



MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

D.LGS.231 DEL 2001

REVISIONE IN DATA 28 NOVEMBRE 2018

Sommario

PARTE GENERALE

1	IL DECRETO LEGISLATIVO N. 231 DEL 2001.	9
1.1	<i>Il regime di responsabilità amministrativa previsto a carico degli enti.</i>	9
1.2	<i>Sanzioni.</i>	10
1.2.1	<i>La sanzione amministrativa pecuniaria.</i>	10
1.2.2	<i>Le sanzioni interdittive.</i>	12
1.2.3	<i>La confisca.</i>	12
1.2.4	<i>La pubblicazione della sentenza di condanna.</i>	13
1.3	<i>Condotte esimenti la responsabilità amministrativa.</i>	13
2	LINEE GUIDA DI CONFINDUSTRIA.	14
3	ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DA PARTE DI LOGIC SPA.	15
3.1	<i>Motivazioni di LOGIC nell'adozione del Modello di Organizzazione, Gestione e Controllo.</i>	15
3.2	<i>Finalità del Modello 231.</i>	15
3.3	<i>Struttura del documento.</i>	16
3.4	<i>Modifiche ed integrazioni del Modello.</i>	16
4	ORGANISMO DI VIGILANZA.	17
4.1	<i>Identificazione dell' OdV.</i>	17
4.1.1	<i>Autonomia e indipendenza.</i>	17
4.1.2	<i>Professionalità.</i>	17
4.1.3	<i>Continuità d'azione.</i>	17
4.2	<i>Funzioni, poteri e doveri dell'OdV.</i>	18
4.3	<i>Flussi informativi dell'OdV nei confronti degli organi societari.</i>	19
4.4	<i>Flussi informativi nei confronti dell'OdV.</i>	19
4.4.1	<i>Segnalazioni da parte di dipendenti aziendali o da parte di terzi.</i>	19
4.4.2	<i>Ulteriori obblighi di informativa relativi alle attività degli organi della Pubblica Amministrazione.</i>	20
4.4.3	<i>Articolazione dei Poteri e Sistema delle deleghe.</i>	20
4.4.4	<i>Struttura organizzativa.</i>	21
5	FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO NEL CONTESTO AZIENDALE E ALL'ESTERNO.	21
5.1	<i>Formazione del personale.</i>	21
5.2	<i>Informativa a collaboratori esterni e partner.</i>	21
6	SISTEMA DISCIPLINARE IN CASO DI MANCATA OSSERVANZA DELLE PRESCRIZIONI DEL MODELLO.	22
6.1	<i>Principi generali.</i>	22
6.2	<i>Sanzioni per i lavoratori dipendenti.</i>	22
6.2.1	<i>Personale dipendente in posizione non dirigenziale.</i>	22
6.2.2	<i>Dirigenti.</i>	23
6.3	<i>Misure nei confronti degli Amministratori e dei Sindaci.</i>	23
6.4	<i>Misure nei confronti di collaboratori esterni, partner, intermediari.</i>	23
7	ATTIVITA' DI VERIFICA SULL'APPLICAZIONE E SULL'ADEGUATEZZA DEL MODELLO DA PARTE DELLA STRUTTURA AZIENDALE.	24
	ALLEGATI.	24

PARTE SPECIALE

PREMESSA	27	
1	PRINCIPI DEL SISTEMA DI CONTROLLO "231"	28
2	STRUMENTI DI CONTROLLO	29
2.1	<i>Sistema di controllo interno.</i>	29
2.2	<i>Sistema delle Procedure.</i>	30

SEZIONE "A"	31
ART. 24 DEL DECRETO 231	31
ART. 25 DEL DECRETO 231	31
ART. 25 DECIES DEL DECRETO 231	31
1 PRINCIPI DI COMPORAMENTO	35
2 CONTROLLI	41
2.1 <i>Ulteriori controlli specifici</i>	41
2.2 <i>Tracciabilità delle transazioni</i>	44
2.3 <i>Segregazione dei compiti</i>	45
2.4 <i>Sistema di procure/deleghe coerente con le responsabilità, ruoli e compiti</i>	46
3 FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA	47
SCHEDA DI EVIDENZA	48
SEZIONE "B"	49
ART. 25 TER DEL DECRETO 231	49
1 ATTIVITÀ SENSIBILI ALLA COMMISSIONE DEI REATI SOCIETARI AD ESCLUSIONE DELLA CORRUZIONE TRA PRIVATI	51
1.1 <i>Principi di comportamento</i>	51
1.2 <i>Controlli</i>	53
1.2.1 <i>Attribuzione delle responsabilità</i>	55
1.2.2 <i>Tracciabilità delle transazioni</i>	55
1.2.3 <i>Segregazione dei compiti</i>	55
1.2.4 <i>Sistema di procure/deleghe coerente con le responsabilità, ruoli e compiti</i>	55
2 ATTIVITÀ SENSIBILI ALLA COMMISSIONE DEL DELITTO DI CORRUZIONE TRA PRIVATI	55
2.1 <i>Principi di comportamento</i>	56
2.2 <i>Controlli</i>	57
SEZIONE "C"	59
ART. 24 TER DEL DECRETO 231	59
1 PRINCIPI DI COMPORAMENTO	60
2 CONTROLLI	62
2.1.1 <i>Attribuzione delle responsabilità</i>	62
2.1.2 <i>Tracciabilità delle transazioni</i>	62
2.1.3 <i>Segregazione dei compiti</i>	62
2.1.4 <i>Sistema di procure/deleghe coerente con le responsabilità, ruoli e compiti</i>	62
SEZIONE "D"	63
ART. 25 OCTIES DEL DECRETO 231	63
1 PRINCIPI DI COMPORAMENTO	64
2 CONTROLLI	66
2.1 <i>Attribuzione delle responsabilità</i>	66
2.2 <i>Controlli specifici</i>	66
2.3 <i>Tracciabilità delle transazioni</i>	68
2.4 <i>Segregazione dei compiti</i>	68
2.5 <i>Sistema delle procure/deleghe coerente con responsabilità, ruoli e compiti</i>	69
SEZIONE "E"	71
ART. 25 BIS1 DEL DECRETO 231	71
ART. 25 NOVIES DEL DECRETO 231	71
ART. 25 BIS DEL DECRETO 231	71
1 PRINCIPI DI COMPORAMENTO	75

2	CONTROLLI	76
2.1	<i>Attribuzione delle responsabilità</i>	76
2.2	<i>Tracciabilità delle transazioni</i>	77
2.3	<i>Segregazione dei compiti</i>	77
2.4	<i>Sistema delle procure/deleghe coerente con responsabilità, ruoli e compiti</i>	77
SEZIONE "F"		79
ART. 24 BIS DEL DECRETO231		79
1	PRINCIPI DI COMPORTAMENTO	81
2	CONTROLLI	83
2.1	<i>Attribuzione delle responsabilità</i>	83
2.2	<i>Il Codice Etico, il Modello 231 e il Protocollo per la Sicurezza Informatica</i>	85
2.3	<i>Tracciabilità delle transazioni</i>	85
2.4	<i>Segregazione dei compiti</i>	86
SEZIONE "G"		87
ART. 25 SEPTIES DEL DECRETO231		87
1	PRINCIPI DI COMPORTAMENTO	88
2	CONTROLLI	90
2.1	<i>Attribuzione delle responsabilità</i>	90
2.2	<i>Controlli specifici</i>	94
2.2.1	<i>Pianificazione</i>	94
2.2.2	<i>Attuazione e funzionamento</i>	95
2.2.3	<i>Azioni correttive e di miglioramento</i>	97
2.2.4	<i>Attività di riesame dell'Alta Direzione</i>	98
2.3	<i>Tracciabilità delle transazioni</i>	98
2.4	<i>Segregazione dei compiti</i>	98
2.5	<i>Sistema di procure/deleghe coerente con responsabilità, ruoli e compiti</i>	99
SEZIONE "H"		101
ART. 25 UNDECIES DEL DECRETO231		101
1	PRINCIPI DI COMPORTAMENTO	104
2	CONTROLLI	109
2.1	<i>Attribuzione delle responsabilità</i>	109
2.2	<i>Protocolli specifici</i>	109

PARTE GENERALE

1 IL DECRETO LEGISLATIVO N. 231 DEL 2001.

1.1 Il regime di responsabilità amministrativa previsto a carico degli enti.

Il Decreto Legislativo n. 231 dell'8 giugno 2001, che, in attuazione della Legge Delega 29 settembre 2000, n. 300, ha introdotto in Italia la *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"* (d'ora innanzi, per brevità, il "Decreto 231" o "Decreto"), ha adeguato la normativa italiana in materia di responsabilità degli enti, in particolare, alla Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari della Comunità Europea, la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione di funzionari pubblici sia delle Comunità Europee che degli Stati membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri in occasione delle operazioni economiche ed internazionali.

Il Decreto stabilisce, pertanto, un regime di responsabilità amministrativa, a carico sia delle persone giuridiche che di quelle non giuridiche (d'ora innanzi, per brevità, l'/gli "ENTE/Enti"), che va ad aggiungersi alla responsabilità penale della persona fisica che ha commesso materialmente il reato e che mira a coinvolgere, nella punizione del fatto illecito, anche gli Enti nel cui interesse e/o vantaggio tale reato è stato compiuto.

L'articolo 4 del Decreto ("Reati commessi all'estero") precisa inoltre che nei casi e alle condizioni previsti dagli articoli 7, 8, 9 e 10¹ del Codice Penale, sussiste la responsabilità amministrativa degli

¹Per maggiore chiarezza nell'esposizione si riportano di seguito gli articoli 7,8,9 e 10 del Codice Penale:

Articolo 7: Reati commessi all'estero.

È punito secondo la legge italiana il cittadino o lo straniero che commette in territorio estero taluno dei seguenti reati:

1. delitti contro la personalità dello Stato italiano;
2. delitti di contraffazione del sigillo dello Stato e di uso di tale sigillo contraffatto;
3. delitti di falsità in monete aventi corso legale nel territorio dello Stato, o in valori di bollo o in carte di pubblico credito italiano;
4. delitti commessi da pubblici ufficiali a servizio dello Stato, abusando dei poteri o violando i doveri inerenti alle loro funzioni;
5. ogni altro reato per il quale speciali disposizioni di legge o convenzioni internazionali stabiliscono l'applicabilità della legge penale italiana.

Articolo 8: Delitto politico commesso all'estero.

Il cittadino o lo straniero, che commette in territorio estero un delitto politico non compreso tra quelli indicati nel n. 1 dell'articolo precedente, è punito secondo la legge italiana, a richiesta del ministro della giustizia.

Se si tratta di delitto punibile a querela della persona offesa, occorre, oltre tale richiesta, anche la querela.

Agli effetti della legge penale, è delitto politico ogni delitto, che offende un interesse politico dello Stato, ovvero un diritto politico del cittadino. È altresì considerato delitto politico il delitto comune determinato, in tutto o in parte, da motivi politici.

Articolo 9: Delitto comune del cittadino all'estero.

Il cittadino, che, fuori dei casi indicati nei due articoli precedenti, commette in territorio estero un delitto per il quale la legge italiana stabilisce (...) l'ergastolo, o la reclusione non inferiore nel minimo a tre anni, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato.

Se si tratta di delitto per il quale è stabilita una pena restrittiva della libertà personale di minore durata, il colpevole è punito a richiesta del ministro della giustizia ovvero a istanza, o a querela della persona offesa.

Nei casi preveduti dalle disposizioni precedenti, qualora si tratti di delitto commesso a danno della Comunità europea, di uno Stato estero o di uno straniero, il colpevole è punito a richiesta del ministro della giustizia, sempre che l'estradizione di lui non sia stata concessa, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto.

Enti che hanno sede principale nel territorio dello Stato per i reati commessi all'estero a condizione che nei confronti di tali Enti non proceda lo Stato del luogo in cui è stato commesso il fatto criminoso.

Il Decreto presuppone:

- a. l'individuazione delle persone che, commettendo un reato nell'interesse e/o a vantaggio dell'ENTE, ne possono determinare la responsabilità. In particolare, possono essere:
 - i. persone fisiche che rivestono posizioni di vertice (rappresentanza, amministrazione o direzione dell'ENTE o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale o persone che esercitano, di fatto, la gestione ed il controllo: d'ora innanzi, per brevità, i "soggetti apicali" o gli "apicali");
 - ii. persone fisiche sottoposte alla direzione o vigilanza di uno dei soggetti apicali (d'ora innanzi, per brevità, i "soggetti sottoposti" o i "sottoposti").

e comprende

- b. i reati indicati negli articoli dal 24 al 25 terdecies del decreto come da allegato IV al presente Modello, aggiornato al mese di aprile 2018.

In considerazione della natura dell'attività imprenditoriale svolta da LOGIC S.p.A. (d'ora innanzi, per brevità, "LOGIC" o la "SOCIETA'") e della circostanza che la maggior parte dei rapporti commerciali intrattenuti da tale impresa riguarda lo studio, la progettazione, la produzione, la messa in opera, la revisione e la manutenzione, il commercio e la rappresentanza sia in Italia che all'Estero di apparecchiature elettroniche industriali ed equipaggiamenti aerospaziali in genere il Consiglio di Amministrazione di LOGIC ha assunto la decisione di adottare il presente Modello di Organizzazione, Gestione e Controllo (d'ora innanzi, per brevità, il "Modello") con riferimento, in particolare, ai reati riportati nelle sezioni della Parte Speciale del Modello stesso.

1.2 Sanzioni

Le sanzioni previste dal decreto per gli illeciti amministrativi dipendenti da reato sono:

- a. la sanzione amministrativa pecuniaria;
- b. le sanzioni interdittive;
- c. la confisca;
- d. la pubblicazione della sentenza di condanna.

1.2.1 La sanzione amministrativa pecuniaria

Articolo 10: Delitto comune dello straniero all'estero.

Lo straniero, che, fuori dei casi indicati negli articoli 7 e 8, commette in territorio estero, a danno dello Stato o di un cittadino, un delitto per il quale la legge italiana stabilisce (...) l'ergastolo, o la reclusione non inferiore nel minimo a un anno, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato, e vi sia richiesta del ministro della giustizia, ovvero istanza o querela della persona offesa.

