controparte (ad esempio, struttura aziendale, sede operativa);
 - profilo soggettivo della controparte (ad esempio, esistenza di precedenti penali, reputazione opinabile, ammissioni o dichiarazioni da parte della controparte in ordine al proprio coinvolgimento in attività criminose);
 - comportamento della controparte (ad esempio, comportamenti ambigui, mancanza di dati occorrenti per la realizzazione delle transazioni o reticenza a fornirli);
 - dislocazione territoriale della controparte (ad esempio, transazioni effettuate in paesi off-shore);
 - profilo economico-patrimoniale dell'operazione (ad esempio, operazioni non usuali per tipologia, frequenza, tempistica, importo, dislocazione geografica);
 - caratteristiche e finalità dell'operazione (ad esempio, uso di prestanomi, modifiche delle condizioni contrattuali standard, finalità dell'operazione);
- le attività di selezione ed analisi dei bandi di gara, di verifica dei requisiti amministrativi e tecnico/economici e di predisposizione dei documenti per i bandi di gara vengono gestite da almeno due unità della Società in modo da garantire la segregazione del processo;
- è garantita la separazione tra gli organi che partecipano alle gare e possono avere rapporti con il potenziale committente ed i responsabili aziendali che hanno il potere di firma e, dunque, di formalizzazione delle offerte;
- le informazioni ed i dati forniti nell'ambito della partecipazione a gare (anche ad evidenza pubblica) ovvero nell'ambito della instaurazione del rapporto commerciale con il cliente sono rispondenti al vero;
- viene garantita un'adeguata formalizzazione in termini di descrizione del servizio, dei criteri di determinazione del compenso e dei termini di fatturazione delle prestazioni;

- i contratti conclusi sono conformi alle politiche aziendali nonché alle normative vigenti e riportare l'impegno al rispetto del Codice Etico adottato dalla Società nonché del D.Lgs231/2001;
- tutta la documentazione rilevante è debitamente archiviata presso la Società in modo da garantire la tracciabilità delle fasi chiave del processo al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle decisioni.

Famiglie di reato associabili

- Reati contro la PA;
- Reati informatici;
- Reati societari -corruzione tra privati;
- Reati di riciclaggio e Autoriciclaggio;
- Associazione per delinquere;
- Reati tributari

Flussi informativi verso l'O.d.V.:

A cura del Ufficio Gare:

1. indicazione delle gare a cui la società ha partecipato nell'anno solare.

10.2. GESTIONE DELLA COMMESSA

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- non è ammesso riconoscere o promettere denaro o altra utilità (ad es. assunzione in Società) a soggetti legati alla Pubblica Amministrazione da vincoli di parentela, amicizia o segnalati dai Funzionari Pubblici, al fine di ottenere indebiti vantaggi per la Società;
- è vietato offrire omaggi e regalie, eccedenti le normali pratiche commerciali o di cortesia, a soggetti privati o a funzionari pubblici, o a loro familiari o a soggetti da loro indicati, che possano influenzarne l'indipendenza di giudizio o indurli ad assicurare un qualsiasi vantaggio indebito alla Società;
- è vietato dare o promettere denaro o altra utilità aderendo ad una richiesta illecita da parte di Pubblico Ufficiale o di un Incaricato di Pubblico Servizio, per ottenere indebiti vantaggi per la Società (ad es. pagamento della fattura per un lavoro male eseguito);
- è vietato, in occasione di visite ispettive, indurre il privato o il funzionario pubblico ad omettere la contestazione di eventuali irregolarità o inadempimenti commessi dalla Società;
- è vietato alterare o falsificare il contenuto della documentazione richiesta dall'Ente Pubblico (ad es. falsa dichiarazione o falsa autocertificazione);
- è vietato porre in essere atti di concorrenza con violenza o minaccia;

- è vietato omettere fraudolentemente dati o informazioni relativi alla documentazione da presentare alla Pubblica Amministrazione;
 - è vietato consegnare cose in tutto o in parte difformi rispetto alle caratteristiche pattuite nell'esecuzione di contratti di fornitura conclusi un ente pubblico ovvero con un'impresa esercente servizi pubblici o di pubblica necessità o nell'adempimento degli altri obblighi contrattuali;
 - non è ammesso riconoscere o promettere denaro o altra utilità (ad es. assunzione in Società) a soggetti privati, al fine di ottenere indebiti vantaggi per la Società;
 - ogni attività relativa all'esecuzione della commessa viene opportunamente registrata e adeguatamente supportata da documentazione scritta, al fine di garantirne la tracciabilità e di verificare, in qualsiasi momento, la correttezza e completezza dei documenti prodotti;
 - nell'esecuzione di lavori, qualora la società dovesse utilizzare aziende terze provvederà alla verifica del rispetto della normativa in tema di salute e sicurezza e della regolarità del personale impiegato;
 - è fatto obbligo di verificare il rispetto di quanto previsto nel CCNL di riferimento rispetto a straordinari, riposi, ferie, permessi etc.
- I medesimi principi, in quanto applicabili, devono essere osservati anche in caso di appalti privati.

Regolamentazione del processo e segregazione dei compiti

Il processo di “**Gestione della commessa**” si svolge secondo le seguenti macro attività:

- apertura della commessa ad esito delle attività descritte nel processo di “Acquisizione delle commesse”;
- l'Account Manager competente raccoglie i dati rilevanti per la progettazione della commessa, ovvero ordine del cliente, documenti tecnici allegati (capitolati, specifiche tecniche), banca dati e know how aziendale;
- analisi dei dati ed elaborazione dell'architettura del progetto (“Project Chart”), dove sono indicate le caratteristiche del prodotto/servizio da realizzare, da parte del Project Manager;
- riesame del Project Chart da parte del Project Manager e successiva verifica da parte dell'Account Manager
- attivazione delle attività di Delivery ed eventuale approvvigionamento dei beni e servizi necessari all'esecuzione del progetto, secondo quanto previsto dal processo descritto nella scheda “Gestione delle attività di Delivery”;
- in corso di esecuzione, presentazione del rapporto attività e nota spese al Project Manager sia per i dipendenti (mediante caricamento di timesheet) sia per i fornitori esterni;
- attribuzione dei costi interni ed esterni sul sistema di gestione delle commesse da parte del Project Manager;
- verifica mensile della correttezza dei costi e ricavi a cura del Project Manager;
- in caso di criticità, coinvolgimento dell'Account Manager ed eventualmente del Business Support per la risoluzione del problema;
- aggiornamento della pianificazione delle commesse a cura del Project Manager;
- termine attività di Delivery e collaudo presso il cliente
- validazione *ex post* del progetto da parte del Delivery Manager competente;
- segnalazione per chiusura commessa da parte del Project Manager;
- ricezione dell'approvazione del progetto da parte del cliente
- chiusura/verifica dello stato di avanzamento della commessa sul gestionale amministrativo e gestione della fatturazione da parte dell'Amministrazione.

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività sensibile è svolta secondo quanto sopra descritto, in conformità ai principi generali di comportamento e controllo.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

La tracciabilità è garantita dall'inserimento su sistema informatico di tutti i dati ed i documenti rilevanti relativi al processo.

Principi di controllo specifici

Nel processo in oggetto, tutti i Destinatari devono attenersi alle regole di seguito indicate:

- i rapporti con i clienti devono essere improntati alla correttezza e trasparenza e imparzialità e vengono tenuti da soggetti chiaramente identificati;
- la valutazione della proposta economica viene effettuata secondo quanto previsto dalle regole aziendali;
- i costi della commessa devono essere inseriti nel sistema informatico utilizzato dalla Società e verificati sulla base di dati veritieri;
- vengono tracciate eventuali modifiche in fase di esecuzione della commessa che comportano cambiamenti nelle prestazioni rese e difformità rispetto ai compensi pattuiti;
- il Project Manager monitora lo stato di avanzamento dei lavori e verifica che quanto eseguito sia in linea con quanto contrattualizzato; un ulteriore controllo sullo svolgimento dell'attività commissionata dal cliente è infine svolto dal Business Support.
- la gestione delle fatture è improntata a criteri di correttezza, congruità e trasparenza. In particolare, sono istituiti opportuni controlli nel processo finalizzati a garantire la correttezza delle fatture emesse e la rispondenza delle stesse a quanto pattuito contrattualmente e alla fornitura effettivamente resa;
- il processo è tracciato e la documentazione è compiutamente registrata e archiviata.

Famiglie di reato associabili:

- Reati contro la Pubblica Amministrazione;
- Reati informatici;
- Reati di riciclaggio e autoriciclaggio;
- Reati societari (corruzione tra privati);
- Delitti contro l'industria e il commercio;
- Associazione per delinquere;
- Reati tributari.

Flussi informativi verso l'O.d.V.:

A cura del Project Manager:

- indicazione delle eventuali criticità segnalate dai clienti rispetto alla gestione della commessa.

10.3. GESTIONE DELLE ATTIVITÀ DI DELIVERY

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- non è ammesso riconoscere o promettere denaro o altra utilità (ad es. assunzione in Società) a soggetti di altre società, al fine di ottenere indebiti vantaggi;
- è vietato offrire omaggi e regalie, eccedenti le normali pratiche commerciali o di cortesia, a soggetti privati, o a loro familiari o a soggetti da loro indicati, che possano influenzarne l'indipendenza di giudizio o indurli ad assicurare un qualsiasi vantaggio indebito alla Società;
- è vietato dare o promettere denaro o altra utilità aderendo ad una richiesta illecita da parte del privato, per ottenere indebiti vantaggi per la Società (ad es. pagamento della fattura per un lavoro male eseguito);
- è vietato, in occasione di visite ispettive dell'Ente Appaltante, indurre il privato o il ad omettere la contestazione di eventuali irregolarità o inadempimenti commessi dalla Società;
- è vietato alterare o falsificare il contenuto della documentazione richiesta dall'Ente appaltante (ad es. falsa dichiarazione o falsa autocertificazione);
- è fatto divieto di utilizzare beni di cui non sia nota la provenienza o la cui provenienza sia illecita;
- ogni attività relativa all'esecuzione della commessa viene opportunamente registrata e adeguatamente supportata da documentazione scritta, al fine di garantirne la tracciabilità e di verificare, in qualsiasi momento, la correttezza e completezza dei documenti prodotti;
- è fatto divieto utilizzare opere dell'ingegno altrui senza i necessari diritti di sfruttamento;
- è fatto divieto fornire al cliente un servizio qualitativamente/quantitativamente difforme rispetto a quello pattuito;
- nell'esecuzione di lavori, qualora la società dovesse utilizzare aziende terze provvederà alla verifica del rispetto della normativa in tema di salute e sicurezza e della regolarità del personale impiegato;
- è fatto obbligo di verificare il rispetto di quanto previsto nel CCNL di riferimento rispetto a straordinari, riposi, ferie, permessi etc.

Regolamentazione del processo e segregazione dei compiti

Il processo di **“Gestione delle attività di Delivery”** è relativo alle fasi di realizzazione ed erogazione del servizio nei confronti del cliente, e si distingue in **“Task Project”**, **“Support/helpdesk”** e **“Time & Material”**.

L'erogazione di **“Task Project”** si sviluppa secondo le seguenti macro attività:

- definizione delle specifiche tecniche dell'attività da parte del Project Manager ;
- assegnazione delle risorse con le competenze necessarie al progetto;
- esecuzione dell'attività da parte delle risorse assegnate al progetto a valle di un'analisi funzionale;
- valutazione ed eventuale modifica del progetto in caso di richieste o variazioni, secondo il processo descritto nella scheda **“Gestione della commessa”**;

- test sulla corretta esecuzione delle attività di manutenzione ;
- termine dell'attività ed attivazione del processo di valutazione *ex post* e fatturazione della commessa, come previsto dall'attività descritta nella scheda intervista "Gestione della commessa".

L'erogazione dei "**Support/Helpdesk**" avviene secondo i seguenti passaggi:

- definizione delle specifiche tecniche di erogazione del servizio
- assegnazione delle risorse con le competenze necessarie al progetto
- erogazione del servizio da parte del Responsabile di Commessa e delle risorse assegnate al progetto;
- implementazione delle eventuali modifiche richieste dal cliente nel corso della erogazione del servizio;
- termine dell'attività ed attivazione del processo di valutazione *ex post* e fatturazione della commessa, come previsto dall'attività descritta nella scheda intervista "Gestione della commessa".

L'erogazione dei servizi "**Time & Material**" si sviluppa nelle seguenti macroattività:

- contatto con il cliente per l'individuazione delle attività da svolgere "Time & Material" da parte del Business Support
- pianificazione dell'attività da parte del Business support;
- individuazione della risorsa interna o esterna da assegnare al progetto e da utilizzare per la erogazione del servizio, da parte del Business Support
- approvazione delle risorse da parte del cliente;
- erogazione del servizio da parte delle risorse assegnate al progetto;
- approvazione del servizio erogato da parte del cliente
- in caso di assenza di richieste di modifica, termine dell'attività ed attivazione del processo di valutazione *ex post* e fatturazione, come previsto dall'attività descritta nella scheda intervista "Gestione della commessa".