Se il delitto è commesso a danno delle Comunità europee, di uno Stato estero o di uno straniero, il colpevole è punito secondo la legge italiana, a richiesta del ministro della giustizia, sempre che:

1. si trovi nel territorio dello Stato;
 2. si tratti di delitto per il quale è stabilita la pena dell'ergastolo, ovvero della reclusione non inferiore nel minimo a tre anni;
 3. l'estradizione di lui non sia stata concessa, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto, o da quello dello Stato a cui egli appartiene.
-

La sanzione amministrativa pecuniaria, disciplinata dagli articoli 10 e seguenti del Decreto, costituisce la sanzione "di base" di necessaria applicazione, del cui pagamento risponde l'ENTE con il suo patrimonio.

Il Legislatore ha adottato un criterio innovativo di commisurazione della sanzione, attribuendo al Giudice l'obbligo di procedere a due diverse operazioni di apprezzamento con la conseguente possibilità di un maggiore adeguamento della sanzione alla gravità del fatto ed alle condizioni economico-patrimoniali dell'ENTE.

La prima valutazione richiede al Giudice di determinare il numero delle quote tenendo conto:

- ❖ della gravità del fatto;
- ❖ del grado di responsabilità dell'ENTE;
- ❖ dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti.

Nel corso della seconda valutazione il Giudice determina, entro i valori minimi e massimi predeterminati in relazione agli illeciti sanzionati, il valore di ciascuna quota [da un minimo euro 258,00 ad un massimo di Euro 1.549,00 per ogni quota] *"sulla base delle condizioni economiche e patrimoniali dell'ENTE allo scopo di assicurare l'efficacia della sanzione"* (articolo 11, comma secondo del Decreto). È previsto sia un minimo (cento) sia il massimo (mille) delle quote che possono essere applicate dal Giudice.

Come affermato al punto 5.1. della Relazione ministeriale al Decreto, "...omissis...quanto alle modalità di accertamento delle condizioni economiche e patrimoniali dell'ENTE, il giudice potrà avvalersi dei bilanci o delle altre scritture comunque idonee a fotografare tali condizioni. In taluni casi, la prova potrà essere conseguita anche tenendo in considerazione le dimensioni dell'ENTE e la sua posizione sul mercato... il giudice non potrà fare a meno di calarsi, con l'ausilio di consulenti, nella realtà dell'impresa, dove potrà attingere anche le informazioni relative allo stato di solidità economica, finanziaria e patrimoniale dell'ENTE...omissis...".

L'articolo 12 prevede una serie di casi in cui la sanzione pecuniaria viene ridotta. Essi sono schematicamente riassunti nella tabella sottostante con indicazione della riduzione apportata e dei presupposti per l'applicazione della riduzione stessa.

Riduzione	Presupposti
1/2 (e non può comunque essere superiore a € 103.291,00)	<ul style="list-style-type: none"> • L'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ENTE non ne ha ricavato un vantaggio o ne ha ricavato un vantaggio minimo; oppure • Il danno patrimoniale cagionato è di particolare tenuità.
da 1/3 a 1/2	<p>[Prima della dichiarazione di apertura del dibattimento di primo grado]</p> <ul style="list-style-type: none"> • L'ENTE ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; oppure • è stato attuato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.
da 1/2 a 2/3	<p>[Prima della dichiarazione di apertura del dibattimento di primo grado]</p> <ul style="list-style-type: none"> • L'ENTE ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; ed • è stato attuato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

1.2.2 Le sanzioni interdittive

Le sanzioni interdittive previste sono:

- ❖ l'interdizione dall'esercizio dell'attività (questa comporta anche la sospensione ovvero la revoca delle autorizzazioni, licenze o concessioni quando sono funzionali allo svolgimento della predetta attività);
- ❖ il divieto di contrattare con la Pubblica Amministrazione;
- ❖ la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- ❖ l'esclusione da agevolazioni, finanziamenti, contributi e sussidi, e/o la revoca di quelli eventualmente già concessi;
- ❖ il divieto di pubblicizzare beni o servizi.

Esse si applicano solo in relazione ai reati per i quali sono espressamente previste al ricorrere di almeno una delle condizioni di cui all'articolo 13 del Decreto, di seguito indicate:

- ❖ "l'ENTE ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in questo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative";
- ❖ "in caso di reiterazione degli illeciti" (cioè la commissione di un illecito dipendente da reato nei cinque anni dalla sentenza definitiva di condanna per un altro precedente illecito).

In ogni caso, non si procede all'applicazione delle sanzioni interdittive quando il reato è stato commesso nel prevalente interesse dell'autore o di terzi e l'ENTE ne ha ricavato un vantaggio minimo o nullo ovvero il danno patrimoniale cagionato è di particolare tenuità. È esclusa altresì l'applicazione quando l'ENTE abbia posto in essere le condotte riparatorie previste dall'articolo 17 e, più precisamente, quando concorrono le seguenti condizioni:

- ❖ "l'ENTE ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
- ❖ l'ENTE ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi;
- ❖ l'ENTE ha messo a disposizione il profitto conseguito ai fini della confisca".

Le sanzioni interdittive hanno una durata compresa tra tre mesi e due anni e la scelta della misura da applicare e per quanto tempo viene effettuata dal Giudice sulla base dei criteri in precedenza indicati per la commisurazione della sanzione pecuniaria, "tenendo conto dell'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso e, se necessario, possono essere applicate congiuntamente" (articolo 14 del Decreto).

Si sottolinea il fatto che tali sanzioni, in alcuni casi, possono essere adottate sin durante le indagini preliminari, in via cautelare, quindi anche prima del rinvio a giudizio e, pertanto, antecedente alla sentenza alla fine del processo di primo grado.

1.2.3 La confisca

Ai sensi dell'articolo 19 del Decreto, è sempre disposta, con la sentenza di condanna, la confisca - anche per equivalente - del prezzo (denaro o altra utilità economica data o promessa per indurre o determinare un altro soggetto a commettere il reato) o del profitto (utilità economica ricavata) del reato, salvo che per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquisiti dai

terzi in buona fede.

1.2.4 La pubblicazione della sentenza di condanna

La pubblicazione in uno o più giornali della sentenza di condanna, per estratto o per intero, può essere disposta dal Giudice, unitamente all'affissione nel Comune dove l'ENTE ha la sede principale, quando è applicata una sanzione interdittiva. La pubblicazione è eseguita a cura della Cancelleria del Tribunale a spese dell'ENTE.

1.3 Condotte esimenti la responsabilità amministrativa

Gli artt. 6 e 7 del Decreto prevedono tuttavia forme specifiche di esonero dalla responsabilità amministrativa dell'ENTE per i reati commessi nell'interesse e/o a vantaggio dello stesso sia da soggetti apicali sia da soggetti sottoposti.

In particolare, nel caso di reati commessi da soggetti apicali, l'art. 6 prevede l'esonero qualora l'ENTE stesso dimostri che:

- a. l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi" (per brevità il "Modello");
- b. il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporre l'aggiornamento sia stato affidato ad un Organismo di Vigilanza dell'ENTE (d'ora innanzi, per brevità, l' "OdV" o l'"Organismo")), dotato di autonomi poteri di iniziativa e controllo;
- c. le persone che hanno commesso il reato abbiano agito eludendo fraudolentemente il Modello;
- d. non vi sia stata omessa o insufficiente vigilanza da parte dell'OdV.

Quindi, in caso di illeciti commessi dai soggetti apicali l'ENTE dovrà sostenere una difesa più articolata e complessa per dimostrare, nel procedimento penale, l'effettività e l'efficienza del Modello di Organizzazione, Gestione e Controllo 231.

Per quanto concerne i sottoposti, l'art. 7 prevede l'esonero della responsabilità nel caso in cui l'ENTE abbia adottato ed efficacemente attuato, prima della commissione del reato, un Modello idoneo a prevenire reati della specie di quello verificatosi. Ciò, infatti, fa escludere, in ogni caso, che gli apicali non abbiano osservato i loro obblighi di direzione e vigilanza.

Il Decreto prevede, inoltre, che tale Modello debba rispondere alle seguenti esigenze:

1. individuare le attività nel cui ambito esiste la possibilità che siano commessi reati;
2. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ENTE in relazione ai reati da prevenire;
3. individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
4. prevedere obblighi di informazione (flussi informativi) nei confronti dell'OdV;
5. introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
6. prevedere la formazione del personale.

2 LINEE GUIDA DI CONFINDUSTRIA.

La predisposizione del presente Modello è ispirata alle Linee Guida emanate da Confindustria per la prima volta il 7 marzo 2002 ed integrate in data 3 ottobre 2002 con l'Appendice integrativa in tema di reati societari" (di seguito le "Linee Guida") e successivamente aggiornate più volte fino alla elaborazione dell'ultima versione, quella del 2014.

Il percorso da queste indicato per l'elaborazione del Modello può essere schematizzato secondo i seguenti punti fondamentali:

- ❖ individuazione delle attività a rischio, volta a verificare in quali aree/settori aziendali sia possibile la realizzazione dei reati;
- ❖ predisposizione di un sistema di controllo in grado di ridurre i rischi attraverso l'adozione di appositi protocolli. A supporto di ciò soccorre l'insieme coordinato di strutture organizzative, attività e regole operative applicate - su indicazione del vertice apicale - dal management e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti in un buon sistema di controllo interno. Le componenti più rilevanti del sistema di controllo preventivo proposto da Confindustria sono:
 - codice etico;
 - sistema organizzativo;
 - procedure;
 - poteri autorizzativi e di firma;
 - sistemi di controllo e gestione;
 - comunicazioni al personale e sua formazione.

Il sistema di controllo inoltre deve essere informato ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- separazione delle funzioni (nessuno può gestire in autonomia tutte le fasi di un processo);
- documentazione dei controlli;
- introduzione di un adeguato sistema sanzionatorio per le violazioni delle norme e dei protocolli previsti dal Modello;
- individuazione di un OdV i cui principali requisiti siano:
 - autonomia e indipendenza,
 - professionalità,
 - continuità di azione.
- ❖ obbligo da parte delle funzioni aziendali, e segnatamente di quelle individuate come maggiormente "a rischio", di fornire informazioni all'OdV, sia su base strutturata (informativa periodica in attuazione del Modello stesso), sia per segnalare anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (in quest'ultimo caso l'obbligo è esteso a tutti i dipendenti senza necessariamente seguire linee gerarchiche).

Resta inteso che il documento di Confindustria rappresenta una guida e come tale deve poi essere modulato per ogni ENTE in base alle specifiche proprie organizzazioni, alle varie rispettive attività e alle procure e deleghe adottate dal Consiglio di Amministrazione e dagli apicali. Mai uno stesso Modello 231 potrà essere considerato come uno standard valido per tutti gli enti.

3 ADOZIONE DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DA PARTE DI LOGIC SPA.

3.1 Motivazioni di LOGIC nell'adozione del Modello di Organizzazione, Gestione e Controllo

Logic, al fine di assicurare sempre più condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, ha ritenuto conforme alle proprie politiche aziendali procedere all'adozione di un Modello di organizzazione, gestione e di controllo in linea con le prescrizioni del Decreto 231 e sulla base delle Linee Guida di Confindustria.

Tale iniziativa, unitamente alla predisposizione e conseguente adozione da parte del Consiglio di Amministrazione di LOGIC del Codice Etico contestualmente al presente Modello, è stata assunta nella convinzione che tali documenti (al di là delle prescrizioni contenute nel Decreto, che indicano comunque il Modello come non obbligatorio) possano costituire un valido strumento di sensibilizzazione nei confronti di tutti i dipendenti della SOCIETA' e di tutti gli altri soggetti alla stessa cointeressati (Clienti, Fornitori, Partner, Collaboratori, Intermediari a diverso titolo), affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da ridurre il rischio di commissione dei reati contemplati nel Decreto.

3.2 Finalità del Modello 231

Il Modello predisposto da LOGIC si fonda su un sistema di regole contenute sia nel Codice Etico sia nel Modello che nei protocolli, nonché di attività di controllo che nella sostanza:

- ❖ individuano le aree/i processi di possibile rischio nelle attività aziendali vale a dire quelle nel cui ambito si ritiene rilevante il rischio di commissioni dei reati;
- ❖ definiscono un sistema regolatorio interno diretto a programmare la formazione e l'attuazione delle decisioni della SOCIETA' in relazione ai rischi/reati da prevenire tramite:
 - un Codice Etico, che esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività aziendali assunti dai dipendenti, amministratori, collaboratori, intermediari a vario titolo della SOCIETA';
 - un sistema di deleghe di funzioni e di procure per la firma di atti aziendali che assicuri una chiara e trasparente rappresentazione del processo di formazione e di attuazione delle decisioni;
- ❖ determinano una struttura organizzativa coerente volta ad ispirare e controllare la correttezza dei comportamenti, garantendo una chiara ed organica attribuzione dei compiti, applicando una giusta segregazione delle funzioni, assicurando che gli assetti indicati nella struttura organizzativa siano correttamente attuati;
- ❖ individuano i processi di gestione e controllo delle risorse finanziarie nelle attività a rischio;
- ❖ attribuiscono all'OdV il compito di vigilare sul funzionamento e sull'osservanza del Modello e di proporre l'aggiornamento.

Pertanto, il Modello si propone come finalità quelle di:

- migliorare il sistema di *Corporate Governance*;
- predisporre un sistema strutturato ed organico di prevenzione e controllo finalizzato alla riduzione del rischio di commissione dei reati connessi alle attività aziendali;

- determinare, in tutti coloro che operano in nome e per conto di LOGIC nelle "aree di attività a rischio", la consapevolezza di commettere, in caso di violazione delle disposizioni ivi riportate, non solo un illecito passibile di sanzioni penali nei propri confronti ma anche, sotto il profilo degli illeciti amministrativi, nei confronti dell'azienda;
- informare tutti coloro che operano a qualsiasi titolo in nome, per conto o comunque nell'interesse di LOGIC che la violazione delle prescrizioni contenute nel Modello (e nel Codice Etico) comporterà l'applicazione di apposite sanzioni ovvero la risoluzione del rapporto contrattuale. All'uopo saranno inserite specifiche clausole nei contratti di forniture, vendite, servizi, consulenze;
- ribadire che LOGIC non tollera comportamenti illeciti, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui la SOCIETA' possa averne interesse e/o trarne vantaggio) sono comunque contrari ai principi etici cui LOGIC ha già uniformato la propria missione.

3.3 *Struttura del documento*

Il presente Modello è costituito da una "Parte Generale" e da una "Parte Speciale", predisposta questa per le diverse tipologie di reato, contemplate nel Decreto, considerate di possibile, rilevante rischio da parte di LOGIC. Nella Parte Generale, dopo un richiamo ai principi del Decreto, vengono illustrate le componenti essenziali del Modello, indicati i reati presupposto in uno specifico elenco (allegato IV al Modello), con riferimenti all'Organismo di Vigilanza, alla formazione del personale e diffusione del Modello nel contesto aziendale, al sistema disciplinare e le misure da adottare in caso di mancata osservanza delle prescrizioni del Modello. La Parte Speciale del Modello è suddivisa in Sezioni contenenti la descrizione dei reati valutati con rischio rilevante per l'Ente e che si intendono presidiare con i protocolli di prevenzione in aggiunta al complesso ed articolato sistema dei controlli interni della SOCIETA' (già esistente e attuato) concernente le varie certificazioni cui LOGIC deve conformarsi nella progettazione e produzione (e assistenza) dei propri particolari prodotti, sia a favore delle Amministrazioni Pubbliche sia di società private.

3.4 *Modifiche ed integrazioni del Modello*

Essendo il presente Modello un atto di emanazione dell'Organo amministrativo [in conformità alle prescrizioni dell'art. 6, comma 1, lettera a), del Decreto], la sua adozione, così come le successive modifiche ed integrazioni, quando sostanziali, sono rimesse alla competenza del Consiglio di Amministrazione della SOCIETA'.

In particolare, è demandato al Consiglio di Amministrazione di Logic, su proposta dell'Organismo di Vigilanza, di integrare/modificare le Sezioni della Parte Speciale del presente Modello con altre tipologie di reati che, per effetto di nuove normative o di eventuali successive intervenute decisioni o necessità della SOCIETA', possano essere ulteriormente connesse all'ambito di applicazione del Decreto in relazione alle attività aziendali o di aggiornarlo a seguito di modifiche normative o per effetto di rilevanti variazioni nella struttura o nella attività aziendale.

4 ORGANISMO DI VIGILANZA.

4.1 Identificazione dell' OdV

Secondo le Linee Guida di Confindustria, le norme del Decreto (artt. 6 e 7) e le indicazioni contenute nella Relazione di accompagnamento, le caratteristiche/requisiti dell'OdV debbono coincidere con:

- a. autonomia e indipendenza,
- b. professionalità,
- c. continuità d'azione.

4.1.1 Autonomia e indipendenza

I requisiti di autonomia e indipendenza sono fondamentali affinché l'OdV non sia direttamente coinvolto nelle attività gestionali dell'ENTE.

Tali requisiti si possono ottenere garantendo all'OdV la posizione di staff all'organo di vertice, prevedendo un'attività di reporting periodico direttamente al Consiglio di Amministrazione.

Inoltre, il regolamento OdV, che sarà redatto direttamente dallo stesso Organismo e il budget a sua disposizione, deliberato dal Consiglio di Amministrazione, daranno effettiva evidenza della sua autonomia.

4.1.2 Professionalità

L'OdV deve possedere competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche unite all'indipendenza garantiscono l'obiettività di giudizio.

4.1.3 Continuità d'azione

L'OdV deve:

1. vigilare sull'applicazione del Modello con i necessari poteri d'indagine, garantendo continuità nell'attività di controllo;
2. curare l'attuazione del Modello e assicurarne il costante aggiornamento;
3. non svolgere mansioni operative che possano condizionare i necessari ed imprescindibili caratteri di autonomia e indipendenza nello svolgimento dei compiti assegnatigli.

Il Consiglio di Amministrazione di LOGIC ha nominato, ai sensi dell'art. 6, lettera b) del Decreto, un Organismo monocratico, che, nello svolgimento dei propri compiti, potrà avvalersi di altre funzioni aziendali di LOGIC o di professionisti esterni che, di volta in volta, si reputerà necessario incaricare per lo svolgimento dei controlli disposti dallo stesso OdV. I compiti, le attività ed il funzionamento sono disciplinati dal regolamento di cui sopra. La durata del mandato dell'OdV è stabilita in 3 anni. I membri dello stesso decadono al perdere dei requisiti e/o delle qualità sulla base dei quali è avvenuta la nomina.

Ai sensi del comma 4-bis dell'art. 6 del Decreto, nelle SOCIETA' di capitali il Collegio Sindacale, il Consiglio di Sorveglianza e il Comitato di Controllo della gestione possono svolgere le funzioni dell'Organismo di Vigilanza.

4.2 Funzioni, poteri e doveri dell'OdV

L'attività dell'OdV di LOGIC consiste nel:

1. vigilare sull'applicazione del Modello in relazione alle diverse tipologie di reati contemplate dal Decreto e considerate a rischio per la SOCIETA';
2. verificare l'efficacia del Modello e la sua effettiva capacità, in relazione alla struttura aziendale, di prevenire la commissione dei reati di cui al Decreto;
3. individuare e proporre aggiornamenti e modifiche del Modello stesso in relazione alla possibile evoluzione della normativa di riferimento, della mutata organizzazione e del contesto operativo della SOCIETA' o di ogni altra esigenza di revisione.
4. monitorare costantemente il sistema dei protocolli aziendali di prevenzione dei reati ex Decreto e l'applicazione del sistema di *Corporate Governance*, suggerendo, se del caso, le modifiche necessarie.

Su di un piano più operativo sono affidati all'OdV i seguenti compiti:

- ❖ attivare le procedure di controllo, tenendo presente che una responsabilità primaria sul controllo delle attività, soprattutto per quelle relative alle aree a rischio, resta comunque demandata ai Vertici e a tutti i Responsabili di funzione e forma parte integrante dei controlli di primo livello;
- ❖ verificare periodicamente le aree a rischio reato al fine di adeguare la mappatura delle stesse ai mutamenti dell'attività e/o della struttura aziendale. A tal fine gli Amministratori e i Responsabili delle singole funzioni devono segnalare all'OdV le eventuali situazioni in grado di esporre l'azienda al rischio di reato. Queste comunicazioni, come tutte le altre effettuate nel contesto del Decreto, devono essere documentate (se sufficiente via e-mail oppure con report specifici) in quanto devono essere sempre formalmente "tracciate";
- ❖ effettuare periodicamente verifiche mirate su determinate operazioni o atti specifici, posti in essere nell'ambito delle aree di attività a rischio come definite nella Parte Speciale del Modello. Tali controlli saranno pianificati in un Piano di lavoro dell'OdV eventualmente rimodulabile in relazione a nuove esigenze. In ogni caso, l'Organismo potrà effettuare anche audit non pianificati ma disposti al momento;
- ❖ controllare che la diffusione del Modello sia avvenuta con riscontri diretti tra tutto il Personale;
- ❖ raccogliere, elaborare e conservare le informazioni (comprese le segnalazioni di cui al successivo paragrafo 4.4) rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere obbligatoriamente trasmesse allo stesso OdV;
- ❖ condurre, o far condurre da professionisti esterni, gli audit per la verifica di presunte violazioni delle prescrizioni del presente Modello;
- ❖ coordinarsi con le diverse funzioni aziendali per il monitoraggio delle attività nelle aree a rischio. L'OdV riceve dagli Amministratori e dai Responsabili delle funzioni aziendali comunicazione di ogni attività da essi svolta relativamente ad eventuali situazioni che possano esporre la SOCIETA' ai rischi di reato contemplati dal Decreto.

Inoltre, per lo svolgimento dei suoi compiti, l'OdV:

- ❖ gode dei più ampi poteri ispettivi e di accesso ai documenti aziendali;
- ❖ dispone di risorse finanziarie e professionali adeguate;
- ❖ si avvale del supporto e la cooperazione di tutte le funzioni aziendali che possano essere interessate o comunque coinvolte nelle attività di controllo. Quest'ultime daranno sempre la massima disponibilità e costante collaborazione, posto che i compiti che l'OdV andrà a svolgere sono non solo previsti nel presente Modello (che rappresenta un regolamento interno che la

SOCIETA' ha inteso adottare) ma anche dal Decreto 231, quindi da una legge nazionale che deve essere rispettata una volta che il CdA ha approvato il Modello medesimo;

- ❖ cura che tutta la documentazione raccolta per lo svolgimento delle verifiche e quella ricevuta come flusso informativo (periodico od occasionale) sia custodita in apposito archivio curato dallo stesso OdV.

4.3 *Flussi informativi dell'OdV nei confronti degli organi societari*

Sono assegnate all'OdV di LOGIC due linee di reporting:

- ❖ la prima, su base continuativa, direttamente con l'Amministratore Delegato, in esito agli audit condotti di volta in volta;
- ❖ la seconda, su base annuale, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale.

L'OdV di LOGIC potrà essere convocato in qualsiasi momento dai suddetti Organi o potrà, a sua volta, presentare richiesta in tal senso, per riferire in merito all'efficacia e all'effettiva osservanza del Modello all'interno della SOCIETA' o in relazione a situazioni specifiche

4.4 *Flussi informativi nei confronti dell'OdV*

4.4.1 *Segnalazioni da parte di dipendenti aziendali o da parte di terzi*

In ambito aziendale dovrà essere portata a conoscenza dell'OdV, oltre ai flussi informativi periodici prescritti nei singoli protocolli e che riguardano le attività istituzionali della SOCIETA', ogni altra informazione, di qualsiasi tipo, proveniente anche da terzi ed attinente all'attuazione e all'osservanza del Modello.

Valgono al riguardo le seguenti prescrizioni:

- ❖ devono essere inviate all'OdV eventuali segnalazioni relative alla violazione del Modello (che, si sottolinea, comprende il Codice Etico, il Modello, i protocolli e l'intero sistema delle certificazioni) o comunque conseguenti a comportamenti non in linea con le regole di condotta adottate da Logic;
- ❖ l'OdV valuterà le segnalazioni ricevute e le eventuali conseguenti iniziative a sua ragionevole discrezione e responsabilità, raccogliendo, se del caso, ulteriori informazioni direttamente dal segnalante e/o dal responsabile della presunta violazione, redigendo un apposito verbale dell'incontro e motivando per iscritto le sue decisioni in merito;
- ❖ le segnalazioni dovranno avere ad oggetto ogni violazione o sospetto di violazione del Modello. L'OdV agirà in osservanza delle vigenti norme in materia di *whistleblowing* (legge 179 del 2017) a tutela dell'identità del segnalante (che ora, con questa legge, è garantita anche nel settore privato), ponendosi (la segnalazione) come giusta causa di rivelazione di notizie coperte dal segreto di cui agli artt. 622 e 623 del Codice Penale e 2105 del Codice Civile. (rivelazione di segreto professionale, di segreti scientifici o industriali, obbligo di fedeltà). In merito si evidenzia che:
 - all'art. 6 del Decreto 231/2001 sono stati aggiunti i commi: 2bis, 2ter e 2quater;
 - questi commi dispongono, tra l'altro, l'adozione di uno o più canali che consentano, ai soggetti apicali e sottoposti, di presentare, a tutela dell'integrità dell'ENTE, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto 231 e fondate su elementi di fatto precisi e concordanti o di violazioni del Modello di Organizzazione, Gestione e

Controllo dell'ENTE, di cui siano venuti a conoscenza in ragione delle funzioni svolte. Tali canali garantiscono la riservatezza dell'identità del segnalante nella attività di gestione della segnalazione;

- almeno un canale alternativo di segnalazione idoneo a garantire la riservatezza dell'identità del segnalante sia adottato con modalità informatiche;
 - sia osservato il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
 - siano previste sanzioni disciplinari 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.
- ❖ al fine di facilitare il flusso di segnalazioni ed informazioni verso l'OdV, è stata istituita una casella di posta elettronica oltre quella tradizionale presso la sede della SOCIETA'.
- La e-mail è: org.vigilanzadlgs231-01@logic-spa.com
oppure: Organismo di Vigilanza presso LOGIC S.p.A., via Galileo Galilei n. 5, 20060 Cassina de Pecchi (Milano) se si vuole utilizzare il sistema cartaceo;
- ❖ le segnalazioni pervenute all'OdV devono essere raccolte e conservate in un apposito archivio al quale sia consentito l'accesso solo da parte dei membri dell'OdV o di altri soggetti appositamente autorizzati dal Presidente dell'OdV medesimo;
- ❖ le segnalazioni anonime saranno vagliate dall'Organismo di Vigilanza che potrà archivarle o svilupparle con specifici approfondimenti e controlli. In ogni caso l'OdV motiverà sempre, caso per caso, le sue scelte e valutazioni verbalizzandole nei suoi atti.

4.4.2 *Ulteriori obblighi di informativa relativi alle attività degli organi della Pubblica Amministrazione.*

Oltre alle segnalazioni di cui al paragrafo precedente, devono essere obbligatoriamente e tempestivamente trasmesse all'OdV di LOGIC le informative concernenti:

- ❖ i provvedimenti e/o notizie provenienti da organi di Polizia Giudiziaria o da qualsiasi altra Autorità pubblica, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto;
- ❖ qualsiasi attività ispettiva svolta da organi pubblici nei confronti della SOCIETA', sia al suo inizio sia al termine, riportando la sintesi del suo esito e allegando i rispettivi verbali se richiesti dall'OdV;
- ❖ le domande di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
- ❖ l'inosservanza delle regole del Decreto;
- ❖ le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- ❖ i rapporti preparati dai Responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo dai quali possano emergere fatti, atti, eventi od omissioni relativi al rispetto del Decreto e del Modello.

4.4.3 *Articolazione dei Poteri e Sistema delle deleghe*

All'OdV deve essere comunicata l'articolazione dei poteri e il sistema delle deleghe adottato da LOGIC e ogni modifica di essi. A tal fine sarà elaborato un organigramma con il quale saranno evidenziati i soggetti in possesso di procure e/deleghe.