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività sensibile è svolta secondo quanto sopra descritto, in conformità ai principi generali di comportamento e controllo.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

Il processo decisionale è documentato e la documentazione viene archiviata dalle funzioni che intervengono nel processo, ognuna per la propria competenza.

La tracciabilità è garantita dalla registrazione ed archiviazione di tutta la documentazione rilevante e attraverso l'inserimento dei dati di progetto all'interno del sistema informatico della società.

Principi di controllo specifici

Nel processo in oggetto, tutti i Destinatari devono attenersi alle regole di seguito indicate:

- i soggetti coinvolti nel processo sono formalmente individuati e autorizzati;
- i rapporti con i clienti sono improntati alla correttezza, trasparenza e imparzialità;

- i dipendenti impiegati nello svolgimento delle attività aziendali sono legati alla Società da un regolare rapporto di lavoro e viene garantito il rispetto delle condizioni di lavoro secondo quanto previsto nei CCNL applicabili, anche qualora la propria attività venga prestata all'estero;
- è garantita l'effettività dei contratti e delle prestazioni erogate;
- il Business Support verifica che quanto eseguito sia in linea con quanto contrattualizzato;
- la gestione delle fatture è improntata a criteri di correttezza, congruità e trasparenza. In particolare, sono istituiti opportuni controlli nel processo finalizzati a garantire la correttezza delle fatture emesse e la rispondenza delle stesse a quanto pattuito contrattualmente e alla fornitura effettivamente resa;
- il processo è tracciabile e la documentazione viene compiutamente registrata e archiviata.

Famiglie di reato associabili

- Reati contro la Pubblica Amministrazione;
- Reati societari - corruzione tra privati;
- Reati informatici;
- Delitti in materia di violazione del diritto di autore;
- Delitti contro l'industria e il commercio;
- Reati di ricettazione, riciclaggio e autoriciclaggio;
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
- Intermediazione illecita e sfruttamento del lavoro;
- Associazione per delinquere;
- Reati Tributari

Flussi informativi verso l'O.d.V.:

A cura del Business Support:

- indicazione delle eventuali criticità segnalate dai clienti rispetto alla gestione delle attività di delivery.

10.4. GESTIONE DEGLI EVENTUALI CONTENZIOSI GIUDIZIALI O PROCEDIMENTI ARBITRALI

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- è fatto obbligo di eseguire con la massima tempestività, correttezza e buona fede tutte le richieste provenienti dagli organi di Polizia Giudiziaria e dall’Autorità Giudiziaria, fornire tutte le informazioni, dati e notizie richiesti;
- è fatto obbligo di avere, nei confronti degli organi di Polizia Giudiziaria e dell’Autorità Giudiziaria, un atteggiamento collaborativo e corretto.
- è vietato di far uso di minacce ovvero promettere, offrire o concedere un’indebita utilità per indurre chi abbia la facoltà di astenersi nel procedimento penale, a non rendere dichiarazioni o a rendere false dichiarazioni all’Autorità Giudiziaria, al fine di ottenere una pronuncia favorevole alla Società o di ottenere qualsiasi altro vantaggio in favore della stessa;
- il rapporto con l’autorità giudiziaria e i suoi ausiliari, anche nell’ambito della partecipazione alle udienze, viene gestito attraverso la nomina di legali e consulenti esterni;
- ai professionisti esterni viene data comunicazione dell’adozione del Modello di Organizzazione e Gestione da parte della Società.

Regolamentazione del processo e segregazione dei compiti

Il processo di “**gestione degli eventuali contenziosi giudiziari o procedimenti arbitrali**” si articola nelle seguenti fasi:

- raccolta delle informazioni e della documentazione relativi alla controversia da parte dei Responsabili di Funzione;
- segnalazione all’Amministrazione per le tematiche giuslavoristiche ed analisi della pratica;
- valutazione dell’eventuale contenzioso legale da intraprendere da parte dell’Amministratore
- nomina di un legale esterno di specifica competenza ed affidamento della gestione del contenzioso;
- coinvolgimento nella gestione del contenzioso del consulente esterno incaricato;
- autorizzazioni su decisioni rilevanti nella causa ad opera dell’Amministratore;

Esistenza di procedure/linee guida/prassi operative consolidate

L’attività sensibile viene svolta secondo quanto sopra descritto, in conformità ai principi generali di comportamento e controllo.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

Il processo decisionale è documentato e la tracciabilità dell’intero processo è assicurata dall’archiviazione della documentazione rilevante da parte dell’Amministrazione

Principi di controllo specifici

Nel processo di gestione dei contenziosi giudiziali o procedimenti arbitrali, tutti i destinatari del presente Modello devono agire nel rispetto delle regole di seguito indicate:

- il rapporto con l’Autorità Giudiziaria e i suoi ausiliari, anche nell’ambito della partecipazione alle udienze, è gestito, attraverso la nomina di legali dell’Amministrazione;
- nell’ambito della gestione dei contenziosi tributari, il consulente legale esterno è informato nel caso di ispezioni in ambito tributario e fiscale, al fine di coadiuvare la Società nella gestione della visita ispettiva, nell’interlocuzione con l’amministrazione finanziaria e nella produzione di ogni documento utile e/o richiesta, oltre che per la valutazione dell’eventuale adesione alle speciali procedure conciliative, di adesione all’accertamento, previste dalle norme tributarie nonché del ravvedimento operoso;
- l’incarico a professionisti esterni viene conferito per iscritto con indicazione del compenso pattuito e dell’oggetto della prestazione;
- ai professionisti esterni viene data comunicazione dell’adozione del Codice Etico e del Modello di Organizzazione e Gestione da parte della Società; questi ultimi dovranno impegnarsi ad osservarne il contenuto del Codice e del D.Lgs. 231/2001;
- i compensi, le provvigioni o le commissioni ai professionisti esterni vengono determinate in misura congrua rispetto alle prestazioni rese e conformi all’incarico conferito, secondo le condizioni o le prassi esistenti sul mercato, tenendo conto delle tariffe professionali vigenti per la categoria interessata;

Famiglie di reato associabili:

- Reati contro la Pubblica Amministrazione;
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria;
- Associazione per delinquere;
- Autoriciclaggio;
- Reati Tributari.

Flussi informativi verso l’O.d.V.:

A cura dell’Amministrazione:

1. segnalazione tempestiva della notificazione di atti relativi a procedimenti giudiziali e/o arbitrali riguardanti la Società o, in senso lato, i Destinatari del Modello;
2. elenco dei contenziosi pendenti, con distinzione degli stessi in relazione alla materia, e specificazione dello stato del procedimento.

10.5. GESTIONE DELLE ATTIVITÀ PER L’OTTENIMENTO DI CONTRIBUTI/FINANZIAMENTI, ANCHE SOTTOFORMA DI CREDITO D’IMPOSTA

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- è vietato esibire a Funzionari Pubblici documenti incompleti, falsi o contraffatti e/o comunicare dati falsi o alterati;
- è vietato presentare dichiarazioni non veritiere a Funzionari Pubblici, nazionali o comunitari, al fine di ottenere indebitamente erogazioni pubbliche, contributi o finanziamenti agevolati;
- è vietato tenere una condotta ingannevole che possa indurre in errore i Funzionari Pubblici;
- è vietato procurare indebitamente, a sé, a terzi o alla Società, vantaggi di qualsivoglia natura a danno della Pubblica Amministrazione;
- i soggetti coinvolti nella gestione del processo in oggetto e che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Società devono essere muniti dei necessari poteri;
- i soggetti che richiedono e gestiscono finanziamenti erogati da Enti Pubblici e che intrattengono rapporti con gli Enti finanziatori nell'interesse della Società, devono essere formalmente autorizzati, nel rispetto del sistema di deleghe e procure;
- non è consentito destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti a scopi diversi da quelli cui erano state originariamente erogate;
- non è ammesso riconoscere o promettere denaro o altra utilità (ad es. assunzione in Società) a soggetti privati, al fine di ottenere indebiti vantaggi per la Società;
- è fatto obbligo di chiedere una perizia a soggetti qualificati per la verifica dell'ammissibilità delle spese al finanziamento.

I principi sopra indicati, in quanto applicabili, devono essere osservati anche in caso di rapporti con i privati.

Regolamentazione del processo e segregazione dei compiti

Il processo di **“Gestione delle attività per l’ottenimento di contributi/finanziamenti, anche sottoforma di credito d’imposta”** si articola nelle seguenti fasi:

- presentazione all'Amministratore di un piano dei finanziamenti pubblici che la Società intende richiedere, ovvero presentazione del piano relativo al singolo investimento al sorgere dell'opportunità;
- il piano include i requisiti richiesti dalla PA, i motivi della scelta dei contributi specifici e i costi presunti;
- verifica della presenza dei requisiti per l'ottenimento del finanziamento da parte della Direzione Commerciale;
- controllo sul possesso dei requisiti;
- predisposizione della documentazione da parte della funzione amministrativa
- sottoscrizione della richiesta di finanziamento da parte dell'amministratore
- esecuzione delle attività finanziate da parte delle Funzioni competenti secondo quanto previsto dalle condizioni di accesso al finanziamento;
- redazione dello stato di avanzamento delle attività finanziate da parte delle Funzioni competenti e successiva verifica da parte dell'Amministratore;
- controllo e rendicontazione del contributo ottenuto da parte della Funzione Administration, con la supervisione dell' Amministratore, con eventuale ausilio del consulente esterno;
- sottoscrizione della rendicontazione da parte dell'Amministrazione

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività si svolge secondo quanto previsto nel protocollo "Finanziamenti e contributi pubblici", in conformità ai principi generali di comportamento e controllo.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

La tracciabilità è garantita dall'archiviazione della documentazione relativa al processo da parte delle Funzioni che intervengono. La rendicontazione del finanziamento ottenuto è archiviata dalla Funzione Administration.

Principi di controllo specifici

Nel processo in oggetto, i Destinatari devono attenersi alle regole di seguito indicate:

- la completezza formale e sostanziale della documentazione da produrre viene verificata dall'Amministratore;
- l'eventuale coinvolgimento di un consulente esterno nelle attività di predisposizione della documentazione è autorizzata dai soggetti muniti di appositi poteri in conformità al sistema di deleghe e procure esistente;
- nel caso di esposizione di crediti d'imposta, la Società si avvale di un consulente che fornisce perizia giurata sulla veridicità e correttezza delle somme portate a credito; tale perizia viene verificata anche dal Revisore;
- il contratto non deve prevedere compensi per il consulente legati in maniera preponderante al beneficio ottenuto;
- in caso di affidamento a consulenti esterni, il compenso viene preventivamente stabilito conformemente alle tariffe professionali vigenti;
- in casi di affidamento a consulenti esterni, l'attività svolta a contatto con gli organi della Pubblica Amministrazione è oggetto di specifica verifica;
- le attività poste in essere e lo stato di avanzamento del progetto stesso sono monitorate costantemente dalle Funzioni interne competenti;
- la rendicontazione dei costi è predisposta dagli uffici preposti e verificata dall'Amministratore.

Famiglie di reato associabili:

- Reati contro la Pubblica Amministrazione;
- Reati informatici;
- Reati di riciclaggio e autoriciclaggio;
- Reati societari (corruzione tra privati);
- Associazione per delinquere;
- Reati tributari

Flussi informativi verso l'O.d.V.:

A cura dell'Amministrazione:

- elenco dei contributi o finanziamenti richiesti e di quelli ottenuti dalla Società.

10.6. GESTIONE DELLE ISPEZIONI

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- è richiesto il rispetto della normativa vigente;
- i soggetti autorizzati ad intrattenere rapporti con la Pubblica Amministrazione sono formalmente individuati;
- nell'ambito dei rapporti con la Pubblica Amministrazione, sono vietati gli omaggi al di fuori di quanto previsto dalla prassi aziendale, pertanto, sono vietate le regalie che eccedano le normali pratiche commerciali o di cortesia;
- nell'ambito dei rapporti, diretti o indiretti, con i rappresentanti della Pubblica Amministrazione, è fatto divieto di tenere comportamenti volti ad influenzarne l'indipendenza di giudizio per ottenere benefici in favore proprio o della Società;
- al personale autorizzato ad intrattenere rapporti con la Pubblica Amministrazione è fatto obbligo di garantire il rispetto dei principi di onestà e correttezza, al fine di non compromettere l'integrità e la reputazione della Società;
- al personale autorizzato a intrattenere rapporti con funzionari appartenenti alla Pubblica Amministrazione, è fatto obbligo di astenersi dall'influenzare in maniera impropria o illecita le decisioni dei rappresentanti che trattano o decidono per conto della Pubblica Amministrazione relativamente alla Società;
- è vietato procurare indebitamente, a sé, a terzi o alla Società, vantaggi di qualsivoglia natura a danno della Pubblica Amministrazione;
- è vietato dare o promettere denaro o altra utilità aderendo ad una richiesta illecita da parte un rappresentante di un Ente Pubblico per ottenere indebiti vantaggi per la Società;
- è fatto obbligo di evitare o comunque segnalare qualsiasi situazione di conflitto di interessi con funzionari della Pubblica Amministrazione, al fine di garantire la massima trasparenza nei rapporti con la stessa;
- elaborare la documentazione destinata alla Pubblica Amministrazione in modo puntuale, oggettivo ed esaustivo, utilizzando un linguaggio chiaro, al fine di fornire informazioni complete, trasparenti, comprensibili e accurate;
- improntare i rapporti con i rappresentanti della Pubblica Amministrazione alla massima trasparenza, collaborazione, disponibilità, nel rispetto del loro ruolo istituzionale, dando puntuale e sollecita esecuzione alle prescrizioni e agli adempimenti richiesti.