4.4.4 *Struttura organizzativa*

All'OdV, infine, deve essere comunicata la struttura organizzativa di LOGIC ed ogni modifica che intervenga sulla stessa. All'uopo sarà inviato all'OdV l'organigramma.

5 FORMAZIONE DEL PERSONALE E DIFFUSIONE DEL MODELLO NEL CONTESTO AZIENDALE E ALL'ESTERNO.

5.1 *Formazione del personale*

LOGIC promuove la conoscenza del Modello, del Codice Etico, nonché dei relativi protocolli aziendali tra tutti i Dipendenti che sono pertanto tenuti a conoscerne il contenuto, ad osservarli e contribuire alla loro efficace attuazione.

A tal fine la funzione del Personale gestisce, in cooperazione con l'OdV, la formazione del Personale che sarà articolata sui livelli qui di seguito indicati:

- ❖ Personale dirigenziale e con funzioni di rappresentanza dell'ENTE (gli apicali): moduli di formazione in aula svolti dal formatore; informativa al momento dell'assunzione dell'incarico; accesso al sito intranet della SOCIETA' nella parte dedicata, oltre al Modello completo, anche alle slide utilizzate dal suddetto formatore;
- ❖ altro Personale dipendente (i sottoposti): moduli di formazione in aula svolti dal formatore; informativa in sede di assunzione; accesso al sito intranet contenente le stesse informazioni di cui alla precedente alinea; e-mail di aggiornamento;
- ❖ al momento della assunzione di ogni dipendente di qualsiasi livello, compresi gli Amministratori, i Sindaci e i Revisori, con apposita informativa e accettazione della stessa.

5.2 *Informativa a collaboratori esterni e partner*

LOGIC promuove la conoscenza e l'osservanza del Modello e del Codice Etico anche tra i partner commerciali e finanziari, i consulenti, gli intermediari, i collaboratori, anche occasionali, i tirocinanti, gli agenti, i clienti ed i fornitori, e, in generale, con chiunque vengano instaurati rapporti in nome e per conto della SOCIETA'.

A tal fine nel sito istituzionale della LOGIC sarà inserito il Codice Etico e la Parte Generale del Modello in maniera da renderli conoscibili a tutti gli stakeholder in assoluta trasparenza.

A questi verrà pertanto fornita informativa sui principi, le politiche e i protocolli che LOGIC ha adottato sulla base del Modello anche a mezzo delle clausole contrattuali che, coerentemente a detti principi e politiche, verranno adottate dalla SOCIETA' e inserite nei contratti stessi.

6 SISTEMA DISCIPLINARE IN CASO DI MANCATA OSSERVANZA DELLE PRESCRIZIONI DEL MODELLO.

6.1 Principi generali

LOGIC prende atto e afferma che la predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole contenute nel Codice Etico, nonché nei protocolli, nel Modello e nel sistema delle certificazioni è condizione essenziale per assicurare l'effettività e l'efficacia del Modello stesso.

Al riguardo, infatti, lo stesso articolo 6 comma 2, lettera e), del D. Lgs. n. 231/'01 prevede che i Modelli di organizzazione, gestione e controllo devono "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento instaurato dalla Pubblica Autorità nei confronti della persona fisica e/o dell'ENTE, in quanto le regole di condotta imposte dal Modello sono assunte da LOGIC in piena autonomia e indipendentemente dalla tipologia di illecito che le violazioni del Modello possono determinare nelle diverse discipline giuridiche.

6.2 Sanzioni per i lavoratori dipendenti

6.2.1 Personale dipendente in posizione non dirigenziale

I comportamenti tenuti dai lavoratori dipendenti in violazione delle norme contenute nel presente Modello sono definiti come illeciti disciplinari.

Con riferimento alla tipologia di sanzioni irrogabili nei loro riguardi, esse rientrano tra quelle previste dal Contratto Collettivo Nazionale di Lavoro per gli addetti all'industria metalmeccanica privata (d'ora innanzi per brevità "CCNL"), nel rispetto delle procedure previste dall'articolo 7 della Legge n. 300/1970 (d'ora innanzi, per brevità, "Statuto"), dalle eventuali normative speciali applicabili e dai rispettivi CCNL.

La violazione da parte del Personale dipendente delle norme del presente Modello (ivi incluso il Codice Etico) nonché dei protocolli aziendali nonché del sistema delle certificazioni può dar luogo, secondo la gravità della violazione stessa, ai seguenti provvedimenti, che vengono disposti in applicazione dei principi di proporzionalità, nonché dei criteri di correlazione tra infrazione e sanzione e, comunque, nel rispetto della forma e delle modalità previste dalla normativa vigente.

In particolare, in applicazione dei "criteri di correlazione tra le mancanze dei lavoratori ed i provvedimenti disciplinari" contenuti nel vigente CCNL, si prevede che:

- incorre nel provvedimento di rimprovero verbale (o scritto), multa, sospensione dal lavoro o dalla retribuzione, il lavoratore che: violi le procedure/protocolli interni previsti dal sistema di certificazione e dal presente Modello (ad esempio, ometta di dare comunicazione all'OdV dei flussi informativi, ometta di svolgere controlli di primo livello) o adotti, nell'espletamento delle sue attività un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare in tali comportamenti una "non esecuzione degli ordini impartiti dall'azienda sia in forma scritta che verbale" di cui ai suddetti criteri di correlazione;
- incorre nel provvedimento di licenziamento con preavviso il lavoratore che adotti, nell'espletamento delle sue attività, un comportamento non conforme alle prescrizioni del

presente Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, dovendosi ravvisare in tale comportamento un atto tale da far venire meno radicalmente la fiducia dell'azienda nei confronti del lavoratore di cui ai suddetti criteri di correlazione a prescindere dall'apertura di una indagine a carico della SOCIETA';

- incorre, infine, nel provvedimento di licenziamento senza preavviso il lavoratore che adotti, nell'espletamento delle sue attività, un comportamento palesemente in violazione delle prescrizioni del presente Modello, tale da determinare, da parte del Pubblico Ministero a carico della SOCIETA', il provvedimento di inizio indagine per un reato previsto dal Decreto, dovendosi ravvisare nel suddetto comportamento, una condotta tale da provocare alla SOCIETA' grave nocumento materiale e di reputazione.

Il tipo e l'entità di ciascuna sanzione saranno applicate in relazione:

- a. all'intenzionalità del comportamento e del conseguente evento (valutandone il dolo) o grado di negligenza, imprudenza o imperizia (in caso di colpa) con riguardo anche alla prevedibilità dell'evento;
- b. al comportamento complessivo del dipendente, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- c. alle sue mansioni;
- d. alla sua posizione funzionale;
- e. ad altre particolari, eventuali circostanze.

6.2.2 *Dirigenti*

In caso di violazione da parte dei Dirigenti delle norme del presente Modello (ivi incluso il Codice Etico) nonché dei protocolli aziendali e del sistema delle certificazioni, nell'espletamento delle loro attività, di un comportamento non conforme alle prescrizioni sopra citate, si provvederà ad applicare nei loro confronti la misura disciplinare più idonea in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti industriali.

6.3 *Misure nei confronti degli Amministratori e dei Sindaci*

Nel caso di violazione del Modello da parte degli Amministratori o dei Sindaci di LOGIC, l'OdV ne informerà il Consiglio di Amministrazione ed il Collegio Sindacale, i quali procederanno alla convocazione dell'Assemblea degli Azionisti per deliberare in merito alla assunzione delle opportune iniziative previste dalla normativa e, se necessario, alla revoca del mandato.

6.4 *Misure nei confronti di collaboratori esterni, partner, intermediari*

Ogni comportamento posto in essere dai collaboratori, anche occasionali, consulenti, intermediari, tirocinanti, agenti di LOGIC o da partner commerciali, in contrasto con le linee di condotta indicate dal presente Modello e dal Codice Etico potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali, la risoluzione immediata del rapporto, fatta salva l'eventuale richiesta di risarcimento di eventuali danni derivanti alla SOCIETA'.

La funzione Amministrazione, Finanze e Controllo cura, con l'eventuale collaborazione dell'OdV, l'elaborazione, l'aggiornamento e l'inserimento nelle lettere di incarico o nei contratti, di tali specifiche clausole che possono prevedere anche l'eventuale richiesta di risarcimento del danno, derivante alla SOCIETA' dall'applicazione delle sanzioni previste dal Decreto, nei confronti delle controparti negoziali.

Particolare attenzione sarà posta al momento della scelta del consulente, partner, intermediario, fornitore e cliente nel senso che saranno verificate eventuali loro condanne penali per i reati presupposto e/o di condanna degli enti in base al Decreto avvalendosi anche delle dichiarazioni previste dal DPR. 445 del 2000, ex art. 46, sia per le persone fisiche sia per gli enti stessi. Le clausole contrattuali potranno utilmente essere adoperate anche per questo presidio preventivo.

7 ATTIVITA' DI VERIFICA SULL'APPLICAZIONE E SULL'ADEGUATEZZA DEL MODELLO DA PARTE DELLA STRUTTURA AZIENDALE.

Il Modello, oltre agli audit svolti dall'OdV, sarà soggetto a due tipologie di verifiche da parte dei Responsabili di funzione:

- I. attività di monitoraggio - semestrale - sull'attuazione e l'osservanza del Modello (cioè nella verifica della coerenza tra i comportamenti concreti dei destinatari ed il Modello stesso) attraverso dichiarazioni periodiche (semestrali) da parte degli apicali con le quali si attesta che non sono state poste in essere azioni in contrasto con il Modello. In particolare, che:
 - a. sono state rispettate le indicazioni ed i contenuti del Codice Etico e del presente Modello;
 - b. sono stati rispettati i poteri di delega ed i limiti di firma;
 - c. eventuali deroghe ai protocolli sono state preventivamente autorizzate dagli organi sovraordinati oppure ratificate in caso di urgenza e necessità.

I Responsabili di funzione hanno il compito di trasmetterle, dopo averle viste e integrate, se del caso, con le dichiarazioni dei propri sottoposti, all'OdV che ne curerà l'archiviazione ed effettuerà a campione, come da suo piano delle verifiche, i relativi controlli.

- II. verifiche dei protocolli: l'effettivo funzionamento del Modello sarà costantemente verificato comunicandone, semestralmente, l'esito all'OdV. Inoltre, sarà intrapresa una revisione di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni correttive e di miglioramento suggerite dall'OdV e dagli altri soggetti interessati, degli eventi considerati rischiosi, della consapevolezza del personale rispetto alle ipotesi di reato previste dal Decreto.

L'esito di tale attività, con la sottolineatura di eventuali criticità riscontrate ed i suggerimenti proposti per le azioni correttive e di miglioramento, sarà incluso nella relazione annuale che l'OdV invia al Consiglio di Amministrazione e al Collegio Sindacale.

ALLEGATI

- I) Codice Etico
- II) Struttura organizzativa di LOGIC S.p.A.
- III) Articolazione dei poteri e sistema delle deleghe
- IV) Elenco reati presupposto del Decreto 231 aggiornato al mese di maggio 2018.

PARTE SPECIALE

PREMESSA

1 PRINCIPI DEL SISTEMA DI CONTROLLO “231”

I principi di controllo che sono alla base del sistema “231” sono qui di seguito indicati:

- a) **procedure:** esistenza di disposizioni aziendali idonee a fornire principi di comportamento, ruoli e responsabilità, modalità operative e controlli per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione. La Società ha in corso l’adeguamento delle procedure finalizzato all’aggiornamento e alla revisione dell’intero sistema organizzativo dell’azienda;
- b) **tracciabilità e verificabilità ex post delle transazioni:** per ogni operazione c’è un adeguato supporto documentale di ausilio ai controlli attraverso i quali sono provate sia le caratteristiche sia le motivazioni della transazione individuando il soggetto che ha richiesto, che ha autorizzato, che ha effettuato, che ha registrato, che ha verificato. La tutela di dati e procedure in ambito informatico può essere assicurata mediante l’adozione di idonee misure tecniche di sicurezza;
- c) **segregazione dei compiti:** il sistema “231” deve garantire la sussistenza del principio di separazione delle funzioni, per cui l’autorizzazione all’effettuazione di un’operazione deve essere sotto la responsabilità di persona diversa da chi esegue operativamente o controlla l’operazione stessa. Inoltre, occorre che: i) i poteri e le responsabilità siano sempre chiaramente definiti e conosciuti all’interno dell’organizzazione; ii) i poteri autorizzativi e di firma siano coerenti con le procure e le deleghe date e ricevute da ogni persona con compiti definiti di responsabilità. La separazione delle funzioni può essere regolata anche attraverso l’utilizzo di sistemi informatici che abilitano alcune operazioni solo ad alcune persone specificatamente autorizzate;
- d) **sistema di poteri coerente con le responsabilità organizzative assegnate:** i poteri autorizzativi e di firma assegnati devono essere: i) coerenti con le responsabilità organizzative e gestionali assegnate; ii) chiaramente definiti e conosciuti all’interno di LOGIC. Sono definiti i ruoli aziendali ai quali è assegnato il potere di impegnare la Società in determinate spese specificando i limiti e la natura delle spese. Per la salute e sicurezza sui luoghi di lavoro sarà rispettato quanto previsto dall’art.16 del TU 81 del 2008;
- e) **disciplina formale delle deroghe** a quanto previsto dal sistema organizzativo. Di ogni deroga dovranno sempre essere tracciate: la motivazione, il soggetto che è operato in deroga e quello che ha autorizzato/ratificato. Di esse sarà sempre informato l’OdV attraverso un flusso informativo almeno semestrale.

Codice Etico, Modello di organizzazione, gestione e controllo: tutte le attività sensibili sono svolte coerentemente ai principi di comportamento e alle regole contenute nella predetta documentazione.

2 STRUMENTI DI CONTROLLO

2.1 Sistema di controllo interno

Il sistema di controllo interno è costituito dall'organizzazione, dai principi, dalle regole di comportamento ed operative e dalle procedure aventi lo scopo di monitorare il rispetto delle policy ed il conseguimento delle seguenti finalità:

- efficacia ed efficienza dei processi e operazioni aziendali;
- qualità e affidabilità dell'informazione economico-finanziaria;
- rispetto di leggi e regolamenti, delle norme e delle procedure aziendali.

In particolare, nell'ambito del sistema di controllo interno, LOGIC ha adottato e aggiorna:

- il Codice Etico, che esprime i valori ed i principi di comportamento, ai quali si attribuisce un valore etico e che indirizzano l'attività aziendale in un percorso di trasparenza e di correttezza, all'interno e all'esterno dell'ente;
- il presente Modello di organizzazione, gestione e controllo, redatto ai sensi del D.Lgs. 231/2001, che ha come obiettivo quello di rappresentare in modo organico e strutturato i principi di prevenzione dei reati richiamati dal suddetto decreto, tra cui, in particolare, quelli commessi a danno della Pubblica Amministrazione e quelli indicati nella presente parte speciale;
- le disposizioni organizzative, con cui vengono definite, comunicate ed attuate le scelte aziendali;
- il Manuale Sistema Gestione Qualità ed Organizzazione la cui ultima edizione di aggiornamento (la 21^a) è di ottobre 2017;
- i protocolli, le procedure, le istruzioni operative e tutti gli adempimenti previsti dalle certificazioni nazionali, internazionali e di Stati esteri che regolano singole attività o processi aziendali affinché LOGIC sia scelta e resti tra i fornitori ufficiali dei prodotti aeronautici, che la stessa Società progetta o produce, dei clienti sia privati sia appartenenti alla Pubblica Amministrazione nazionale ed estera. Per ultima, ma non ultima, la legge 185 del 1990 alla quale LOGIC deve rifarsi, sin dalla contrattazione, per molto della sua progettazione e produzione.

Da sottolineare l'importanza svolta dai controlli di primo livello e quelli dell'Organismo di Vigilanza, avendo essi lo scopo di assicurare un costante e sistematico monitoraggio: i) delle attività aziendali, in particolare quelle sensibili perché comprese nelle aree aziendali dove vengono svolte tutte quelle operazioni indicate nelle diverse Sezioni di questa Parte Speciale del Modello; ii) dei rispettivi rischi individuando per essi le opportune azioni di mitigazione, proponendo e attuando le azioni correttive e di miglioramento.

È il caso di sottolineare che l'OdV, nella sua autonomia e indipendenza, se lo riterrà necessario per le specifiche professionalità e competenze richieste, potrà disporre audit - su determinate attività aziendali - svolti da terze parti (consulenti esterni) anche utilizzando il budget a sua disposizione.

Per quanto sopra, ritenuta ed esclusa la rilevanza (essendo il rischio di grado basso) dei reati presupposto del Decreto 231 non indicati nelle sezioni di questa parte speciale, si considerano rilevanti quei reati che, al contrario, vengono elencati e per i quali sono adottati gli specifici presidi

di controllo di cui al presente Modello e ai sistemi di certificazioni sopra evidenziati anche tenendo conto:

- delle attività aziendali;
- del particolare mercato in cui opera la Società;
- dei rapporti commerciali posti in essere;
- delle interviste e dei colloqui svolti con i Vertici dell'Ente e con i Responsabili di funzione.

2.2 *Sistema delle Procedure*

Il Codice, il Modello 231, il Manuale, le procedure, le istruzioni operative adottate da LOGIC hanno come obiettivo la definizione di precise regole operative per la gestione delle attività e dei processi aziendali tra cui quelli valutati sensibili e indicati in questa parte speciale del Modello stesso.

Tale sistema procedurale è per sua natura dinamico, in quanto soggetto alle mutabili esigenze operative e gestionali dell'azienda tra cui, per esempio, variazioni organizzative, mutate esigenze commerciali, abrogazioni di norme, nuove leggi e regolamenti, nuovi reati presupposto inseriti nel catalogo del Decreto231.

Questo comporta il suo costante aggiornamento del quale dovrà avere cura, in primis, l'Organismo di vigilanza essendo esso compreso tra i suoi compiti (art. 6, comma 1, lettera b del Decreto231).

Il sistema organizzativo è adeguatamente diffuso e reso disponibile a tutti i destinatari del Modello nelle forme ritenute più efficaci (per esempio, mediante la rete intranet aziendale accessibile dal Personale appartenente a LOGIC).

SEZIONE "A"

Art. 24 del Decreto 231

Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico

Art. 25 del Decreto 231

Concussione, induzione indebita a dare o promettere utilità e corruzione

Art. 25 decies del Decreto 231

Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

Il D.Lgs. 231/2001, agli artt. 24, 25 e 25 decies, prevede i reati contro la Pubblica Amministrazione, il patrimonio della stessa e contro l'Amministrazione della Giustizia, disciplinati dal Codice Penale e che sono stati individuati come presupposto della responsabilità dell'ente.

Tali reati affinché rilevino ai sensi del D.Lgs. 231/2001 devono essere commessi "da soggetti che rivestono funzioni apicali ovvero da soggetti che con questi collaborino (sottoposti) ma sempre "nell'interesse e/o a vantaggio dell'ente".

In relazione all'attività svolta dalla Società sono state ritenute potenzialmente rilevanti le seguenti fattispecie di reato:

- **Concussione (art. 317 c.p.):** è il reato commesso dal pubblico ufficiale o dall'incaricato di pubblico servizio che, abusando della propria qualità o dei propri poteri, costringe taluno a dare o promettere indebitamente denaro o altra utilità a sé o ad altri;
- **Corruzione per l'esercizio della funzione o per atto contrario ai doveri d'ufficio e corruzione di persona incaricata di un pubblico servizio (artt. 318 – 319 - 320 c.p.):** tali reati sono costituiti dalla condotta del pubblico ufficiale o dell'incaricato di pubblico servizio che, per l'esercizio delle sue funzioni o dei suoi poteri, o in alternativa per l'omissione o il ritardo di un atto del suo ufficio, ovvero per il compimento di un atto contrario ai doveri di ufficio, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.
- **Corruzione in atti giudiziari (art. 319-ter c.p.):** la condotta tipica di questo reato è la stessa dei reati di cui all'art. 318 e 319, con la differenza nella finalità, quella di favorire o danneggiare una parte in un processo civile, penale o amministrativo.
- **Induzione indebita a dare o promettere utilità (art. 319-quater c.p.):** il reato è costituito dal comportamento di un pubblico ufficiale o di un incaricato di pubblico servizio che, abusando della propria qualità o dei propri poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.
- **Istigazione alla corruzione (art. 322 c.p.):** punisce chiunque offre o promette denaro o altra utilità non dovuti a un pubblico ufficiale o a un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri o per la commissione di un atto contrario, nel caso in cui l'offerta e la promessa non sia accettata, nonché il pubblico ufficiale o l'incaricato di pubblico servizio che sollecita la dazione indebita di denaro o altra utilità.
- **Malversazione a danno dello Stato (art. 316 bis c.p.):** il reato è commesso da chi, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità.
- **Indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.)** è il conseguimento indebito, per sé o per altri, di contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute.

- **Truffa in danno allo Stato, di altro ente pubblico o dell'Unione Europea (art. 640, comma 2, n. 1 c.p.):** il reato consiste nel conseguimento di un ingiusto profitto in danno di tali enti indotti in errore mediante artifici o raggiri.
- **Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.):** la fattispecie si differenzia dalla precedente perché la condotta ha ad oggetto contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.
- **Frode informatica (se il fatto è commesso in danno dello Stato o di altro Ente Pubblico) (art. 640 ter c.p.):** Il reato è commesso da chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.
- **Concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (art. 322 bis c.p.):** il reato estende la configurabilità dei reati indicati in rubrica anche nell'ipotesi in cui in luogo del pubblico ufficiale o dell'incaricato di pubblico servizio sia coinvolto un membro degli organi delle Comunità europee o un funzionario delle medesime o di Stati esteri.
- **Istigazione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.):** il reato può essere commesso da chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere.

In evidenza qui le definizioni di soggetto "attivo" ai fini dei reati presupposto del Decreto 231 (gli appartenenti all'ente) e delle conseguenti prescrizioni del Modello di Organizzazione Gestione e Controllo della Società, e soggetti "passivi" i seguenti soggetti individuati negli articoli del Codice Penale:

- art. 357, in riferimento al Pubblico Ufficiale, inteso come colui il quale "esercita una pubblica funzione legislativa, giudiziaria o amministrativa"²;
- art. 358, in riferimento all'Incaricato di Pubblico Servizio, inteso come colui il quale "a qualunque titolo, presta un pubblico servizio"³;

Nell'ambito dei soggetti che svolgono pubbliche funzioni, la qualifica di pubblico ufficiale è poi riservata a coloro che formano o concorrono a formare la volontà della P.A. o che svolgono tale

² Dallo stesso articolo la "funzione pubblica amministrativa" è definita come "disciplinata da norme di diritto pubblico e da atti autorizzativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autorizzativi o certificativi".

³ Per "pubblico servizio" deve intendersi "un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

attività per mezzo di poteri autoritativi o certificativi, mentre quella di incaricato di pubblico servizio è assegnata dalla legge in via residuale a coloro che non svolgono pubbliche funzioni ma che svolgano attività diretta al soddisfacimento di bisogni di interesse pubblico, purché non svolgano semplici mansioni di ordine, né prestino opera meramente materiale.

Al fine di individuare se l'attività svolta da un soggetto possa essere qualificata come pubblica, ai sensi e per gli effetti di cui agli art. 357 e 358 c.p., è necessario verificare se essa sia disciplinata da norme di diritto pubblico, quale che sia la connotazione soggettiva del suo autore, distinguendosi poi - nell'ambito dell'attività definita oggettivamente pubblica - la pubblica funzione dal pubblico servizio per la presenza (nell'una) o la mancanza (nell'altro) dei poteri tipici della potestà amministrativa, come indicati dal comma 2 del predetto art.357. Il pubblico servizio è infatti un'attività non autoritativa, accessoria o complementare ad una pubblica funzione, che non può coincidere in un lavoro meramente manuale.

Tra tali elementi, che devono costituire oggetto di analisi da parte di tutti i Destinatari del presente Modello e che, nel dubbio, devono essere interpretati secondo un principio estensivo di prudenza, si menzionano a titolo non esaustivo:

- il fatto che l'attività dell'Ente sia finanziata in modo maggioritario dallo Stato, dalle Regioni, dagli Enti Locali, da altri enti pubblici o da organismi di diritto pubblico o che la gestione dello stesso sia sottoposta al loro controllo ovvero condotta con organismi di amministrazione, direzione o vigilanza costituiti in misura non inferiore alla metà da componenti designati dai medesimi soggetti;
- il fatto che l'Ente derivi dalla trasformazione di un "ente pubblico economico" (ad es. IRI, INA, ENI, ENEL) fino a quando sussista una partecipazione esclusiva o maggioritaria dello Stato al capitale azionario;
- il fatto che l'Ente sia sottoposto ad un regime di controllo pubblico, di carattere funzionale o strutturale, da parte dello Stato o di altra Pubblica Amministrazione;
- il fatto che l'Ente possa o debba compiere atti in deroga al diritto comune ovvero che possa godere di c.d. "istituti di privilegio" ovvero che sia titolare di poteri amministrativi in senso tecnico (ad esempio in virtù di concessioni, diritti speciali o esclusivi concessi dall'autorità secondo le norme vigenti);
- il fatto che l'Ente ed i soggetti attivi in esso operanti, svolgano attività ricollegabili a interessi pubblici e, in particolare, siano incaricati di servizi pubblici essenziali quali, a titolo non esaustivo:
 - la sanità;
 - l'igiene pubblica;
 - la protezione civile;
 - la raccolta e lo smaltimento dei rifiuti;
 - le dogane;
 - i servizi di supporto ed erogazione in merito all'assistenza e la previdenza sociale.

A titolo esemplificativo, rivestono la qualifica di Pubblico Ufficiale e/o di Incaricato di Pubblico Servizio: dipendenti comunali non esercenti attività meramente materiale, componenti della Commissione gare d'appalto indette dalla P.A., militari della Guardia di Finanza o dei Carabinieri,

Vigili Urbani, componenti dell'Ufficio Tecnico del Comune, curatore (in qualità di organo del fallimento), impiegato addetto al rilascio di certificati presso la cancelleria di un Tribunale, medico dipendente del Servizio Sanitario Nazionale, ispettore ASL.

In considerazione della specificità delle attività aziendali svolte da LOGIC e della sua struttura interna, le principali attività sensibili e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- selezione e avanzamento in carriera del Personale;
- affidamento di lavori, servizi e forniture;
- affidamento di incarichi per consulenze di natura legale, tecnica, economico-finanziaria;
- attività di rappresentanza istituzionale e commerciale con le pubbliche amministrazioni;
- gestione rimborsi spese a dipendenti e spese di rappresentanza;
- gestione adempimenti ed operazioni in materia societaria;
- predisposizione del bilancio di esercizio;
- gestione dei procedimenti e dei contenziosi giudiziari e stragiudiziali (civili, penali, amministrativi e tributari), nomina dei legali e coordinamento della loro attività;
- gestione rapporti con l'amministrazione finanziaria e ispezioni da parte dell'Amministrazione Tributaria e Organi di Polizia Tributaria in occasione di controlli e accertamenti;
- omaggi, donazioni, sponsorizzazioni, attività promozionali ed erogazioni liberali;
- adempimenti a tutela della privacy;
- gestione dei flussi finanziari e delle attività di tesoreria;
- richiesta, acquisizione e gestione di contributi e finanziamenti pubblici;
- gestione delle verifiche sul sistema di controllo interno concernenti le certificazioni;
- progetti per la concessione dei contributi europei;
- partecipazione a bandi di gara nazionali, europei e di altri Stati.

1 Principi di comportamento

I seguenti principi di comportamento si applicano ai Destinatari del presente Modello che, a qualunque titolo, intrattengano rapporti con la Pubblica Amministrazione (quindi con Pubblici Ufficiali e Incaricati di Pubblico Servizio) per conto o nell'interesse della Società ovvero a coloro che hanno rapporti diretti o indiretti con l'Autorità Giudiziaria, in relazione a circostanze oggetto di attività processuale attinenti alla Società stessa.