Le medesime regole, in quanto applicabili, vengono seguite anche in caso di visite ispettive da parte di enti privati (ad es. enti di certificazione).

Regolamentazione del processo e segregazione dei compiti

Il processo di “**Gestione delle ispezioni**” si articola come segue:

- eventuale individuazione di risorse deputate all'ispezione da parte dell'Amministrazione e, sulla base degli ambiti, se del caso anche tra i consulenti esterni (commercialista, consulente del lavoro, etc);

- partecipazione alla redazione del verbale da parte dell'Amministratore o dei soggetti individuati ed annotazione di eventuali dichiarazioni;
- sottoscrizione per presa visione del verbale da parte dell'Amministratore o dei soggetti individuati;
- registrazione e archiviazione della documentazione rilevante da parte delle Funzioni interessate dall'ispezione.

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività sensibile è svolta secondo quanto sopra descritto, in conformità ai principi generali di comportamento e controllo.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

Il processo decisionale è documentato e la documentazione viene archiviata dalle funzioni che intervengono nel processo, ognuna per la propria competenza

Principi di controllo specifici

Nel processo di gestione delle ispezioni, tutti i Destinatari del presente Modello devono attenersi alle regole di seguito indicate:

- il personale è espressamente autorizzato a gestire i rapporti con Enti privati/Pubblica Amministrazione o suoi rappresentanti;
- il personale autorizzato verifica la documentazione predisposta prima del relativo inoltro agli Enti privati/Pubblica Amministrazione garantendo la corrispondenza tra quanto predisposto dalle aree aziendali competenti e quanto inviato;
- all'ispezione partecipano almeno due dipendenti della Società, fatte salve le ipotesi in cui i funzionari pubblici richiedano colloqui diretti con personale specificamente individuato. I dipendenti hanno l'incarico di accompagnare ed assistere gli ispettori nello svolgimento di tutta l'attività di accertamento;
- il personale della Società che ha presenziato all'ispezione sottoscrive il verbale redatto dagli ispettori e verifica che i contenuti siano coerenti con le risultanze dell'accertamento, riservandosi espressamente le eventuali controdeduzioni;
- dell'ispezione e delle relative risultanze viene data immediata informazione all'Amministrazione
- tutta la documentazione relativa ai rapporti con Enti privati/Pubblica Amministrazione viene archiviata a cura della Funzione interessata dalla visita ispettiva/accertamento.

Famiglie di reato associabili:

- Reati contro la Pubblica Amministrazione;
- Corruzione tra privati;
- Associazione per delinquere.

Flussi informativi verso l'O.d.V.:

A cura dell'Amministrazione:

1. avviso delle ispezioni ricevute, con indicazione delle eventuali prescrizioni impartite;

2. indicazione delle azioni intraprese a fronte delle prescrizioni impartite dagli ispettori all'esito dell'ispezione e delle implementazioni effettuate.

10.7. GESTIONE DEGLI INVESTIMENTI

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolto nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- le risorse utilizzate per gli investimenti provengono da fonti tracciabili e non sono oggetto di attività illecite;
- gli investimenti devono essere autorizzati da soggetti muniti di appositi poteri;
- non è ammesso riconoscere o promettere denaro o altra utilità a soggetti privati, al fine di ottenere indebiti vantaggi per la Società.

Regolamentazione del processo e segregazione dei compiti

Il processo di “**Gestione degli investimenti**” si articola come segue:

- segnalazione dell'opportunità di interventi che richiedono investimenti da parte dei Responsabili di Funzione;
- valutazione degli eventuali investimenti da effettuare (sia per esigenze di mercato che per ottemperare ad adempimenti normativi) da parte dell'Amministratore con ausilio dei Responsabili di Funzione interessati;
- discussione, condivisione e approvazione degli investimenti da parte degli Amministratori;
- effettuazione dell'investimento secondo le fasi previste per gli approvvigionamenti;
- verifica dello stato di avanzamento degli investimenti da parte dei Responsabili di Funzione interessati ed informativa all'Amministratore
- archiviazione di tutta la documentazione rilevante da parte della Funzione Administration.

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività sensibile è svolta secondo quanto sopra descritto, in conformità ai principi generali di comportamento e controllo.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

La tracciabilità è garantita dall'indicazione degli investimenti da effettuare mediante informative tra gli amministratori che vengono archiviate.

Principi di controllo specifici

Nel processo di gestione degli investimenti, tutti i Destinatari del presente Modello devono attenersi alle regole di seguito indicate:

- la decisione sugli investimenti viene presa dall'Amministratore

- i soggetti coinvolti nel processo verificano la corretta esecuzione dell'attività;
- la verifica sullo stato di avanzamento degli investimenti viene effettuata dai Responsabili di Funzione che informano l'Amministratore

Famiglie di reato associabili:

- Corruzione tra privati;
- Riciclaggio e autoriciclaggio;
- Reati societari;
- Associazione per delinquere;
- Reati tributari.

Flussi informativi verso l'O.d.V.:

A cura dell'Amministrazione:

- elenco degli investimenti effettuati con indicazione dei relativi importi.

10.8. GESTIONE DEGLI ACQUISTI

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolto nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- è vietato effettuare prestazioni o pagamenti in favore di fornitori, collaboratori, consulenti, partner o altri soggetti terzi che operino per conto della Società qualora non trovino adeguata giustificazione nel rapporto contrattuale formalizzato con gli stessi e in relazione al tipo di incarico svolto o da svolgere;
- è vietato favorire indebitamente, nei processi di acquisto, collaboratori, fornitori, consulenti o altri soggetti terzi indicati da rappresentanti della Pubblica Amministrazione, senza una adeguata giustificazione;
- è vietato costringere o indurre terzi a dare o promettere, anche in favore di propri familiari o di terzi, denaro o altre utilità;
- è vietato danneggiare, in sede di selezione, fornitori in possesso dei requisiti richiesti, ricorrendo a criteri parziali, non oggettivi e fittizi;
- è vietato affidare incarichi ad eventuali fornitori/consulenti esterni eludendo criteri di valutazione obiettivi quali competitività, prezzo, integrità, solidità e capacità di garantire un servizio continuativo;
- è vietato riconoscere o promettere denaro o altra utilità (ad es. assunzione in Società) a soggetti privati, al fine di ottenere indebiti vantaggi per la Società con danno per il fornitore;
- è vietato acquistare beni la cui provenienza sia illecita o comunque non affidabile;

- è vietato effettuare pagamenti con mezzi non tracciabili, su conti correnti diversi da quello del fornitore che ha prestato il servizio;
- è vietato utilizzare fornitori che non rispettino la normativa in materia di salute e sicurezza sui luoghi di lavoro;
- è vietato impiegare lavoratori extracomunitari che siano privi di permesso di soggiorno o il cui permesso di soggiorno sia irregolare, in quanto scaduto, annullato o non rinnovato;
- è vietato utilizzare fornitori ambientali che non siano professionalmente qualificati per lo svolgimento dell'attività necessaria.

Regolamentazione del processo e segregazione dei compiti

Il processo di “**Gestione degli acquisti**” si svolge secondo le seguenti macrofasi:

- inserimento della RdA (Richiesta di Acquisto) sul gestionale della Società da parte della Funzione interessata all'acquisto;
- verifica della RdA da parte del Responsabile della Funzione interessata all'acquisto;
- approvazione della RdA da parte dell'Amministratore ed invio all'Accountant e il suo team;
- scelta del fornitore da parte del Responsabile della Funzione interessata all'acquisto sulla base dei criteri di qualificazione previsti dalle procedure interne; eventualmente la scelta ricade tra i soggetti che sono indicati all'interno dell'elenco fornitori;
- emissione della richiesta di offerta da parte dell'Amministrazione ad almeno 3 fornitori; nel caso in cui la scelta non possa avvenire tra più fornitori o offerte, a causa delle caratteristiche specifiche del prodotto o delle qualità professionali del consulente esterno, se ne dà atto con specifica annotazione;
- ricezione delle offerte da parte dell'Accountant e decisione sul fornitore da parte del Responsabile di Funzione;
- stampa dell'ordine elaborato dal sistema e sottoscrizione da parte dell'Amministratore;
- invio dell'ordine al fornitore da parte dell'Accountant;
- esecuzione dell'attività da parte del fornitore;
- valutazione dell'attività svolta ed in caso di valutazione positiva eventuale aggiornamento dell'elenco fornitori;
- ricezione delle fatture secondo quanto previsto dall'ordine di acquisto/contratto da parte dell'Accountant;
- autorizzazione al pagamento da parte dell'Amministrazione
- pagamento della fattura mediante sistema di internet banking
- archiviazione informatica e cartacea della documentazione

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività si svolge secondo quanto sopra descritto, in conformità ai principi generali di comportamento e controllo.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

Il processo decisionale è documentato e la documentazione viene archiviata dalle funzioni che intervengono nel processo, ognuna per la propria competenza.

Principi di controllo specifici

Nella gestione del processo di approvvigionamento, i Destinatari del presente Modello devono attenersi alle regole di seguito indicate:

- gli acquisti in nome e per conto della Società sono effettuati in conformità alle regole interne;
- i soggetti coinvolti nel processo sono individuati ed autorizzati;
- è fatto obbligo di astenersi dal decidere nel caso in cui si versi in conflitto d'interesse, anche solo potenziale, rispetto all'operazione da effettuare;
- gli acquisti di beni e servizi effettuati in nome e per conto della Società avvengono esclusivamente sulla base di richieste formulate per iscritto;
- sono intrattenute relazioni soltanto con fornitori che rispettino le leggi, e aderiscano a convenzioni sui diritti umani o agli standard internazionali, in materia di lavoro, con particolare riferimento agli orari di lavoro, al lavoro straordinario, alle ferie, alle retribuzioni, alla discriminazione sul luogo di lavoro;
- i consulenti individuati posseggono requisiti professionali, economici e organizzativi a garanzia degli standard qualitativi richiesti;

Famiglie di reato associabili

- Reati contro la Pubblica Amministrazione;
- Reati societari (Corruzione tra privati);
- Ricettazione, riciclaggio e autoriciclaggio;
- Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, favoreggiamento dell'ingresso clandestino degli stranieri e della permanenza illegale dello straniero nello Stato;
- Associazione per delinquere;
- Intermediazione illecita e sfruttamento dei lavoratori;
- Reati tributari

Flussi informativi verso l'O.d.V.:

A cura dell'Accountant:

1. elenco delle fatture passive, con indicazione del fornitore e del valore dei corrispettivi;
2. elenco dei contratti di consulenza stipulati, con indicazione dei corrispettivi.

10.9. SELEZIONE, ASSUNZIONE E GESTIONE DEL PERSONALE (COMPRESI I SOGGETTI APPARTENENTI A CATEGORIE PROTETTE O LA CUI ASSUNZIONE È AGEVOLATA)

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- è vietato promettere o concedere promesse di assunzione a favore di rappresentanti/esponenti della Pubblica Amministrazione ovvero loro parenti e affini allo scopo di influenzare l'indipendenza di giudizio dei rappresentanti della Pubblica Amministrazione o di indurre gli stessi ad attribuire un qualsiasi vantaggio alla Società;
- è fatto divieto di utilizzare lavoratori extracomunitari che siano privi di permesso di soggiorno o il cui permesso di soggiorno sia irregolare, in quanto scaduto, annullato o non rinnovato;
- è fatto divieto di non applicare le regole previste dalla legge e dal CCNL di riferimento (ad es. per quanto concerne retribuzione, ferie, permessi riposo e straordinari);
- è fatto divieto di consentire l'esecuzione delle prestazioni lavorative a personale non formato;
- è fatto divieto di sottoporre il lavoratore a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti;
- è fatto divieto di permettere la diffusione di ideologie, nonché il perpetrarsi di atteggiamenti, di carattere discriminatorio o violento, fondato su motivi razziali, etnici, nazionali o religiosi;
- è fatto divieto di assumere soggetti che, in costanza di un precedente rapporto di dipendenza con la Pubblica Amministrazione, abbiano compiuto atti decisori nei confronti della Società.

Gli stessi principi, in quanto applicabili, devono essere seguiti anche nei rapporti con i privati.