A tali Destinatari è fatto divieto di porre in essere, collaborare o realizzare comportamenti tali che integrino o possano costituire, direttamente o indirettamente, i reati previste dagli artt. 24, 25, e 25 - *decies* del Decreto²³¹. È proibito porre in essere comportamenti che determinino situazioni di conflitto di interesse nei confronti di rappresentanti della Pubblica Amministrazione ovvero creino degli ostacoli all'Autorità Giudiziaria.

In particolare, coerentemente con i principi etici aziendali espressi nel Codice Etico della Società, è fatto divieto di:

- promettere o effettuare erogazioni in denaro a favore di rappresentanti della Pubblica Amministrazione, italiana o straniera, per finalità diverse da quelle istituzionali e di servizio e in violazione delle prescrizioni normative;
- distribuire omaggi e regali eccedenti quanto previsto dal Codice Etico e dal presente Modello (in ogni caso ogni forma di regalia eccedente le normali pratiche di cortesia o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale. A tal proposito, si evidenzia che il Codice di Comportamento dei dipendenti pubblici, DPR. 62 del 2013, prevede che, di norma, il valore degli omaggi non superi 150 euro). In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa) o a loro familiari, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda;
- promettere o concedere vantaggi di qualsiasi natura (come le assunzioni o le promesse di esse, gli affidamenti di consulenze a familiari o conoscenti, contributi vari) in favore di rappresentanti della Pubblica Amministrazione, italiana o straniera, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda;
- decidere spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;
- erogare prestazioni o compensi in favore di collaboratori, fornitori, consulenti, partner o altri soggetti terzi che operano per conto della Società e che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi e/o in relazione al tipo di incarico da svolgere e alla prestazione effettivamente resa e documentata;
- favorire, negli acquisti, collaboratori, fornitori, consulenti o altri soggetti terzi in quanto indicati dai rappresentanti della Pubblica Amministrazione, italiana o straniera, come condizione per ottenere vantaggi dagli stessi;
- fornire o promettere di rilasciare informazioni e/o documenti riservati;
- promettere/offrire denaro o qualsivoglia utilità ovvero ricorrere all'uso di violenza o minaccia, al fine di indurre un soggetto chiamato a testimoniare a non rilasciare dichiarazioni ovvero a rilasciare dichiarazioni false davanti all'Autorità Giudiziaria, qualora tali dichiarazioni possano essere utilizzate all'interno di un processo penale.

I divieti sopra rappresentati si intendono estesi anche ai rapporti indiretti (attraverso parenti, affini ed amici) con i rappresentanti della Pubblica Amministrazione, italiana o straniera.

Inoltre, nei confronti della Pubblica Amministrazione, italiana o straniera - così come nei confronti di privati - è fatto divieto di:

- esibire documenti con dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre la Pubblica Amministrazione in errore di valutazione tecnico-economica dei prodotti

offerti/servizi forniti. Omettere informazioni dovute al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione;

- fornire informazioni o dichiarazioni non veritiere al fine di ottenere erogazioni, contributi, sovvenzioni o finanziamenti ovvero destinare erogazioni, contributi, sovvenzioni o finanziamenti a finalità diverse da quelle per le quali sono stati ottenuti.

In relazione alle attività svolte per ottenere, concessioni, erogazioni, contributi, sovvenzioni o finanziamenti pubblici, i Destinatari coinvolti dovranno rispettare le seguenti regole:

- le modalità di gestione delle richieste di contributi, erogazioni, sovvenzioni, concessioni e finanziamenti pubblici, con particolare riferimento all'identificazione dei ruoli e delle responsabilità dei soggetti, nonché delle Funzioni che interagiscono con la Pubblica Amministrazione e che sono coinvolte nelle fasi istruttorie, devono essere preventivamente formalizzate;
- devono essere effettuate specifiche attività di controllo, sia sulla predisposizione della documentazione (ad esempio in merito alla conformità della documentazione di progetto e della documentazione attestante i requisiti tecnici, economici e professionali della Società), sia sul rispetto degli stati di avanzamento previsti dal progetto, nonché sulla correttezza e completezza delle relative attività di rendicontazione. Tali controlli sono finalizzati a verificare il rispetto dei requisiti comunicati dall'Ente Pubblico erogante;
- deve essere garantita la separazione tra chi gestisce le attività oggetto dell'erogazione, contributo, sovvenzione, concessione o finanziamento agevolato, chi è responsabile della relativa rendicontazione e chi ha deciso di domandarla;
- per ogni progetto deve essere predisposto un piano di informazione, verso tutte le strutture coinvolte, circa le regole riguardanti l'attuazione degli interventi finanziati e la loro successiva gestione;
- la documentazione fornita ai funzionari della Pubblica Amministrazione deve essere adeguatamente autorizzata, tracciata e archiviata;
- è fatto inoltre assoluto divieto di fornire informazioni o dichiarazioni non veritiere al fine di ottenere concessioni, erogazioni, contributi, sovvenzioni o finanziamenti ovvero destinare erogazioni, contributi, sovvenzioni o finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti.

Ai Destinatari del Codice Etico e del Modello che intrattengono rapporti con la Pubblica Amministrazione deve essere formalmente conferito potere in tal senso, con apposita procura/delega per i dipendenti o gli Amministratori o con specifica indicazione contrattuale per consulenti o partner. Quando necessario sarà rilasciata a tali soggetti specifica procura.

In occasione di incontri con rappresentanti della Pubblica Amministrazione o di Incaricati di Pubblico Servizio, devono essere seguite, in assenza di diverse specifiche indicazioni da parte dei funzionari pubblici (come è il caso delle ispezioni o perquisizioni), le seguenti regole:

- agli incontri, tenuti presso la sede di LOGIC o presso gli uffici dell'Ente Pubblico, dovranno di norma partecipare almeno due soggetti;

- i partecipanti dovranno controllare il contenuto del verbale relativo all'incontro per la condivisione e prima che sia predisposta la versione definitiva dello stesso o comunque subito dopo averne ricevuto copia dall'Ente Pubblico, verificando che da tale documento ci sia la rappresentazione corretta dell'evento;
- qualora l'Ente Pubblico non provveda a fornire il verbale, i partecipanti dovranno predisporre un verbale interno che descriva in modo completo, corretto e veritiero i fatti avvenuti durante l'incontro da allegare alla scheda di evidenza prevista da questo Modello.

In relazione ai rimborsi di spese sostenute da dipendenti o collaboratori la Società definisce le regole e i criteri da applicare alla richiesta, all'autorizzazione e all'erogazione del rimborso.

I dipendenti o collaboratori che facciano richiesta di rimborsi spese sono tenuti alla predisposizione della nota spese.

Le spese di rappresentanza sono rimborsate solo se motivate e pertinenti con l'attività svolta, proporzionate alla tipologia di acquisto, validamente documentate e solo se sostenute nel rispetto della normativa.

In relazione agli adempimenti finalizzati all'ottenimento di autorizzazioni, licenze, concessioni o permessi nonché alla gestione dei rapporti con gli Enti in caso di ispezioni, accertamenti e contenziosi, i Destinatari del presente Modello, in particolare i Responsabili di Funzione, sono tenuti a porre in essere tutti i controlli necessari per:

- assicurare che tutte le informazioni trasmesse agli Enti di riferimento in forma scritta, anche attraverso l'uso di sistemi info-telematici siano:
 - predisposte nel rispetto della specifica normativa che regola queste attività della PA;
 - analizzate e verificate, prima della trasmissione, da parte di tutti i soggetti aziendali a ciò preposti;
 - autorizzate e sottoscritte da parte dei soggetti aziendali a ciò esplicitamente delegati;
 - complete, veritiere e corrette;
 - ricostruibili attraverso la tracciabilità dei rispettivi dati;
 - archiviate secondo il piano di archiviazione.
- non omettere le informazioni necessarie alla P.A.;
- assicurare che gli adempimenti richiesti dagli Enti, anche quando conseguenti ad accertamenti o visite ispettive, siano tempestivamente e correttamente rispettati;
- informare prontamente il proprio Responsabile di Funzione allorché questi adempimenti possano subire ritardi nell'esecuzione o variazioni rispetto a quanto previsto dalla normativa o richiesto dall'Ente Pubblico;
- in caso di ispezioni, verifiche o controlli, la Società identifica, in funzione della natura dell'accertamento e nel rispetto delle deleghe in essere, il referente interno per l'ispezione;

- il referente e gli altri Responsabili di Funzione (eventualmente coinvolti nell'ispezione) devono attenersi alle seguenti condotte:
 - tenere un atteggiamento improntato ai principi di trasparenza, correttezza, professionalità, pronta e leale collaborazione nel corso dell'intera ispezione;
 - assicurare che ogni informazione fornita agli ispettori in forma verbale o scritta sia veritiera, precisa e non derivi da induzioni, interpretazioni o valutazioni personali;
 - non ricercare e/o instaurare relazioni di favore, idonee potenzialmente a condizionare, direttamente o indirettamente, l'esito dell'ispezione;
 - non elargire, né promettere doni, omaggi o qualsivoglia altra utilità, anche se di modico valore e compresa nella soglia prevista nel Codice di Comportamento dei dipendenti pubblici;
 - non tenere una condotta ingannevole che possa indurre gli ispettori in errore;
 - non omettere informazioni al fine di orientare un esito favorevole dell'ispezione verso la Società.

I Destinatari dei presenti protocolli sono obbligati a:

- in caso di tentata concussione/induzione indebita a dare o promettere denaro o altra utilità da parte di un pubblico funzionario, ovvero nel caso di contatto/minaccia da parte di terzi finalizzato ad impedire/condizionare una testimonianza davanti all'Autorità Giudiziaria:
 - i. non dare seguito alla richiesta;
 - ii. fornire tempestivamente informativa al proprio Responsabile di Funzione (in caso di dipendente LOGIC) o al referente interno (in caso di soggetti terzi) e ad informare subito l'Organismo di Vigilanza;
- in caso di contrasti con gli appartenenti alla Pubblica Amministrazione o con l'Autorità Giudiziaria, il Destinatario deve subito informare il proprio Responsabile (in caso di dipendente LOGIC) o il referente interno (in caso di soggetto terzo) e l'Organismo di Vigilanza;
- in caso sorgesse un dubbio sul rispetto dei principi comportamentali nel corso delle attività operative, il Destinatario deve subito informare il proprio Responsabile di Funzione (in caso di dipendente LOGIC) o il referente interno (in caso di soggetto terzo) e l'Organismo di Vigilanza.

L'utilizzo delle liberalità, donazioni o sponsorizzazioni finalizzate all'ottenimento di favori e concessioni da parte del soggetto/Ente beneficiario è vietato da LOGIC.

Nell'eventuale caso di donazioni/elargizioni liberali ad Enti ovvero sponsorizzazione degli stessi, i Destinatari sono tenuti a porre in essere i controlli per verificare il rispetto dei seguenti principi:

- le donazioni e sponsorizzazioni non possono essere effettuate nei confronti di persone fisiche né in denaro;
- il potere decisionale per tali iniziative spetta esclusivamente agli Organi di vertice;
- la Società si impegna a verificare i beneficiari, assicurando che le eventuali

iniziative vengano realizzate solo nei confronti di Enti che, oltre alla propria buona reputazione, siano credibili e abbiano sempre indirizzato la propria gestione a criteri di eticità e trasparenza;

- il processo decisionale adottato per pervenire alla scelta dell'iniziativa deve essere prontamente verificabile a posteriori e i Destinatari, che hanno preso parte al processo, devono essere ben identificati;
- in caso di sponsorizzazioni il negozio giuridico, oltre ad essere reciprocamente congruo, deve essere formalizzato con un contratto.

Nella selezione, assunzione e gestione del Personale, la Società assicura che:

- l'assunzione dei dipendenti avviene mediante un iter formalizzato nel rispetto della normativa di settore;
- la valutazione degli aspiranti è sempre documentata;
- in occasione della selezione devono essere valutate le eventuali situazioni di conflitto di interesse del candidato in relazione alla ruolo aziendale che sarà ricoperto.

Nella selezione dei consulenti, intermediari e fornitori, la Società assicura il rispetto dei presenti principi che trovano ulteriori regole nelle procedure:

- gli acquisti devono essere effettuati nel totale rispetto di tutte le disposizioni previste dalle procedure, dal Codice Etico e dal presente Modello;
- le offerte presentate dai fornitori sono valutate sulla base di criteri oggettivi sempre dimostrabili, trasparenti ed evidenziabili a posteriori;

I contratti conclusi con le parti devono:

- essere scritti, in tutte loro condizioni e termini;
- contenere le clausole "231" (se si tratta di soggetto straniero, o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a quelle fattispecie che, per l'ordinamento nazionale, possono corrispondere alla corruzione e alla truffa ai danni di Enti pubblici);
- evidenziare la dichiarazione delle parti di essere a conoscenza della normativa di cui al Decreto 231 (in caso di soggetto straniero, o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a quei comportamenti corrispondenti alla corruzione e alla truffa ai danni di Enti pubblici) e di impegnarsi alla conformità normativa;
- avere la clausola che disciplini, ex ante, le conseguenze delle violazioni del Decreto 231 (se si tratta di soggetto straniero, o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a quei comportamenti corrispondenti alla corruzione e alla truffa ai danni di Enti pubblici) (come le clausole risolutive espresse e le penali).

2 Controlli

2.1 *Attribuzione delle responsabilità*

Le responsabilità sono attribuite con formali procure/deleghe che individuano ruoli, compiti, responsabilità per:

- rappresentare LOGIC in tutti i rapporti con la P.A. ed in particolare, per la richiesta di licenze e delle autorizzazioni, in occasione di eventuali verifiche ispettive per il controllo dei requisiti richiesti dalle norme nazionali, estere e stabilite dal cliente contrattualmente, nei casi di accertamenti, ispezioni, comunicazioni, informazioni per il rispetto delle norme in materia ambientale, la gestione dei rifiuti nonché delle normative in materia di sicurezza, salute sui luoghi di lavoro e la prevenzione incendi;
- la richiesta e il rilascio di atti autorizzativi e le verifiche su autocertificazioni e certificazioni sostitutive di atti notori;
- la gestione dei rapporti con le Autorità di pubblica vigilanza, come il Garante per la protezione dei dati personali, l'A.N.A.C., l'Autorità Garante della Concorrenza e del Mercato e l'Autorità Giudiziaria come il Tribunale Amministrativo Regionale, il Consiglio di Stato, i Tribunali, le Corti d'Appello in riferimento ai contenziosi giudiziari;
- la proposta, la gestione e la determinazione di accordi transattivi con fornitori e clienti;
- la gestione dei rapporti con i soggetti pubblici per l'acquisizione e/o gestione di contributi/sovvenzioni/finanziamenti;
- rappresentare la Società nei rapporti con gli enti previdenziali e assistenziali, anche nei casi di contenziosi giuslavoristici;
- la gestione dei dati retributivi e dei trattamenti previdenziali, utilizzati per la predisposizione e l'invio della documentazione agli enti previdenziali e assistenziali;
- l'organizzazione e la partecipazione alle gare pubbliche, sulla base di quanto previsto dalla normativa vigente in materia;
- la pianificazione finanziaria, riconciliazione e registrazione dei pagamenti, esecuzione e registrazione delle uscite, apertura e chiusura dei conti correnti e controllo delle relative movimentazioni;
- l'approvazione, gestione e rimborso delle note spese;
- la gestione e l'organizzazione di eventuali sponsorizzazioni;
- la selezione, assunzione, formazione e incentivazione del Personale.

2.2 *Ulteriori controlli specifici*

- In relazione alla gestione delle attività di rappresentanza istituzionale e per gli scopi

relativi alla missione aziendale con la P.A., l'obbligo di formalizzazione degli incontri di particolare rilevanza. A tal fine, è istituito un flusso informativo strutturato e periodico sulle attività con la P.A. verso l'Organismo di Vigilanza attraverso la "**scheda di evidenza**" riportata in calce alla presente Sezione.

- Le informazioni e i documenti trasmessi alle P.A. in occasione di accertamenti o di ispezioni o anche su specifiche richieste, con riferimento al rispetto delle condizioni igienico-sanitarie, nonché in materia di emissioni in atmosfera, la gestione dei rifiuti, sicurezza e salute sul lavoro, prevenzione incendi, ad ogni adempimento di legge ai quali soggiace LOGIC, siano sempre adeguatamente verificate e validate dai Responsabili della Funzione competente al fine di garantire la correttezza e la completezza di quanto riportato.
- Controlli sulle richieste relative a licenze, autorizzazioni, concessioni connesse alla progettazione, produzione, riparazioni e manutenzioni, nonché sulla documentazione allegata alle medesime richieste al fine di garantire la completezza, l'accuratezza e la veridicità dei dati comunicati alla P.A.
- Verifiche periodiche da parte del Titolare e del Responsabile del trattamento dei dati personali o di loro delegato (normativa Privacy) sulla puntuale osservanza delle disposizioni del Regolamento UE 679 del 2016 e della normativa nazionale.
- Gestione del trattamento dei dati personali ex sensibili (ora denominati particolari) negli archivi cartacei ed elettronici, limitata alle sole persone autorizzate. Controlli di accuratezza e completezza della documentazione/dati trasmessi all'Autorità di vigilanza.
- Valutazione delle opportunità di richieste di finanziamento.
- Controlli sull'elaborazione e la trasmissione della documentazione relativa ai trattamenti previdenziali, contributivi e fiscali, al fine di garantire la completezza, l'accuratezza e la veridicità dei dati comunicati agli uffici della P.A.
- Gestione delle controversie prevedendo:
 - un sistema di registrazione degli atti giudiziari ricevuti;
 - regole di accreditamento e selezione dei legali esterni;
 - formalizzazione dei criteri di selezione dei professionisti esterni (ad esempio, capacità tecnica, esperienza, requisiti soggettivi di professionalità e onorabilità, referenze qualificanti, tariffe);
 - verifica della mancanza di cause di incompatibilità del professionista esterno; valutazione di congruità della parcella con riferimento alle prestazioni ricevute e approvazione del pagamento anche da parte della Funzione aziendale che ha fruito della consulenza;
 - specifiche linee di reporting periodico agli Organi di vertice e all'OdV sullo stato delle vertenze, sulle possibilità e sui termini di definizione stragiudiziale o di conciliazione giudiziale .
- Monitoraggio degli adempimenti contabili e fiscali, anche ai fini dell'invio all'amministrazione finanziaria e agli organismi di controllo per mezzo di un sistema di verifiche per il riscontro del calcolo delle imposte.

- Approvazione delle registrazioni di contabilità generale da parte del Responsabile della competente Funzione.
- Specifici controlli in relazione alla gestione della tesoreria, con particolare riferimento:
 - agli strumenti di pianificazione e controllo;
 - al monitoraggio dei movimenti finanziari;
 - all'apertura e utilizzo dei conti correnti bancari e postali della Società;
 - alla verifica periodica e l'aggiornamento degli specimen di firma, mantenuti presso le banche in cui opera l'azienda e delle persone delegate a rilasciare autorizzazioni e ad effettuare i prelievi ed i versamenti;
 - all'esecuzione periodica delle riconciliazioni bancarie.
- Formalizzazione dei contatti avuti con la P.A. in sede di verifica degli adempimenti di legge in materia di ambiente, salute e sicurezza sul lavoro.
- Attività periodiche di verifica sul sistema di controllo in conformità a quanto previsto dalla normativa vigente e dalle certificazioni ISO in materia di ambiente.
- Verifica delle forniture con validazione da parte della Funzione che le ha utilizzate prima del pagamento da parte della Funzione Amministrazione.
- Regole valide per tutte le Funzioni aziendali concernenti l'approvazione, gestione e rendicontazione delle trasferte e delle note spese ed in particolare:
 - definizione delle spese rimborsabili (tipologia e limiti);
 - approvazione della trasferta e della nota spese del dipendente da parte del Responsabile di funzione previo controllo di merito delle spese;
 - le spese dei Responsabili sono approvate dall'Amministratore Delegato;
 - controllo di completezza e accuratezza dei giustificativi della trasferta.
- controllo relativo ad eventuali sponsorizzazioni che prevede la:
 - definizione e approvazione di un fondo sponsorizzazioni;
 - definizione preventiva delle tipologie di eventi ed Enti sponsorizzabili;
 - formalizzazione della sponsorizzazione se approvata.
- Procedura per la selezione e assunzione del Personale che prevede la:
 - definizione e approvazione del budget per il relativo fabbisogno;
 - adozione di criteri oggettivi e trasparenti per la selezione dei candidati;
 - tracciabilità della trasmissione e della archiviazione dei curricula, della valutazione dei candidati così da garantire le evidenze delle motivazioni che hanno indotto alla scelta o alla esclusione del candidato;
 - adeguata archiviazione e conservazione della documentazione rilevante per il processo di selezione e assunzione.
- Gestione e amministrazione del personale con controlli riferiti in particolare alla:

- gestione delle anagrafiche dipendenti, dell'elaborazione delle buste paga e del pagamento degli stipendi;
- coerenza tra ore retribuite ed ore di lavoro effettuate;
- variazione dei dati retributivi per garantire che le modifiche apportate all'anagrafica del personale (inserimento di nuovo personale, cancellazioni, modifiche delle retribuzioni) sono state debitamente autorizzate;
- riconciliazione periodica tra dati del personale e contabilità generale.
- Formazione, sviluppo e incentivazione del Personale con controlli al/alla:
 - predisposizione del budget e del piano annuale della formazione del Personale;
 - approvazioni e autorizzazioni dei moduli di formazione e di selezione dei formatori;
 - determinazione degli obiettivi dell'attività formativa basata su criteri di oggettività, specificità e misurabilità;
 - monitoraggio degli obiettivi e definizione di un sistema formalizzato di valutazione del personale, basato sull'uso di criteri predefiniti allo scopo di comprendere la bontà delle attività svolte e le azioni da intraprendere per il futuro;
 - erogazione degli incentivi basata sul collegamento diretto con gli obiettivi raggiunti.

2.3 Tracciabilità delle transazioni

In riferimento ai reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia, al fine di garantire un idoneo supporto documentale, attraverso cui si possa procedere in ogni momento ai controlli per verificare le motivazioni dell'operazione e di individuare chi ha autorizzato, effettuato, registrato è prevista l'archiviazione:

- dei verbali/note interne sugli incontri significativi con esponenti della P.A. e della documentazione relativa agli incontri effettuati con esponenti della Pubblica Amministrazione annotati nelle già citate schede di evidenza;
- delle comunicazioni inviate alle/ricevute dalla P.A. competenti in materia di accertamenti, ispezioni, specifiche richieste documentali, in relazione alle normative per la sicurezza e la salute sul lavoro, alla prevenzione incendi, attraverso un sistema che ne agevola l'identificazione/catalogazione;
- delle comunicazioni inviate alle/ricevute dalla P.A., per la richiesta di licenze, autorizzazioni, concessioni, finanziamenti, contributi, agevolazioni, attraverso un sistema che ne consente l'identificazione/catalogazione;
- della documentazione relativa ai trattamenti previdenziali, assicurativi e fiscali del personale;
- della documentazione contabile e fiscale, eventualmente oggetto di verifica da parte della Amministrazione Finanziaria, compresa quella con gli esiti delle verifiche svolte;

- della documentazione concernente gli adempimenti in materia di ambiente, salute e sicurezza sui luoghi di lavoro;
- della documentazione attestante la consegna delle forniture e l'esecuzione di lavori e servizi, con evidenza dei controlli svolti al fine di verificarne la conformità, mediante l'utilizzo di appositi sistemi gestionali con la conservazione della documentazione giustificativa a supporto;
- dei dati e della documentazione delle registrazioni contabili nel sistema gestionale aziendale;
- della documentazione e dei dati relativi alle operazioni di incasso e pagamento, mediante l'utilizzo di sistemi gestionali in grado di tracciare i soggetti che effettuano le diverse operazioni con la conservazione della documentazione giustificativa a supporto;
- della documentazione relativa all'apertura/chiusura dei conti corrente;
- della documentazione a supporto delle trasferte effettuate e delle relative note spese;
- della documentazione relativa alle eventuali sponsorizzazioni, con particolare riferimento al contratto di sponsorizzazione e la documentazione relativa all'esecuzione del contratto;
- della documentazione relativa alla selezione e assunzione di Personale, attraverso un sistema che consente l'identificazione/catalogazione dei candidati tenendo conto del rispetto del Regolamento UE 679 del 2016 sulla protezione e sul trattamento dei dati personali e della relativa normativa nazionale di armonizzazione;
- dei dati e della documentazione relativa all'amministrazione e gestione del Personale, mediante l'utilizzo di sistemi gestionali e la conservazione della documentazione giustificativa a supporto;
- dei dati e della documentazione relativa alla gestione della formazione del Personale, all'assegnazione degli obiettivi e al monitoraggio del grado di raggiungimento degli stessi.

2.4 Segregazione dei compiti

In riferimento ai reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia, per garantire il rispetto del principio di separazione delle funzioni, i presidi prevedono la segregazione delle responsabilità:

- tra i soggetti deputati al reperimento ed ottenimento delle informazioni richieste dalle P.A. ed i soggetti deputati a validarle e a sottoscriverle in base ai poteri di firma conferiti;
- tra i soggetti che valutano le possibili richieste di finanziamento/contributo/garanzia/agevolazione da inoltrare alla P.A. rispetto a coloro che autorizzano il progetto da presentare e validano la documentazione/modulistica a supporto della richiesta e a coloro che verificano la pertinenza, e la corretta rendicontazione, dell'utilizzo delle risorse pubbliche acquisite;

- tra i soggetti incaricati della predisposizione delle comunicazioni alla P.A., contenenti informazioni inerenti ai rapporti di lavoro, rispetto ai soggetti deputati al controllo di tali comunicazioni e l'invio agli enti competenti;
- tra i soggetti che gestiscono operativamente il contenzioso in fase giudiziale e arbitrale, rispetto a coloro che autorizzano le azioni da adottare e coloro che approvano le scelte dei professionisti esterni;
- tra i soggetti che richiedono rimborsi spese rispetto a coloro che verificano la congruità ed ammissibilità delle spese sostenute e a chi ne autorizza il pagamento;
- tra i soggetti incaricati dell'esecuzione delle registrazioni in contabilità generale e predisposizione del bilancio, rispetto ai soggetti deputati al controllo ed alla validazione delle registrazioni stesse. La redazione, l'approvazione del progetto di bilancio e poi del bilancio sono effettuate in base al codice civile, sottoposte al controllo del Collegio Sindacale e a quello della Società di revisione legale dei conti ognuno di questi Organi secondo la rispettiva propria competenza;
- tra i soggetti che propongono eventuali sponsorizzazioni, i soggetti che gestiscono i rapporti con gli enti che beneficiano della sponsorizzazione e i soggetti che sottoscrivono i contratti di sponsorizzazione;
- tra i Responsabili delle Funzioni aziendali che richiedono l'assunzione del Personale rispetto ai soggetti incaricati della valutazione/selezione del personale, della definizione della proposta di assunzione e a coloro deputati alla firma della lettera di assunzione;
- tra i soggetti incaricati della predisposizione ed erogazione dei piani formativi, rispetto a coloro deputati ad approvare i piani medesimi, nonché tra i soggetti incaricati di predisporre la proposta degli obiettivi aziendali, rispetto a coloro incaricati dell'approvazione degli stessi e a coloro deputati al monitoraggio del raggiungimento degli obiettivi medesimi.

2.5 Sistema di procure/deleghe coerente con le responsabilità, ruoli e compiti

In riferimento ai reati contro la Pubblica Amministrazione e l'Amministrazione della Giustizia, al fine di garantire che i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative e gestionali assegnate e chiaramente definiti e conosciuti all'interno di LOGIC, è previsto:

- un sistema di procure/deleghe che assegna i poteri ad impegnare la società verso l'esterno distinguendo se con le parti private e pubbliche, coerentemente alle mansioni ricoperte e alle attività effettivamente svolte;
- un sistema di procure/deleghe che assegna i poteri di sottoscrivere i contratti di assunzione del Personale in funzione dei ruoli, compiti e responsabilità ricoperti;
- un sistema che garantisca che l'eventuale transazione e/o conciliazione venga condotta dal soggetto titolare di un'apposita procura e che possiede, quindi, il potere di conciliare o transigere la controversia in nome e per conto della Società.