Regolamentazione del processo e segregazione dei compiti

Il processo di "Selezione, assunzione e gestione del personale (compresi i soggetti appartenenti a categorie protette o la cui assunzione è agevolata)" si articola nelle seguenti fasi:

- segnalazione dell'esigenza di assunzione di personale da parte dei Responsabili di Funzione
- approvazione della richiesta di procedere alla ricerca ;

- valutazione dell'obbligo di procedere ad assunzione di categorie protette sulla base dei parametri normativi quantitativi (numero di dipendenti) e qualitativi (inquadramento nelle categorie protette) e contatto con i centri per l'impiego da parte dell'Amministrazione
- autorizzazione a procedere all'assunzione ad opera dell'Amministrazione;
- ricerca e selezione del personale direttamente o, eventualmente, con l'ausilio di agenzie interinali a cura del Team Recruiting
- ricezione dei curricula e primo contatto con i candidati a cura del Team Recruiting;
- somministrazione di un eventuale test di valutazione ed esecuzione del primo colloquio conoscitivo da parte dei Responsabili di Funzione; eventuale secondo colloquio da parte di altri soggetti di livello gerarchico più elevato a seconda delle figure professionali ricercate;
- approvazione dell'assunzione da parte dell'Amministratore;
- richiesta e controllo sulla regolarità della documentazione personale del candidato (anche per quanto concerne il permesso di soggiorno per extracomunitari) e tenuta dello scadenziario da parte dell'Amministrazione
- predisposizione della documentazione necessaria all'assunzione da parte di HR Administration;
- sottoscrizione del contratto/lettera di assunzione;
- invio al candidato della lettera di assunzione e ricezione del documento da quest'ultimo firmato;
- archiviazione della documentazione a cura dell'Amministrazione.

Per ciò che concerne la **formazione del personale**, la gestione delle attività prevede:

- predisposizione di un piano annuale di formazione sulle soft skills a cura della Major Bit Academy;
- richiesta di formazione su aspetti tecnici evidenziati dalle specifiche Service Line con approvazione della funzione di Grow Up
- la pianificazione della formazione in materia di ambiente e sicurezza viene formalizzata in apposito piano di formazione predisposto dall'ASPP
- approvazione dei piani di formazione da parte dell'Amministrazione

Per ciò che concerne i “**provvedimenti disciplinari**” il processo prevede le seguenti fasi:

- segnalazione da parte dei Responsabili di Funzione del comportamento sanzionabile ;
- istruttoria per verificare i fatti a cura della Direzione o da soggetti delegati o da soggetti da questi delegati;
- contestazione e sottoscrizione del provvedimento disciplinare da parte dell'Amministrazione secondo i poteri esistenti.

Il processo di gestione del personale relativo ai “**rimborsi spesa**” si articola nelle seguenti fasi:

- caricamento delle note spese sulle commesse mediante invio mail con ricevute di spesa in allegato da parte dei singoli dipendenti;
- approvazione della nota spese da parte dell'Amministrazione
- Comunicazione al consulente del lavoro per il pagamento;
- liquidazione da parte del consulente del lavoro mediante inserimento delle somme nei cedolini del mese successivo;
- archiviazione della documentazione ad opera dell'Amministrazione per i pagamenti.

Esistenza di procedure/linee guida/prassi operative consolidate

Le attività di “**Selezione, assunzione e gestione del personale**” e di “**Formazione del personale**” si svolgono secondo prassi conosciuta da tutti coloro che intervengono nel processo.

Per ciò che concerne l’attivazione del “**Procedimento disciplinare**” e la comminazione delle sanzioni l’attività si svolge sulla base di quanto previsto dal CCNL applicabile.

Il processo relativo ai “**Rimborsi spesa**” si svolge secondo la policy aziendale

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

Il processo decisionale è documentato e la tracciabilità è garantita dall’archiviazione della documentazione rilevante da parte dell’Administration.

Principi di controllo specifici

Nel processo di selezione, assunzione e gestione del personale, i Destinatari del presente Modello devono agire nel rispetto delle regole di seguito indicate:

- i soggetti autorizzati a intervenire nel processo sono chiaramente identificati e devono essere muniti dei necessari poteri in conformità al sistema di procure esistente;
- il fabbisogno di personale è basato su effettive esigenze organizzative;
- l’avviso di ricerca di nuovo personale riporta le condizioni principali della proposta di lavoro;
- è assicurata la corretta archiviazione di tutta la documentazione relativa al processo di selezione al fine di consentire la tracciabilità dell’iter decisionale e delle motivazioni della scelta dei candidati;
- la selezione del personale è basata su una valutazione oggettiva della professionalità del candidato;
- le informazioni richieste ai candidati in sede di colloquio conoscitivo sono rispettose della sfera privata e delle opinioni personali;
- in fase di selezione viene chiesto al candidato l’eventuale esistenza di un precedente rapporto lavorativo nella Pubblica Amministrazione e, in caso affermativo, viene verificato che lo stesso non abbia partecipato all’emissione di atti di interesse per la Società;
- il personale viene assunto con regolare contratto di lavoro, stipulato nel rispetto del CCNL applicabile, e non è ammessa alcuna forma di lavoro irregolare;
- il rapporto di lavoro è formalizzato attraverso la sottoscrizione del contratto da parte dei soggetti muniti dei necessari poteri e, per accettazione, da parte del soggetto selezionato;
- al neoassunto viene inviata un’e-mail con le indicazioni su dove poter visionare le policy aziendali e il Modello Organizzativo e il Codice Etico adottati dalla Società, nonché delle procedure/istruzioni operative esistenti; il dipendente assume l’obbligo di rispettare le disposizioni e i principi previsti nel Codice Etico e del Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D.Lgs. n. 231/2001;
- al personale neoassunto sono fornite tutte le informazioni, l’assistenza, i supporti e gli strumenti utili e/o necessari al suo inserimento ed all’espletamento delle mansioni affidate;
- i dossier di ciascun dipendente sono custoditi nel rispetto del Regolamento UE 679/2017 (GDPR), le eventuali sanzioni disciplinari per comportamenti non in linea con quanto stabilito dalla legge o dalla Società sono irrogate da soggetti muniti dei necessari poteri;
- non sono ammessi anticipi o rimborsi delle spese sostenute direttamente da soggetti non dipendenti della Società, qualora non previsto dal contratto/lettera di incarico;

- la gestione dei rimborsi spese avviene in accordo con la normativa, anche fiscale, applicabile;
- le uniche spese di trasferta rimborsabili sono quelle direttamente collegabili ad incarichi di lavoro.

Famiglie di reato associabili

- Reati contro la Pubblica Amministrazione;
- Corruzione tra privati;
- Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, favoreggiamento dell'ingresso clandestino degli stranieri e della permanenza illegale dello straniero nello Stato;
- Intermediazione illecita e sfruttamento del lavoro;
- Associazione per delinquere;
- Reati tributari.

Flussi informativi verso l'O.d.V.:

A cura della funzione "Formazione " e della funzione "Grow Up"

1. elenco delle nuove assunzioni/licenziamenti effettuati;
2. segnalazione di contestazioni e di apertura del procedimento disciplinare (con specifica indicazione del motivo della contestazione), nonché delle eventuali sanzioni irrogate.

10.10. GESTIONE DEI FLUSSI FINANZIARI (PAGAMENTI E INCASSI)

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- è vietato promettere o effettuare erogazioni in denaro a favore di funzionari della Pubblica Amministrazione;
- è vietato effettuare pagamenti in favore di collaboratori, fornitori, consulenti, partner o altri soggetti terzi che operino per conto della Società e che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi;
- è vietato trasferire a qualsiasi titolo, se non per il tramite di banche o istituti di moneta elettronica, denaro contante o libretti di deposito bancari al portatore o titoli al portatore in euro o in valuta estera, quando il

valore dell'operazione, anche frazionata, sia complessivamente pari o superiore a quello previsto dalla vigente normativa;

- è vietato emettere assegni per importi pari o superiori a quello previsto dalla vigente normativa che non rechino l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- effettuare pagamenti in paesi diversi da quelli di residenza del fornitore o di esecuzione della prestazione.
- è espressamente vietato violare le limitazioni all'uso del contante e titoli al portatore attualmente vigenti di cui al D.Lgs. 231/2007 e s.m.i.;
- il personale coinvolto, a qualsiasi titolo, nella gestione dei flussi monetari e finanziari ha l'obbligo di agire nei limiti dei poteri conferiti formalmente così come previsto dal sistema di poteri esistenti;
- ogni operazione finanziaria deve essere effettuata a fronte di una controparte adeguatamente identificata;
- la Società deve assicurare la tracciabilità dei flussi finanziari nel rispetto di quanto previsto dalla L. 136/2010 laddove applicabile.

Regolamentazione del processo e segregazione dei compiti

Il processo di "**Gestione dei pagamenti**" si articola nelle seguenti fasi:

- ricezione della fattura da parte del fornitore a cura dell'Accountant e il suo team;
- registrazione della fattura a cura del team dell'Accountant previa verifica della completezza dei dati indicati in fattura e della coincidenza tra il soggetto che ha emesso la fattura e il soggetto indicati negli ordini/contratti e dell'approvazione della prestazione da parte della Funzione che ha richiesto il bene/servizio;
- registrazione della fattura a cura del team dell'Accountant previa verifica della completezza dei dati indicati in fattura e della coincidenza tra il soggetto che ha emesso la fattura e il soggetto indicati negli ordini/contratti e dell'approvazione della prestazione da parte della Funzione che ha richiesto il bene/servizio;
- nel caso in cui vengano riscontrati errori o anomalie, il team dell'Accountant contatta il fornitore a cui viene chiesto un documento di rettifica;
- registrazione in contabilità e generazione delle scadenze dei pagamenti (scadenzario) sul sistema informatico;
- autorizzazione al pagamento a cura dell'Amministrazione
- disposizione del pagamento mediante remote banking ;

La gestione dei "**Pagamenti del personale**" si articola nelle seguenti fasi:

- caricamento dei timesheet sulle commesse da parte dei dipendenti;
- verifica dei timesheet da parte del Responsabile di Commessa ed invio dei dati all'Amministrazione
- raccolta dei dati da parte dell'Amministrazione ed invio al consulente del lavoro per la predisposizione dei cedolini;
- predisposizione del pagamento;

Il processo di "**Gestione degli incassi**" si articola nelle seguenti fasi:

- caricamento delle ore/lavoro delle commesse sul sistema informatizzato da parte dei dipendenti mediante timesheet;
- verifica mensile del timesheet da parte del Responsabile di Commessa;

- emissione delle fatture attive sulla base delle indicazioni concordate/previste negli accordi contrattuali, alle scadenze previste e inserimento in contabilità;
- controllo degli incassi giornaliero da parte dell'Amministrazione mediante estrazione dal sistema scadenziario clienti, analisi del credito e sollecito nel caso di ritardi;
- in caso di mancato pagamento, segnalazione all'Amministratore di insoluti ed eventuale attivazione della procedura di recupero crediti (nel caso di crediti scaduti).

Esistenza di procedure/linee guida/prassi operative consolidate

Le attività si svolgono secondo quanto sopra descritto, in conformità ai principi generali di comportamento e controllo.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

La tracciabilità del processo è assicurata dall'impiego, tanto nella gestione dei pagamenti, quanto nella gestione degli incassi, del sistema bancario.

Le operazioni che comportano l'utilizzo o l'impiego di risorse economiche (acquisizione, gestione, trasferimento di denaro e valori) o finanziarie sono inoltre interamente documentate e registrate in conformità ai principi di correttezza gestionale e contabile.

La documentazione rilevante è conservata nel sistema informatico.

Principi di controllo specifici

Nel processo di gestione dei flussi finanziari, tutti i destinatari del presente Modello devono agire nel rispetto delle regole di seguito indicate:

- tutte le operazioni effettuate in contanti, purché di modesto importo e nel rispetto dei limiti di legge, sono annotate in un apposito registro;
- i soggetti autorizzati a intervenire nel processo (i.e. soggetto che autorizza il pagamento, soggetto preposto ad effettuare il pagamento e soggetto preposto al controllo) devono essere chiaramente identificati;
- le operazioni di apertura, gestione e chiusura dei conti correnti bancari e postali (ad es. invio di documentazione, di comunicazioni etc.) sono effettuate da soggetti muniti di appositi poteri o da delegati;
- i movimenti che transitano in addebito sul conto corrente (i.e. pagamento di fatture, etc.) ottengono l'autorizzazione da parte dei soggetti aziendali aventi adeguati poteri, prima di essere effettuati;
- i pagamenti avvengono mediante l'utilizzo del sistema bancario e, in ogni caso, con mezzi che ne garantiscano la tracciabilità;
- gli incassi avvengono mediante l'utilizzo nelle transazioni del sistema bancario;
- i pagamenti e gli incassi ritenuti anomali relativamente a controparte, importo, tipologia, oggetto, frequenza o entità sospette sono sottoposti ad attività di rilevazione e analisi e sono segnalati all'Amministratore prima di procedere al pagamento o alla registrazione contabile;
- sono svolti controlli finalizzati ad assicurare che i pagamenti effettuati siano corrispondenti all'effettiva e completa ricezione dei beni/servizi riportati nella fattura ricevuta;
- viene verificata la piena corrispondenza tra il nome del fornitore cui è indirizzato il pagamento e il soggetto che ha erogato il servizio o la prestazione o che ha venduto i beni;

- possono essere effettuati pagamenti solo nei confronti di soggetti preventivamente registrati in anagrafica fornitori;
- le operazioni che comportano l'utilizzo o l'impiego di risorse economiche (acquisizione, gestione, trasferimento di denaro e valori) o finanziarie sono sempre contrassegnate da una causale espressa, documentate e registrate in conformità ai principi di correttezza gestionale e contabile;
- i pagamenti e gli incassi vengono effettuati/ricevuti nel/dal paese di residenza del soggetto che ha prestato/ha acquistato il bene/servizio o dove è stato eseguito l'incarico;
- viene effettuata periodicamente la verifica sulla corrispondenza di ciascun pagamento e incasso con la documentazione contabile e contrattuale giustificativa.

Famiglie di reato associabili

- Reati contro la Pubblica Amministrazione;
- Reati societari (corruzione tra privati);
- Reati di ricettazione, riciclaggio, autoriciclaggio;
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria;
- Delitti con finalità di terrorismo e di eversione dell'ordine democratico;
- Associazione per delinquere;
- Reati tributari

Flussi informativi verso l'O.d.V.:

A cura dell'Amministrazione:

1. segnalazione tempestiva di ogni modifica organizzativa nell'ambito delle funzioni preposte e/o nelle procure per operazioni finanziarie;
2. elenco dei pagamenti effettuati con indicazione degli importi, del beneficiario e del mezzo di pagamento utilizzato;
3. elenco degli incassi ricevuti con indicazione degli importi, del disponente e del mezzo di pagamento utilizzato.

10.11. GESTIONE DEI RAPPORTI INFRAGRUPPO

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- è obbligatorio definire accordi contrattuali tra le società con indicazione
 - dei criteri di identificazione dei costi;
 - della metodologia di calcolo dei costi;
 - delle tempistiche e le modalità di addebito dei costi dei servizi intercompany.

- è vietato acconsentire all'emissione di fatture e documenti aventi valore fiscale nei confronti di soggetti diversi rispetto agli effettivi acquirenti o beneficiari delle prestazioni o dei servizi resi;
- le operazioni Intercompany che comportano l'utilizzazione o l'impiego di risorse economiche o finanziarie devono avere sempre una causale espressa e devono essere documentate e registrate in conformità ai principi di chiarezza, correttezza professionale e contabile;
- le fatture o i documenti aventi valore fiscale devono sempre riportare la descrizione delle prestazioni eseguite o specifico riferimento alla prestazione sottostante;
- è vietato porre in essere operazioni volte a trasferire i ricavi della Società in paesi ove la tassazione è più favorevole;
- è vietato, altresì, porre in essere operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o altri mezzi fraudolenti al fine di ostacolare l'accertamento fiscale o predisposti per indurre in errore l'amministrazione finanziaria.

Regolamentazione del processo e segregazione dei compiti

Il processo "Gestione dei rapporti infragruppo" si svolge secondo le seguenti fasi:

- decisione sulla opportunità di concludere accordi infragruppo da parte dell'Amministratore;
- definizione del rapporto contrattuale tra le società secondo le indicazioni dell'Amministrazione;
- esecuzione della prestazione da parte dei soggetti interessati secondo quanto previsto nell'accordo contrattuale;
- controllo delle prestazioni da parte dei soggetti interessati;
- monitoraggio sui flussi finanziari intercompany da parte dell'Amministrazione;
- conservazione di tutta la documentazione necessaria a tracciare l'effettività delle prestazioni infragruppo da parte dell'Accountant.

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività sensibile è svolta secondo quanto sopra descritto, in conformità alle disposizioni di legge.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

La documentazione rilevante è registrata ed archiviata a sistema, a cura dell'Accountant.

Principi di controllo specifico

- decisione del compimento dell'operazione infragruppo da parte dell'Amministratore;
- esecuzione delle prestazioni da parte dei soggetti aziendali coinvolti;
- il prezzo di trasferimento è in linea con il valore normale delle prestazioni stesse;
- L'Amministrazione compie una verifica della effettività e correttezza delle prestazioni infragruppo.

Famiglie di reato associabili

- Reati societari;
- Delitti di criminalità organizzata;
- Delitto di autoriciclaggio;
- Reati tributari.

Flussi informativi verso l'O.d.V.:

A cura dell'Accountant:

- elenco dei contratti stipulati infragruppo.

10.12 ELABORAZIONE DEL BILANCIO E DEL RENDICONTO FINANZIARIO E COMUNICAZIONE A STAKEHOLDERS E/O A TERZI DI DATI E INFORMAZIONI RELATIVI ALLA SITUAZIONE ECONOMICA, PATRIMONIALE E FINANZIARIA DELLA SOCIETÀ

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- nella gestione delle attività contabili devono essere osservate le regole di corretta, completa e trasparente contabilizzazione, secondo i criteri indicati dalla legge e dai principi contabili applicabili, in modo tale che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;
- ciascuna registrazione contabile deve riflettere esattamente le risultanze della documentazione di supporto;
- eventuali operazioni straordinarie devono essere poste in essere nel rispetto della disciplina prevista dal Codice Civile;
- nello svolgimento delle attività di verifica e controllo da parte del Revisore è necessario agire con trasparenza, tempestività e prestare la massima collaborazione.

In particolare è fatto divieto di:

- porre in essere operazioni simulate o diffondere notizie false sulla Società e sulle sue attività;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilancio, in relazioni o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della Società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;

- porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte degli organi sociali.

Regolamentazione del processo e segregazione dei compiti

Il processo di “**Elaborazione del bilancio e del rendiconto finanziario e comunicazione a stakeholders e/o a terzi di dati e informazioni relativi alla situazione economica, patrimoniale e finanziaria della società**” si articola come segue:

- estrazione dei dati contabili dal sistema informatico da parte dell'Accountant con il supporto del consulente esterno;
- chiusura dei bilanci di verifica con la supervisione dell'Amministratore;
- verifica periodica da parte del Revisore dei dati contabili e finanziari;
- redazione della proposta di bilancio e della nota integrativa e della relazione sulla gestione da parte dell'Accountant con il supporto del consulente esterno;
- verifica e validazione della proposta di bilancio da parte dell'Amministratore;
- verifica ed esame della proposta di bilancio da parte del Revisore, che redige apposita relazione;
- sottoposizione da parte dell'Amministratore del fascicolo di bilancio all'Assemblea;
- approvazione della proposta di bilancio da parte dell'Assemblea;
- archiviazione della documentazione ad opera dell'Accountant.

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività sensibile è svolta secondo quanto sopra descritto, in conformità alle disposizioni di legge.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

La tracciabilità dei dati e delle informazioni relativi al processo è assicurata dall'impiego di strumenti informatici. La documentazione relativa all'attività è archiviata a cura dell'Accountant.

Principi di controllo specifici

Nel processo in oggetto, i Destinatari devono attenersi alle regole di seguito indicate:

- il sistema informatico utilizzato garantisce la tracciabilità dei dati e delle informazioni;
- ogni modifica ai dati contabili è effettuata dall'Accountant tenuto conto della documentazione su input del Responsabile di Funzione che li ha generati, garantendo la tracciabilità dell'operazione di modifica;
- il personale coinvolto nella predisposizione del bilancio segue le modalità operative indicate dalla Società, in conformità alle disposizioni della normativa civilistica e fiscale in materia;
- l'Accountant inserisce a sistema i dati necessari alla redazione del bilancio, garantendo la completezza e la veridicità degli stessi;
- le Funzioni coinvolte nella redazione del bilancio e dei documenti connessi partecipano ad attività di formazione di base (in merito alle principali nozioni e problematiche giuridiche e contabili sul bilancio);
- la Società, anche mediante i consulenti esterni, definisce regole formalizzate che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall'approvazione del progetto da parte dell'Amministrazione al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione;

- i soggetti responsabili del processo pongono in essere tutte le attività necessarie per il monitoraggio delle informazioni contenute nei sistemi contabili e gestionali dando evidenza documentale delle attività poste in essere.

Famiglie di reato associabili

- Reati societari;
- Reati di ricettazione, riciclaggio e auto riciclaggio;
- Associazione per delinquere;
- Reati tributari

Flussi informativi verso l'O.d.V.:

A cura dell'Amministrazione:

- trasmissione di copia del fascicolo di bilancio e del verbale di approvazione dello stesso.

10.13. PREDISPOSIZIONE DI DICHIARAZIONI DEI REDDITI O DI SOSTITUTI D'IMPOSTA O DI ALTRE DICHIARAZIONI FUNZIONALI ALLA LIQUIDAZIONE DI TRIBUTI IN GENERE

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- i dati contenuti nelle dichiarazioni devono rispecchiare fedelmente quanto riportato nella documentazione sottostante alle stesse;
- nella gestione delle attività contabili devono essere osservate le regole di corretta, completa e trasparente contabilizzazione, secondo i criteri indicati dalla legge e dai principi contabili applicabili, in modo tale che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;
- ciascuna registrazione contabile deve riflettere esattamente le risultanze della documentazione di supporto. Pertanto, sarà compito delle funzioni a ciò preposte assicurare che la documentazione di supporto sia facilmente reperibile e ordinata secondo criteri logici;
- nello svolgimento delle attività di verifica e controllo del Revisore è necessario agire con trasparenza e prestare la massima collaborazione,
- in caso di verifiche da parte di organi ispettivi è vietato compiere atti corruttivi.

È fatto espresso divieto di:

- utilizzare nelle dichiarazioni sui redditi o sul valore aggiunto fatture o altri documenti relativi ad operazioni non effettivamente svolte, che descrivano genericamente l'oggetto della prestazione (o che non lo descrivano affatto) o che non siano attribuibili all'emittente del documento;
- porre in essere comportamenti che, mediante l'occultamento o la distruzione in tutto o in parte delle scritture contabili o dei documenti di cui è obbligatoria la conservazione, non consentano all'amministrazione finanziaria la ricostruzione dei redditi o del volume d'affari;
- violare le norme in materia tributaria, fiscale e previdenziale.

Regolamentazione del processo e segregazione dei compiti

Il processo di "Predisposizione di dichiarazioni dei redditi o di sostituti d'imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere" si articola nelle seguenti macro attività:

- reperimento da parte dell'Accountant dei dati contabili/tributari/fiscali;
- elaborazione dei dati utili per la redazione delle dichiarazioni da parte dei consulenti esterni (consulente del lavoro);
- predisposizione delle bozze delle dichiarazioni e degli F24 a cura dei consulenti esterni;
- sottoscrizione delle dichiarazioni da parte del Legale Rappresentante e controllo da parte del Revisore;
- invio telematico da parte del consulente esterno incaricato dalla Società;
- deposito delle dichiarazioni da parte del consulente esterno;
- pagamento su autorizzazione dell'Amministrazione;
- intervento in caso di visite ispettive relative all'attività da parte dell'Amministratore ed eventualmente del consulente esterno incaricato.

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività sensibile è svolta secondo quanto sopra descritto, in conformità ai principi generali di comportamento e controllo.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

La tracciabilità è garantita dall'archiviazione della documentazione relativa al processo, che avviene a cura dell'Accountant e del consulente del lavoro, ciascuno con riferimento alla propria area di competenza.

Principi di controllo specifici

Nel processo in oggetto, tutti i Destinatari devono attenersi alle regole di seguito indicate:

- è svolta dalle Funzioni e dai consulenti competenti una verifica sulla correttezza dei dati contenuti nelle dichiarazioni e nei prospetti di liquidazione delle imposte;
- nel caso di esposizione di crediti d'imposta, la Società si avvale di un consulente che fornisce perizia giurata sulla veridicità e correttezza delle somme portate a credito; tale perizia viene verificata anche dal Revisore;
- è sempre effettuata la verifica sulla corrispondenza tra le certificazioni rilasciate quale sostituto d'imposta e le relative dichiarazioni e versamenti;

- nel caso di anomalie rispetto a fatture registrate in contabilità, viene svolta un'approfondita valutazione documentata e una decisione motivata circa la decisione di apportare "riprese" in sede di presentazione della dichiarazione;
- è verificata la tempestiva liquidazione delle imposte della Società da parte dell'Amministratore e del Revisore;
- i consulenti esterni si occupano di monitorare l'evoluzione normativa e giurisprudenziale in materia fiscale e tributaria, nonché gli interventi relativi all'interpretazione e alla corretta applicazione delle norme tributarie.
- i rapporti con i consulenti esterni sono regolati da una lettera d'incarico che indica l'attività da espletare e prevedono apposite clausole che richiamano gli adempimenti e le responsabilità derivanti dal Decreto e dal rispetto del Modello e del Codice Etico.

Famiglie di reato associabili

- Reati societari;
- Reati contro la Pubblica Amministrazione;
- Reati di ricettazione, riciclaggio e auto riciclaggio;
- Associazione per delinquere;
- Reati tributari

Flussi informativi verso l'O.d.V.:

A cura dell'Amministrazione:

- trasmissione delle dichiarazioni e dell'attestazione della presentazione delle stesse nonché dei pagamenti effettuati.

10.14. GESTIONE DELLE RISORSE INFORMATICHE

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- è richiesto di custodire i codici identificativi assegnati, astenendosi dal comunicarli a terzi non autorizzati;
- è richiesto di astenersi da qualsiasi condotta che possa compromettere la sicurezza, riservatezza e integrità delle informazioni e dei dati aziendali contenuti nel sistema informatico;
- è richiesto di astenersi da qualsiasi condotta diretta ad aggirare le protezioni del sistema informatico aziendale o altrui;
- nel caso di attività di gestione dei sistemi informativi e del patrimonio informativo date in outsourcing, i contratti devono contenere espresse previsioni che il fornitore operi in conformità alla normativa vigente.
- è vietato introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza o permanervi contro la volontà del titolare del diritto all'accesso;
- è vietato accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati aziendali e/o esterne, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- è vietato utilizzare dispositivi o software non autorizzati per impedire o interrompere le comunicazioni di un sistema informatico o telematico o intercorrenti tra più sistemi;
- è vietato installare programmi provenienti dall'esterno, salvo espressa autorizzazione ed in particolare:
 - software non approvati;
 - software aziendali in violazioni delle licenze d'uso.
- è vietato installare e/o modificare componenti hardware o utilizzare strumenti software e/o hardware atti a distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente Pubblico o ad essi pertinenti o comunque di pubblica utilità;
- è vietato introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- è vietato detenere, procurarsi, riprodurre, o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso ad un sistema protetto da misure di sicurezza;
- è vietato procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- è vietato alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
- è vietato produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;

- è vietato distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità.

Regolamentazione del processo e segregazione dei compiti

Il processo di “**Gestione delle risorse informatiche**” presenta le caratteristiche di seguito indicate:

- l'inventario delle risorse informatiche di proprietà della Società nonché delle licenze software è tenuto a cura dell'Amministrazione;
- gli elaboratori vengono forniti completi dei *software* utili all'espletamento dell'attività dal fornitore;
- la configurazione dei computer viene effettuata dal dipendente sulla base di apposite istruzioni fornite dalla Società;
- i dispositivi sono protetti da *user id* e *password* (da modificare al primo utilizzo e a cadenze regolari) e sono adottati presidi per la sicurezza dei dati (ad es. antivirus, *antimalware* e *firewall*);
- la gestione dei domini e-mail della Società è a cura di un provider esterno ed è su piattaforma in cloud con dominio dedicato alla Società;
- i dati della Società vengono memorizzati su *server* esterni il cui accesso è disciplinato mediante profilazione delle utenze in base al ruolo ricoperto;
- gli accessi su sistemi di terzi (ad es. clienti) sono regolamentati dai titolari del potere di autorizzazione dell'accesso ai sistemi stessi;

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività sensibile è svolta secondo quanto sopra descritto. La prassi è conosciuta da tutti coloro che intervengono.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

Il processo decisionale è documentato e la documentazione viene archiviata dalle funzioni che intervengono nel processo, ognuna per la propria competenza.

Principi di controllo specifici

Nel processo in oggetto, i Destinatari devono attenersi alle regole di seguito indicate:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per esigenze di lavoro;
- non trasferire e/o trasmettere all'esterno della Società file, documenti o qualsiasi altra documentazione riservata di proprietà di Major Bit se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione dell'Amministrazione
- evitare di lasciare incustodito e/o accessibile ad altri il proprio PC, oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, ecc.);
- utilizzare la connessione a internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività lavorative che hanno reso necessario il collegamento;
- i titolari di un certificato di firma elettronica/elettronica qualificata/digitale sono tenuti ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; sono altresì tenuti ad utilizzare personalmente il dispositivo di firma;

- astenersi dall'operare sui sistemi dei clienti qualora fossero revocate le autorizzazioni per l'accesso;
- astenersi dal modificare dati di proprietà del cliente senza necessaria autorizzazione;
- non abusare di informazioni apprese da clienti in occasione dello svolgimento dell'incarico e non utilizzare dati di proprietà di terzi senza le necessarie autorizzazioni.

Famiglie di reato associabili

- Reati informatici;
- Reati contro la Pubblica Amministrazione;
- Delitti in materia di violazione del diritto d'autore.

Flussi informativi verso l'O.d.V.:

A cura della Direzione:

-eventuali anomalie riscontrate nella gestione delle licenze *software*, degli accessi ai sistemi ed alle dotazioni informatiche della Società.

10.15. GESTIONE DEGLI ADEMPIMENTI IN MATERIA AMBIENTALE

Principi comportamentali generali

I Destinatari, a qualsiasi titolo coinvolti nel processo in esame, sono tenuti ad osservare le modalità di esecuzione indicate nella presente sezione, le previsioni di legge esistenti in materia, i principi richiamati nel Codice Etico e le regole del presente Modello.

Pertanto:

- è obbligatorio provvedere alla qualifica dei fornitori di servizi ambientali;
- è obbligatorio rispettare le leggi applicabili in materia.

Regolamentazione del processo e segregazione dei compiti

Il processo di “**Gestione degli adempimenti in materia ambientale**” presenta le caratteristiche di seguito indicate:

- la Società svolge attività di ufficio e i rifiuti prodotti vengono smaltiti come rifiuti urbani;
- i toner vengono affidati a fornitori esterni che si occupano dello smaltimento;
- nel caso di lavori dati in appalto esistono previsioni contrattuali che pongono a carico dell'appaltatore le azioni necessarie sui rifiuti prodotti.

Esistenza di procedure/linee guida/prassi operative consolidate

L'attività è svolta attraverso fornitori esterni, sulla base di accordi contrattuali.

Tracciabilità e verificabilità ex post delle attività tramite adeguati supporti documentali/informatici

Il processo decisionale è documentato e la documentazione viene archiviata dalle funzioni che intervengono nel processo, ognuna per la propria competenza.

La Società provvede ad archiviare i contratti con i fornitori e tutta la documentazione rilevante.

La Società ha implementato un Sistema di gestione aziendale integrato per la qualità sulla base delle norme UNI EN ISO 9001

Principi di controllo specifici

Nel processo in oggetto, i Destinatari devono attenersi alle regole di seguito indicate:

- prima della stipula del contratto, nonché in corso di esecuzione, i soggetti deputati verificano il possesso/il mantenimento dei requisiti da parte dei fornitori di servizi ambientali;
- i rapporti con i fornitori di servizi ambientali sono formalizzati e prevedono l'inserimento di una clausola con la quale si chiede l'impegno al rispetto del Codice Etico e del D.Lgs. 231/2001;
- sono individuati i soggetti che intervengono nella gestione delle tematiche ambientali;

Famiglie di reato associabili

- Reati ambientali;
- Reati contro la Pubblica Amministrazione;
- Associazione per delinquere.

Flussi informativi verso l'O.d.V.:

A cura dell'Amministrazione:

- copia dei contratti stipulati con i fornitori di servizi ambientali.

10.16. GESTIONE DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO

Regolamentazione del processo e segregazione dei compiti

1. Politica della sicurezza

La politica in materia di salute e sicurezza nei luoghi di lavoro è definita all'interno del Documento di Valutazione dei Rischi.

2. Piano degli investimenti

In relazione ad eventuali investimenti in materia di salute e sicurezza nei luoghi di lavoro, la Direzione, in collaborazione con il RSPP, approva gli interventi da effettuare sulle diverse sedi.

3. Aggiornamento normativo

L'aggiornamento in materia di legislazione nazionale e locale in tema di salute e sicurezza sui luoghi di lavoro viene effettuato dal RSPP che individua quanto di interesse per la Società e lo comunica all'ASPP per la relativa valutazione e per l'eventuale segnalazione al Datore di Lavoro al fine dell'adeguamento.

Per una comunicazione efficace si favorisce l'accesso a fonti istituzionali e si prediligono informazioni semplici e vive (ad esempio infografiche). Con riferimento a particolari situazioni di emergenza, come ad esempio il

rischio biologico transitorio in occasione di pandemie, il RSPP coinvolge il Medico Competente nell'individuazione delle informazioni più adeguate.

4. Norme e documentazione del sistema (Acquisizione di documentazioni e certificazioni obbligatorie)

La Società ha attuato le iniziative volte a conformarsi alle previsioni normative in materia di sicurezza sul lavoro, tra cui il D.Lgs. n. 81 del 2008.

L'ASPP, formalmente individuato, si occupa della gestione e dell'archiviazione della documentazione rilevante in materia di salute e sicurezza sui luoghi di lavoro.

5. Organizzazione e responsabilità

L'Amministratore è stato individuato Datore di Lavoro ai sensi dell'art. 2 del D.Lgs. 81/2008.

È stato designato un Responsabile del Servizio di Prevenzione e Protezione e un ASPP.

È stato nominato un Medico Competente il quale effettua la sorveglianza sanitaria.

Sono stati eletti i Responsabili dei lavoratori per la sicurezza;

Sono stati formalmente individuati e formati i Dirigenti in materia di salute e sicurezza.

Sono stati formalmente incaricati gli addetti per il pronto soccorso e l'antincendio; tali figure hanno ricevuto un'idonea formazione secondo quanto previsto dalla normativa applicabile.

6. Sistema di deleghe di funzione

Il Datore di Lavoro non ha ritenuto necessario assegnare deleghe in materia di salute e sicurezza nei luoghi di lavoro.

7. Documento di Valutazione dei Rischi

Il Datore di Lavoro, con l'ausilio del RSPP, del Medico Competente e del ASPP e con il coinvolgimento del RLS ha adottato un Documento di Valutazione dei Rischi ("DVR") per ciascuna sede in cui si svolge l'attività della Società.

I DVR sono soggetti ad aggiornamento periodico. All'interno dei documenti è presente l'organigramma in materia di salute e sicurezza.

Il Datore di Lavoro, con il supporto del RSPP e del Medico Competente, aggiorna le valutazioni del rischio anche in particolari situazioni di emergenza nell'ambito delle quali il fattore da cui scaturisce il rischio sia esterno all'azienda e non dipenda dalla tipologia di attività svolta (ad es. rischio esogeno).

Nel caso di lavori effettuati da soggetti terzi viene redatto un apposito DUVRI e alla valutazione dei rischi interferenziali viene chiamato a partecipare anche il RSPP. La documentazione rilevante è conservata a cura dell'ASPP.

Nel caso di lavori presso il committente, i dipendenti di Major Bit seguono le istruzioni e procedure che lo stesso committente mette a disposizione. Il DUVRI del committente viene completato previo confronto con il referente per la sicurezza (DL/RSPP) della Società.

8. Gestione delle emergenze e del rischio incendio

La Società ha adottato e formalizzato il piano di emergenza che contiene le istruzioni per l'abbandono degli uffici in caso di emergenza, il programma degli interventi e le modalità di cessazione dell'attività lavorativa.

Le prove di emergenza sono pianificate sulla base del programma stabilito dal gestore del building, verbalizzate e vengono svolte con cadenza annuale.

I lavoratori hanno ricevuto specifiche informazioni in merito alle modalità di abbandono del luogo di lavoro in caso di pericolo grave.

Gli addetti antincendio, evacuazione e primo soccorso hanno frequentato appositi corsi, così come previsto dalla normativa in materia.

Le misure antincendio sono definite all'interno di un apposito documento di cui viene dato atto all'interno del DVR.

La Società inoltre stabilisce, attua e mantiene attive una o più procedure per:

- a) identificare le potenziali situazioni di emergenza (ulteriori rispetto a quelle relative ad eventi legati a calamità naturali o incendi);
- b) rispondere a tali situazioni di emergenza.

9. Consultazione e comunicazione

La Società ha previsto almeno una riunione periodica all'anno tra tutte le Funzioni competenti in materia di salute e sicurezza sul lavoro.

10. Informazione e formazione

Tutti i lavoratori della Società sono informati in merito a tutte le figure rilevanti in materia di salute e sicurezza nei luoghi di lavoro, nonché ai rischi esistenti nell'ambiente aziendale.

L'informazione ai lavoratori in merito ai rischi aziendali viene fornita attraverso la messa a disposizione della documentazione rilevante e dei riferimenti normativi, al momento dell'assunzione, in caso di attivazione del lavoro in modalità *smart working*, e periodicamente a seguito delle evidenze e tematiche emerse nel corso delle riunioni periodiche per la sicurezza.

11. Sorveglianza sanitaria, monitoraggio e azioni correttive

Il Medico Competente collabora con il Datore di Lavoro e con il SPP per la valutazione dei rischi, anche ai fini della programmazione della sorveglianza sanitaria, e per la predisposizione delle misure per la tutela della salute dei lavoratori.

In particolari situazioni di emergenza sanitaria, il Medico Competente suggerisce l'adozione di specifiche misure di prevenzione, quali l'utilizzo di appositi DPI ed eventuali mezzi diagnostici, qualora ritenute utili al fine di tutelare maggiormente la salute dei lavoratori.

Il Medico Competente segnala altresì alla Società eventuali situazioni di particolare fragilità tra i dipendenti e supporta il Datore di Lavoro nell'attività di formazione e informazione dei lavoratori.

La documentazione relativa al controllo periodico del Medico Competente è archiviata presso la Società.

12. Gestione degli asset

Le verifiche periodiche sui luoghi di lavoro sono svolte da RSPP, che esegue controlli sullo stato di manutenzione dei locali e degli ambienti di lavoro, delle attrezzature e dei DPI.

13. Controllo e azioni correttive – monitoraggio delle prestazioni

La Società definisce i criteri, le modalità, i compiti, le responsabilità e le periodicità degli *audit* interni del sistema di gestione salute e sicurezza così da poter determinare se il sistema risulta conforme, implementato ed efficace per il conseguimento della politica e degli obiettivi dell'organizzazione.

Il RSPP effettua il monitoraggio degli infortuni, nonché la rilevazione, registrazione ed analisi statistica degli infortuni.

Flussi informativi verso l'O.d.V.:

A cura del RSPP:

1. segnalazione di eventuali infortuni sul lavoro;
2. verbale della riunione periodica in materia di sicurezza;
3. indicazione dei procedimenti disciplinari per violazioni della normativa in materia di salute e sicurezza nei luoghi di lavoro.

10.17. Gestione dei rischi informatici e cybersecurity

La Società riconosce la rilevanza dei rischi connessi alla sicurezza informatica e alla protezione dei dati, anche in relazione ai reati previsti dall'art. 24-bis del D.Lgs. 231/2001.

A tal fine, la Società adotta misure organizzative e tecniche idonee a:

- prevenire accessi non autorizzati ai sistemi informativi;
- garantire l'integrità, la disponibilità e la riservatezza dei dati;
- monitorare e gestire eventuali incidenti informatici;
- assicurare la tracciabilità delle operazioni effettuate sui sistemi.

Sono altresì previsti specifici protocolli per la gestione degli accessi, delle credenziali, dei backup e delle attività di sviluppo software.

NOTE

-1 Il D. Lgs. 231/2001 è pubblicato sulla Gazzetta Ufficiale del 19 giugno 2001, n. 140, la Legge 300/2000 sulla Gazzetta Ufficiale del 25 ottobre 2000, n. 250.

-2 Art. 5, comma 1, del d.lgs. 231/2001: “Responsabilità dell’ente – L’ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell’ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;
- b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)”.

-3 Si tratta dei reati seguenti: malversazione a danno dello Stato o dell’Unione europea (art. 316-bis c.p.), indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.), truffa aggravata a danno dello Stato (art. 640, comma 2, n. 1, c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.), frode informatica a danno dello Stato o di altro ente pubblico (art. 640-ter c.p.), corruzione per l’esercizio della funzione (artt. 318, 319 e 319-bis c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), corruzione in atti giudiziari (art. 319-ter c.p.), istigazione alla corruzione (art. 322 c.p.), concussione (art. 317 c.p.), induzione indebita a dare o promettere utilità (art. 319-quater c.p.); corruzione, istigazione alla corruzione e concussione di membri delle Comunità europee, funzionari delle Comunità europee, degli Stati esteri e delle organizzazioni pubbliche internazionali (art. 322-bis c.p.). La Legge novembre 2012, n. 190 ha introdotto nel Codice Penale e richiamato nel Decreto la previsione di cui all’art. 319-quater rubricato “Induzione indebita a dare o promettere utilità”.

Con la Legge n. 69 del 27 maggio 2015, è stata modificata la disciplina sanzionatoria in materia di delitti contro la Pubblica Amministrazione con la previsione di pene sanzionatorie più rigide per i reati previsti dal Codice Penale. È stato altresì modificato l’art. 317 c.p. “Concussione”, che prevede ora – come soggetto attivo del reato – anche l’Incaricato di Pubblico Servizio oltre al Pubblico Ufficiale. La Legge 9 gennaio 2019, n. 3 ha introdotto all’interno dell’art. 25 D.Lgs. 231/2001 anche il reato di traffico di influenze illecite (art. 346-bis c.p.).

Da ultimo, l’art. 5 del D. Lgs. 75/2020 di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell’Unione mediante il diritto penale, ha integrato il catalogo dei reati presupposto dell’art. 24 del D.Lgs. 231/2001 con il reato di “frode nelle pubbliche forniture” (art. 356 c.p.) e “frode in agricoltura” (art. 2 L. 898/1986 in materia di aiuti comunitari nel settore agricolo); inoltre l’Unione Europea è stata inserita nel novero dei soggetti ai danni dei quali è compiuto il reato che dà origine alla responsabilità dell’ente. Il medesimo decreto ha altresì modificato l’art. 25 del D. Lgs. 231/2001 inserendo tra i reati presupposto della responsabilità amministrativa degli enti i reati di “peculato” (art. 324 co.1 c.p.), “peculato mediante profitto dell’errore altrui” (art. 316 c.p.) e “abuso di ufficio” (art. 323 c.p.) quando il fatto offende gli interessi finanziari dell’Unione europea.

-4 L’art. 24-bis è stato introdotto nel D.Lgs. 231/2001 dall’art. 7 della legge 48/2008. Si tratta dei reati di falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.), diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.), intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.), installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.), danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.), danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.), danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.), danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.) e frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.). Il D.L. 21 settembre 2019 n. 105, recante “Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica” (c.d. “Decreto Cybersecurity”), convertito con Legge n. 133 del 2019, ha inserito all’interno dell’art. 24 bis del Decreto una nuova fattispecie di reato che punisce le condotte di ostacolo e di false dichiarazioni tenute verso nuove Authority incaricate di vigilare sulla sicurezza informatica.

-5 L’art. 24-ter è stato introdotto nel d.lgs. 231/2001 dall’art. 2 comma 29 della Legge 15 luglio 2009, n. 94. Con il D.Lgs. n. 21 del 1° marzo 2018 è stato abrogato l’art. 22 bis della L. 91/1999, che rappresenta una delle condotte illecite contemplate all’art. 416 c.p. ed è stata inserita la relativa fattispecie di reato all’interno del nuovo articolo 601 bis c.p. (traffico di organi prelevati da persona vivente). La Legge 21 maggio 2019, n. 43 ha modificato il reato di scambio elettorale politico-mafioso (art. 416-ter c.p.), in particolare estendendo la punibilità anche ai casi in cui la condotta incriminata sia stata realizzata mediante il ricorso ad intermediari e ampliando l’oggetto della controprestazione di chi ottiene la promessa di voti, che può consistere non solo nel denaro e ogni altra utilità, ma anche nella disponibilità a soddisfare gli interessi o le esigenze della associazione mafiosa.

-6 L’art. 25-bis è stato introdotto nel d.lgs. 231/2001 dall’art. 6 del D.L. 350/2001, convertito in legge, con modificazioni, dall’art. 1 della L. 409/2001. Si tratta dei reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.), alterazione di monete (art. 454 c.p.), spendita 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.). La previsione normativa è stata poi estesa anche alla contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art.

473 c.p.), e all'introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.) con la modifica introdotta dall'art. 17 co. 7 lettera a) n. 1) della legge 23 luglio 2009.

-7 L'art. 25-bis.1. è stato inserito dall'art. 17, comma 7, letterab), della legge 23 luglio 2009, n. 99; si tratta in particolare dei delitti di turbata libertà dell'industria o del commercio (art. 513 c.p.), illecita concorrenza con minaccia o violenza (art. 513-bis), 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), contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater).

-8 L'art. 25-ter è stato introdotto nel d.lgs. 231/2001 dall'art. 3 del d.lgs. 61/2002. Si tratta dei reati di false comunicazioni sociali e false comunicazioni sociali in danno dei soci o dei creditori (artt. 2621 e 2622 c.c.), impedito controllo (art. 2625, 2° comma, c.c.), formazione fittizia del capitale (art. 2632 c.c.), indebita restituzione dei conferimenti (art. 2626 c.c.), illegale ripartizione degli utili e delle riserve (art. 2627 c.c.), illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.), operazioni in pregiudizio dei creditori (art. 2629 c.c.), omessa comunicazione del conflitto di interessi (art. 2629 bis c.c.), indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.), corruzione tra privati (art. 2635 c.c.), istigazione alla corruzione tra privati (art. 2635 bis c.c.), illecita influenza sull'assemblea (art. 2636 c.c.), aggio (art. 2637 c.c.), ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.). Il d.lgs. 39/2010 ha abrogato la previsione dell'art. 2624 c.c. rubricato falsità nelle relazioni o nelle comunicazioni delle società di revisione che è stato così espunto anche dal d.lgs. 231/2001. L'art. 2635 c.c. rubricato "Corruzione tra privati" è stato introdotto nel Decreto ad opera della Legge 6 novembre 2012, n. 190. Con la L. n. 69 del 2015, recante "Disposizioni in materia di delitti contro la Pubblica Amministrazione, di associazioni di tipo mafioso e di falso in bilancio", sono stati modificati i reati p. e p. dagli artt. 2612 e 2622 c.c.; in particolare, è stata eliminata la precedente soglia di punibilità del falso in bilancio e prevista una specifica responsabilità per amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili, sindaci, liquidatori delle società quotate o che si affacciano alla quotazione, che controllano società emittenti strumenti finanziari quotati o che fanno appello al pubblico risparmio. È stato altresì introdotto l'art. 2621-bis c.c. "Fatti di lieve entità", per la commissione delle condotte di cui all'art. 2621 c.c. caratterizzate da lieve entità tenuto conto della natura, delle dimensioni della società e delle modalità e degli effetti della condotta e dell'art. 2621-ter c.c. che prevede una causa di non punibilità per fatti di particolare tenuità.

Con riferimento all'art. 2621 così come modificato, le SS.UU. hanno statuito che «*sussiste il delitto di false comunicazioni sociali, con riguardo all'esposizione o all'ammissione di fatti oggetto di valutazione, se, in presenza di criteri di valutazione normativamente fissati o di criteri tecnici generalmente accettati, l'agente da tali criteri si discosti consapevolmente e senza darne adeguata informazione giustificativa, in modo concretamente idoneo a indurre in errore i destinatari delle comunicazioni*», pertanto dando una interpretazione estensiva rispetto alla lettera della legge consentendo una applicazione più ampia del precetto normativo.

Il D.Lgs. n. 38/2017 ha apportato modifiche all'art. 2635 c.c. (corruzione tra privati) e ha introdotto l'art. 2635-bis rubricato "istigazione alla corruzione tra privati". È stata inoltre introdotta la pena accessoria della interdizione temporanea dagli uffici direttivi delle persone giuridiche per chi venga condannato per la commissione degli art. 2635 e 2635 bis c.c. (art. 2635-ter c.c.). Infine, l'art. 6 del menzionato decreto prevede modifiche anche all'art. 25-ter del D.Lgs. 231/2001 che andrà a comprendere oltre l'art. 2635 c.c. anche l'art. 2635-bis c.c.

-9 L'art. 25-quinquies è stato introdotto nel d.lgs. 231/2001 dall'art. 5 della legge 11 agosto 2003, n. 228. Si tratta dei reati di riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.), tratta di persone (art. 601 c.p.), acquisto e alienazione di schiavi (art. 602 c.p.), reati connessi alla prostituzione minorile e allo sfruttamento della stessa (art. 600-bis c.p.), alla pornografia minorile e allo sfruttamento della stessa (art. 600-ter c.p.), detenzione di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori (art. 600-quater c.p.), iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.). L'art. 3, comma 1 del d.lgs. 4 marzo 2014, n. 39 ha introdotto, all'art. 25 – quinquies, co. 1, lett. c) del Decreto, il richiamo al reato di adescamento di minorenni (art. 609 – undecies c.p.).

Da ultimo, la legge 29 ottobre 2016, n. 199, ha inserito in tale articolo il riferimento all'art. 603-bis c.p. come modificato dalla medesima legge, con la conseguenza che il reato di caporalato dalla stessa riformulato ("intermediazione illecita e sfruttamento del lavoro") è divenuto reato presupposto della responsabilità degli enti.

L'art. 25-quater.1 è stato introdotto dalla legge 9 gennaio 2006 n. 7 e si riferisce al delitto di mutilazione di organi genitali femminili (art. 583 bis c.p.).

-10 L'art. 25-sexies è stato introdotto nel d.lgs. 231/2001 dall'art. 9, comma 3, della legge 62/2005. Si tratta dei reati di abuso di informazioni privilegiate (art. 184 d.lgs. 58/1998) e manipolazione del mercato (art. 185 d.lgs. 58/1998). Il D.lgs. 10 agosto 2018, n. 107: ha ampliato la lett. b del co. 1 dell'art. 184 D. Lgs. 58/98, prevedendo la punizione del soggetto che comunica informazioni privilegiate ad altri anche "al di fuori di un sondaggio di mercato effettuato ai sensi dell'articolo 11 del regolamento (UE) n. 596/2014". Inoltre, ha introdotto il co. 3 bis: nel caso di operazioni relative agli strumenti finanziari di cui all'articolo 180, comma 1, lettera a), numeri 2), 2-bis) e 2-ter), limitatamente agli strumenti finanziari il cui prezzo o valore dipende dal prezzo o dal valore di uno strumento finanziario di cui ai numeri 2) e 2-bis) ovvero ha un effetto su tale prezzo o valore, o relative alle aste su una piattaforma d'asta autorizzata come un mercato regolamentato di quote di emissioni, la sanzione penale è quella dell'ammenda fino a euro 103.291 e dell'arresto fino a tre anni; ha introdotto, con riferimento all'art. 185 D.lgs. 58/98 una causa di non punibilità per chi ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse. Inoltre ha previsto che l'applicazione della disposizione anche ai fatti concernenti gli indici di riferimento (benchmark).

-11 I reati transnazionali non sono stati inseriti direttamente nel d.lgs. 231/2001 ma tale normativa è ad essi applicabile in base all'art.10 della legge 146/2006. Ai fini della predetta legge si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

- a) sia commesso in più di uno Stato;
- b) sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro stato;
- c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato. Si tratta dei reati di associazione per delinquere (art. 416 c.p.), associazione di tipo mafioso (art. 416-bis c.p.), associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-*quater* d.p.r. 43/1973), associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 d.p.r. 309/1990), disposizioni contro le immigrazioni clandestine (art. 12, co. 3, 3-*bis*, 3-*ter* e 5 d.lgs. 286/1998), induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.) e favoreggiamento personale (art. 378 c.p.).

-12 L'art. 25-*septies* d.lgs. 231/01 è stato introdotto dalla legge 123/07. Si tratta dei reati di omicidio colposo e lesioni colpose, gravi o gravissime commessi con la violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (artt. 589 e 590, co. 3, c.p.). La L. n. 3/2018 ha esteso l'applicazione di tali reati a chi esercita in maniera abusiva una professione sanitaria.

-13 L'art. 25-*octies* è stato introdotto nel d.lgs. 231/2001 dall'art. 63, comma 3, del d.lgs. 231/07. Si tratta dei reati di ricettazione (art. 648 c.p.), riciclaggio (art. 648-*bis* c.p.), impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.), nonché autoriciclaggio (648-*ter*.1 c.p.) introdotto dalla L. n. 186/2014.

-14 L'art. 25-*nonies* è stato introdotto con Legge 23 luglio 2009 n. 99 "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia" e prevede l'introduzione del decreto degli artt. 171 primo comma lett. a), terzo comma, 171 *bis*, 171 *ter*, 171 *septies* e 171 *octies* della L. 22 aprile 1941 n. 633 in tema di "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio".

-15 L'art. 25-*decies* è stato inserito dall'articolo 4, comma 1, della legge 3 agosto 2009, n. 116 che ha introdotto nelle previsioni del d.lgs. 231/2001 l'art. 377-*bis* del codice penale rubricato "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria".

-16 L'art. 25-*undecies* è stato inserito dall'art. 2 del d.lgs. 7 luglio 2011 n. 121 che ha introdotto nelle previsioni del d.lgs. 231/2001 talune fattispecie sia nelle forme delittuose (punibili a titolo di dolo) che in quelle contravvenzionali (punibili anche a titolo di colpa), tra cui:

- 1) art. 137 d.lgs. 152/2006 (T.U. Ambiente): si tratta di violazioni in materia di autorizzazioni amministrative, di controlli e di comunicazioni alle Autorità competenti per la gestione degli scarichi di acque reflue industriali;
- 2) art. 256 d.lgs. 152/2006: si tratta di attività di raccolta, trasporto, recupero, smaltimento o, in generale, di gestione di rifiuti non autorizzate in mancanza di autorizzazione o in violazione delle prescrizioni contenute nelle autorizzazioni;
- 3) art. 257 d.lgs. 152/2006: si tratta di violazioni in materia di bonifica dei siti che provocano inquinamento del suolo, del sottosuolo e delle acque superficiali con superamento delle concentrazioni della soglia di rischio;
- 4) art. 258 d.lgs. 152/2006: si tratta di una fattispecie delittuosa, punita a titolo di dolo, che sanziona la condotta di chi, nella predisposizione di un certificato di analisi dei rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti ed a chi fa uso di un certificato falso durante il trasporto;
- 5) artt. 259 e 260 d.lgs. 152/2006: si tratta di attività volte al traffico illecito di rifiuti sia in forma semplice che organizzata;
- 6) art. 260 *bis* d.lgs. 152/2006: si tratta di diverse fattispecie delittuose, punite a titolo di dolo, concernenti il sistema informatico di controllo della tracciabilità dei rifiuti (SISTRI), che reprimono le condotte di falsificazione del certificato di analisi dei rifiuti, di trasporto di rifiuti con certificato in formato elettronico o con scheda cartacea alterati;
- 7) art. 279 d.lgs. 152/2006: si tratta delle ipotesi in cui, nell'esercizio di uno stabilimento, vengano superati i valori limite consentiti per le emissioni di sostanze inquinanti e ciò determini anche il superamento dei valori limite di qualità dell'aria.

Con il Disegno di Legge n. 1345 sugli "Ecoreati", approvato definitivamente il 19 maggio 2015, è stato aggiunto al libro secondo del codice penale il Titolo VI-*bis* "Dei delitti contro l'ambiente". Ai sensi dell'art. 1 del DDL, sono inseriti – nel novero dei reati presupposto della responsabilità amministrativa degli enti – i seguenti reati ambientali:

- 1) art.452-*bis* c.p. "Inquinamento ambientale";
- 2) art. 452-*ter* "Disastro ambientale";
- 3) art. 452-*quater* "Delitti colposi contro l'ambiente";
- 4) art. 452-*quater* "Traffico e abbandono di materiale ad alta radioattività";
- 5) art. 452-*septies* "Circostanze aggravanti" per il reato di associazione per delinquere *ex* art. 416 c.p.

-17 L'art. 25-*duodecies* è stato inserito dall'art. 2 del Decreto Legislativo 16 luglio 2012, n. 109 che ha introdotto nelle previsioni del Decreto il delitto previsto dall'art. 22, comma 12-*bis*, del decreto legislativo 25 luglio 1998, n. 286.

La Legge 17 ottobre 2017 n. 161 ha inserito all'art. 25-*duodecies* del D.Lgs. 231/01 il riferimento ai delitti di cui all'art. 12 comma 3, comma 3-*bis*, comma 3-*ter* e comma 5 del D.Lgs. n. 286/98 (procurato ingresso illecito e favoreggiamento dell'immigrazione clandestina).

-18 L'art. 25-*terdecies* è stato introdotto dalla Legge Europea 2017, approvata l'8 novembre 2017, con riferimento alla commissione dei delitti previsti dall'articolo 3, comma 3-*bis*, della Legge 13 ottobre 1975, n. 654, così come modificato dalla medesima Legge Europea. Inoltre, si richiama quanto sopra menzionato con riferimento al D.Lgs. 21/2008 e, in particolare, all'art. 604 *bis* c.p. ("Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa"), in sostituzione dell'art. 3 della L. 13 ottobre 1975, n. 654.

-19 L'art. 25 *quaterdecies* è stato inserito dalla Legge 3 maggio 2019, n. 39, entrata in vigore il 16 maggio 2019, che ha introdotto, quali reati presupposto della responsabilità degli enti ex D.Lgs. 231/2001, la frode in competizioni sportive e l'esercizio abusivo di gioco o di scommessa e giochi d'azzardo disciplinati dagli artt. 1 e 4 della Legge 13 dicembre 1989, n. 401.

-20 L'art. 25 *quingiesdecies* è stato inserito dalla Legge 24 dicembre 2019, n. 157, entrata in vigore il 25 dicembre 2019, che ha introdotto quali reati presupposto della responsabilità degli enti ex D.Lgs. 231/2001 alcuni dei reati tributari di cui al D.Lgs. 74/2000 e, più precisamente: dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. 74/00), dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. 74/2000), emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. 74/2000), occultamento o distruzione di documenti contabili (art. 10 D.Lgs. 74/2000) e sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. 74/2000). Da ultimo, l'art. 5 del D. Lgs. 75/2020 ha integrato il catalogo dei reati presupposto inserendo i delitti di "Dichiarazione infedele" (art. 4 D. Lgs. 74/2000), "Omessa dichiarazione" (art. 5 del D. Lgs. 74/2000) e "Indebita compensazione" (art. 10-quater D. Lgs. 231/2001) commessi anche in parte nel territorio di un altro Stato membro dell'Unione europea allo scopo di evadere l'Iva; per tali ipotesi di reato è prevista la sanzione a carico dell'ente qualora l'ammontare dell'evasione sia superiore a 10 milioni di euro.

-21 Articolo introdotto dall'art. 5 del D. Lgs. 75/2020 che prevede, in relazione alla commissione dei reati di contrabbando di cui al D.P.R. n. 43 del 1973, la responsabilità amministrativa degli enti. Le sanzioni pecuniarie sono differenziate a seconda che i diritti di confine dovuti eccedano o meno i 100.000 euro.

-22 Si veda, a tale proposito, l'art. 16 d.lgs. n. 231/2001, secondo cui:

"1. Può essere disposta l'interdizione definitiva dall'esercizio dell'attività se l'ente ha tratto dal reato un profitto di rilevante entità ed è già stato condannato, almeno tre volte negli ultimi sette anni, alla interdizione temporanea dall'esercizio dell'attività.

2. Il giudice può applicare all'ente, in via definitiva, la sanzione del divieto di contrattare con la Pubblica Amministrazione ovvero del divieto di pubblicizzare beni o servizi quando è già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni.

3. Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali è prevista la sua responsabilità è sempre disposta l'interdizione definitiva dall'esercizio dell'attività e non si applicano le disposizioni previste dall'articolo 17".

-23 "Commissario giudiziale – Se sussistono i presupposti per l'applicazione di una sanzione interdittiva che determina l'interruzione dell'attività dell'ente, il giudice, in luogo dell'applicazione della sanzione, dispone la prosecuzione dell'attività dell'ente da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni:

a) l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;

b) l'interruzione dell'attività dell'ente può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione. Con la sentenza che dispone la prosecuzione dell'attività, il giudice indica i compiti ed i poteri del commissario, tenendo conto della specifica attività in cui è stato posto in essere l'illecito da parte dell'ente. Nell'ambito dei compiti e dei poteri indicati dal giudice, il commissario cura l'adozione e l'efficace attuazione dei modelli di organizzazione e di controllo idonei a prevenire reati della specie di quello verificatosi. Non può compiere atti di straordinaria amministrazione senza autorizzazione del giudice. Il profitto derivante dalla prosecuzione dell'attività viene confiscato. La prosecuzione dell'attività da parte del commissario non può essere disposta quando l'interruzione dell'attività consegue all'applicazione in via definitiva di una sanzione interdittiva".

-24 L'art. 4 del d.lgs. n. 231/2001 prevede quanto segue: *"1. Nei casi e alle condizioni previsti dagli articoli 7, 8, 9 e 10 del codice penale, gli enti aventi nel territorio dello Stato la sede principale rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto. 2. Nei casi in cui la legge prevede che il colpevole sia punito a richiesta del Ministro della giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti di quest'ultimo."*

-25 Le persone fisiche sono in possesso dei requisiti di onorabilità se rispettano, congiuntamente, le seguenti condizioni:

- a. non si trovino in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;
- b. non siano state sottoposte a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423 o della legge 31 maggio 1965, n. 575, e successive modificazioni ed integrazioni, salvi gli effetti della riabilitazione;
- c. non siano state condannate con sentenza irrevocabile, salvi gli effetti della riabilitazione, ad una delle seguenti pene:
 - i. reclusione per un tempo superiore a sei mesi per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati, valori mobiliari e strumenti di pagamento, nonché per i reati previsti dal decreto legislativo 27 gennaio 2010, n. 39;
 - ii. reclusione per un tempo superiore a sei mesi per uno dei delitti previsti nel titolo XI del libro V del codice civile;
 - iii. reclusione per un tempo superiore ad un anno per un delitto contro la pubblica Amministrazione, contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria;
 - iv. reclusione per un tempo superiore a due anni per qualunque delitto non colposo;
- v. non abbiano riportato in Stati esteri condanne penali o altri provvedimenti sanzionatori per fattispecie e durata corrispondenti a quelle che comporterebbero, secondo la legge italiana, la perdita dei requisiti di onorabilità.

Il presente Modello si configura come Modello di Gruppo, recepito dalle singole società che ne fanno parte e nello specifico da Major Bit Consulting S.r.l., Major Bit Academy S.r.l., Major Bit Innovation S.r.l., Major Bit Production S.r.l., al fine di garantire un presidio uniforme dei rischi reato.