3 Flussi informativi verso l'Organismo di vigilanza.

All'Organismo di Vigilanza saranno inviate, a cura di ogni Responsabile di Funzione, le schede di evidenza, delle quali qui di seguito viene riportato lo schema standard, compilate in ogni loro parte con cadenza periodica trimestrale. Resta inteso che, in caso di ogni necessità e/o urgenza per azioni e/o eventi relativi ai rapporti con la Pubblica Amministrazione, si informerà immediatamente l'OdV.

SCHEMA DI EVIDENZA

Rapporti con la Pubblica Amministrazione

Periodo:

Destinatario:

All'Organismo di Vigilanza di LOGIC.

Premesso che:

- a. LOGIC ha predisposto il proprio Modello di Organizzazione, Gestione e Controllo ai sensi del Decreto 231;
- b. la Sezione "A" della parte speciale del Modello 231 (reati in danno della Pubblica Amministrazione), al punto 2.1 prevede, da parte di ogni Destinatario, la predisposizione di questa scheda di evidenza nella quale trascrivere, sinteticamente, l'attività svolta in occasione di incontri con rappresentanti della Pubblica Amministrazione.

Pertanto, si dichiara che nel periodo in esame sono stati incontrati rappresentanti della Pubblica Amministrazione, di seguito indicati, per le seguenti principali iniziative/attività:

Pubblica Amministrazione nazionale o estera	Principali iniziative / attività

L'eventuale documentazione relativa agli incontri è disponibile presso la competente Funzione della Società.

Si dichiara di essere a conoscenza di quanto contenuto nel Codice Etico e nel Modello di Organizzazione, Gestione e Controllo e non si segnala, con riferimento ai propri rapporti con le Pubbliche Amministrazioni di cui sopra - ed a quelli intrattenuti con i medesimi dai propri collaboratori all'uopo delegati e le cui attività sono state debitamente controllate e monitorate - alcuna infrazione al Modello stesso e, in particolare, alcun fatto o comportamento che possa violare le disposizioni e rappresentare un elemento dei reati presupposto evidenziati nel Decreto 231 del cui contenuto si dichiara di essere a conoscenza e di averne edotto i propri dipendenti (nel caso dei Responsabili di funzione).

Data: .../.../...

(Firma)

.....

SEZIONE "B"
Art. 25 ter del Decreto 231
Reati Societari

L'art. 25-ter del Decreto prevede i reati societari. Di questi alcuni sono stati ritenuti sensibili per la Società, ovvero:

- **False comunicazioni sociali, anche di lieve entità (artt. 2621 e 2621-bis del c.c.):** il reato punisce, fuori dai casi previsti dall'art. 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali dirette ai soci o al pubblico, previste dalla legge, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero ovvero omettano fatti materiali rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale la stessa appartiene, in modo concretamente idoneo ad indurre altri in errore. Secondo l'attuale orientamento della giurisprudenza delle Sezioni Unite della Cassazione sono punibili anche i falsi derivanti da valutazioni estimative.
- **Impedito controllo (art 2625 c.c.):** è il reato commesso da parte degli amministratori che, occultando documenti o con altri idonei artifici, impediscano o comunque ostacolino lo svolgimento delle attività di controllo legalmente attribuite ai soci, ad altri organi sociali.
- **Operazioni in pregiudizio dei creditori (art. 2629 c.c.):** è il reato commesso da parte degli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuino riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando danno ai creditori.
- **Formazione fittizia del capitale (art. 2632 c.c.):** il reato punisce gli amministratori e i soci conferenti che, anche in parte, formino od aumentino fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione.
 - **Corruzione tra privati (art. 2635 , comma 3 c.c.):** il reato, ai fini della responsabilità dell'ente, è costituito dal comportamento di chi tra gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, di società o enti privati che, anche per interposta persona, sollecitano o ricevono, per sé o per altri, denaro o altra utilità non dovuti, o ne accettano la promessa, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.
 - **Istigazione alla corruzione tra privati (art. 2635 bis c.c.):** il reato in esame punisce, chiunque offra o prometta denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà.
 - **Illecita influenza sull'assemblea (art. 2636 c.c.):** viene punito chiunque, con atti simulati o fraudolenti, determini la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto.
 - **Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.):** questo reato punisce gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di

società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultino con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima.

In considerazione dell'introduzione nel novero di tali reati dell'art. 2635 comma 3 c.c. relativo alla c.d. "corruzione tra privati"⁴ e l'introduzione del reato di "istigazione alla corruzione tra privati"⁵ tra i reati societari e degli aspetti di peculiarità di tale delitto nell'ambito della categoria dei reati societari presupposto ex Decreto 231, la presente sezione è distinta in due paragrafi, il primo è riservato ai reati societari e il secondo al reato di corruzione tra privati.

1 Attività sensibili alla commissione dei reati societari ad esclusione della corruzione tra privati

In considerazione della missione aziendale di LOGIC e della sua organizzazione, le principali attività sensibili e i processi strumentali a rischio di commissione dei reati in oggetto sono:

- gestione degli adempimenti ed operazioni in materia societaria;
- predisposizione del bilancio di esercizio;
- gestione rapporti con l'Amministrazione Finanziaria e degli interventi ispettivi dell'Amministrazione Tributaria e degli Organi di Polizia Tributaria in occasione di controlli e accertamenti.

1.1 Principi di comportamento

I seguenti principi di comportamento si applicano ai Destinatari del presente Modello che, a

⁴ Il D.Lgs. n. 38 del 15 marzo 2017 ha modificato in modo sostanziale il reato di corruzione tra privati (art. 2635 c.c.), in quanto è stato ampliato il novero dei soggetti che possono commettere il reato a "chi nell'ambito organizzativo della società o dell'ente privato esercita funzioni direttive diverse dagli amministratori, dai direttori generali, dai dirigenti preposti alla redazione dei documenti contabili societari, dai sindaci e dai liquidatori". È stato inoltre modificato il presupposto di commissione del reato, che diventa profilabile anche **per interposta persona e senza che necessariamente sia cagionato nocumento alla società**. Infine, è stata inasprita la pena per chi commette il reato in quanto la sanzione pecuniaria, rispetto ad un range compreso tra duecento e quattrocento quote, è passata ad un minimo di quattrocento e ad un massimo seicento quote ed è stata introdotta la sanzione interdittiva.

⁵ Introduzione del reato di "Istigazione alla corruzione tra privati" (art 2635 bis) nei reati societari punibili ai sensi del D.Lgs. 231: «Chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 2635, ridotta di un terzo». Costituiscono esempi del suddetto reato favorire un collaboratore in progressioni economiche e di carriera dietro compenso economico o l'assunzione di persone segnalate da fornitori o da terzi.

qualunque titolo, siano coinvolti nelle attività sensibili rispetto ai reati societari . A tali soggetti è richiesto di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto della legge, del Codice Etico, del presente Modello 231 e delle procedure aziendali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire ai soci ed ai terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della Società;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurare il regolare funzionamento della Società e degli Organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge e la libera e corretta formazione della volontà assembleare;
- effettuare con tempestività e correttezza tutte le comunicazioni previste dalla legge nei confronti delle autorità di vigilanza non ponendo loro alcun ostacolo;
- non realizzare operazioni di acquisto e cessione di partecipazioni di aziende o loro rami, operazioni di fusione, scissione, scorporo che possano ledere l'integrità del capitale sociale.

In questo contesto è vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, individualmente o collettivamente, integrino, direttamente o indirettamente, il reato compresi tra quelli sopra evidenziati.

Per i Destinatari sopra indicati è inoltre previsto il divieto di:

- porre in essere operazioni simulate o diffondere notizie false sulla Società;
- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilancio, relazioni e prospetti o altre comunicazioni sociali contenenti 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;
- restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori provocando loro un danno;
- procedere alla formazione o all'aumento fittizio del capitale sociale;
- porre in essere comportamenti che impediscano materialmente o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione da parte del Collegio Sindacale e/o della Società di revisione mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti;

- determinare o influenzare l'assunzione delle deliberazioni dell'assemblea, ponendo in essere atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- omettere di effettuare, con la dovuta completezza, accuratezza e tempestività, tutte le segnalazioni previste dalle leggi e dalla normativa applicabile nei confronti delle Autorità di vigilanza e delle Autorità pubbliche con funzioni di controllo cui è soggetta l'attività aziendale e la trasmissione dei dati e documenti previsti dalla normativa e/o specificamente richiesti dalle predette Autorità;
- esporre nelle predette comunicazioni e trasmissioni fatti non rispondenti al vero, oppure occultare fatti rilevanti relativi alle condizioni economiche, patrimoniali o finanziarie della Società;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle autorità pubbliche o degli Enti incaricati del controllo (espressa opposizione, rifiuti pretestuosi o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

In caso di dubbi sulla corretta attuazione dei principi comportamentali nel corso dello svolgimento delle rispettive attività è obbligo per il Destinatario di interpellare il proprio Responsabile di Funzione (in caso di dipendente LOGIC) o referente interno (in caso di soggetti terzi) informandone l'Organismo di Vigilanza.

Nei confronti di terze parti contraenti (come i collaboratori, consulenti, intermediari, partner, fornitori, clienti) selezionate anche in funzione di specifici criteri (come l'importo e la significatività della fornitura) e coinvolte nello svolgimento di attività a rischio rispetto ai reati societari che operano per conto o nell'interesse di LOGIC i relativi contratti devono:

- essere scritti;
- contenere le clausole "231".

1.2 Controlli

In relazione ai rischi connessi alla potenziale commissione di reati oggetto del presente paragrafo, i suddetti principi di comportamento prevedono i seguenti controlli:

- definizione di regole etiche che disciplinino il corretto comportamento di tutti i dipendenti coinvolti nelle registrazioni contabili e nelle attività di formazione del bilancio e della documentazione contenente informazioni economico- finanziarie;
- svolgimento di attività di formazione a favore di tutti i Responsabili di Funzione affinché conoscano le principali nozioni sul bilancio (norme di legge, sanzioni);
- esistenza di disposizioni organizzative e procedurali rivolte alle Funzioni aziendali con le quali si stabiliscono quali dati e notizie devono essere forniti alla Funzione Amministrazione, Finanza e Controllo e quali controlli devono essere svolti dall'Amministrazione;
- previsione dell'obbligo per il Responsabile di Funzione preposto alla redazione del Bilancio e delle altre comunicazioni sociali di sottoscrivere una dichiarazione di veridicità e completezza delle informazioni trasmesse da inviare all'Amministratore

Delegato assieme al progetto di bilancio. In questa dichiarazione è riportato ciò che obiettivamente e concretamente il Responsabile può formalmente dimostrare sulla base dei dati in suo possesso;

- ai fini della redazione del bilancio d'esercizio, la Funzione Amministrazione, Finanza e Controllo predispose ed inoltra alle altre Funzioni le istruzioni che riportano la tipologia di informazioni che ognuna di esse deve fornire ai fini della chiusura del bilancio definendone tempi e modalità. Tali istruzioni, in formato elettronico, servono per identificare tutte le informazioni e notizie necessarie ad una corretta gestione del processo di chiusura contabile. La Funzione Amministrazione, ricevute le informazioni, provvederà all'analisi, al consolidamento e alla validazione delle stesse;
- le informazioni trasmesse dalle singole Funzioni alla Funzione Amministrazione tramite un documento informatico sono previamente validate dai Responsabili delle Funzioni medesime. Le istruzioni prevedono che la predisposizione dei format, nei quali le Funzioni inseriscono le informazioni richieste, richieda la responsabilizzazione dell'intera Funzione;
- tempestiva messa a disposizione di tutti i componenti del Consiglio di Amministrazione, inviandola oltre che all'Amministratore Delegato anche al Presidente del CdA, della bozza del progetto di bilancio prima della sua riunione collegiale per l'approvazione dello stesso, prevedendo la documentata certificazione dell'avvenuta consegna della bozza in questione.

È prevista la formalizzazione delle modalità operative per la gestione delle attività di rilevazione contabile, chiusura annuale ed infra-annuale e conseguente predisposizione del bilancio d'esercizio, prevedendo in particolare:

- che siano definiti con chiarezza i principi contabili da adottare per la definizione delle poste di bilancio di esercizio e le modalità operative per la loro contabilizzazione;
- modalità di estrazione dei dati per le chiusure contabili;
- gestione dei controlli;
- formazione e diffusione di istruzioni, rivolte alle strutture aziendali coinvolte, che indichino dati e notizie che è necessario fornire alla Funzione Amministrazione che è la responsabile della redazione del bilancio d'esercizio;
- la verifica delle poste valutative;
- predisposizione, verifica e approvazione della bozza di bilancio;
- regole relative alla tenuta e conservazione del bilancio, dall'approvazione da parte dell'Organo di vertice Amministrativo al deposito e fino alla relativa archiviazione. Sono previsti flussi informativi da/verso l'Autorità di vertice e la Funzione responsabile della formazione del bilancio d'esercizio così da garantire la completezza/correttezza dei fatti aziendali riflessi in bilancio. È prevista una riunione tra la Società di Revisione, il Collegio Sindacale e l'Organismo di Vigilanza prima della seduta dell'Organo Amministrativo indetta per l'approvazione del progetto di bilancio, che abbia ad oggetto il fascicolo di bilancio e la valutazione di eventuali criticità emerse nello svolgimento delle attività di

revisione legale dei conti.

È inoltre:

- prevista la sottoscrizione da parte dell'Amministratore Delegato di un documento che attesti l'avvenuta ricezione della bozza del progetto di bilancio.

1.2.1 Attribuzione delle responsabilità

È prevista la definizione di ruoli, responsabilità e disposizioni aziendali per le funzioni coinvolte nelle attività di predisposizione del bilancio d'esercizio e della documentazione contabile. Ciò serve a regolare le modalità e i controlli per lo svolgimento delle attività sensibili e le modalità di archiviazione della documentazione.

1.2.2 Tracciabilità delle transazioni

In riferimento ai reati societari, al fine di garantire un adeguato supporto documentale per ogni operazione, attraverso cui si possa procedere in ogni momento all'esecuzione di controlli che consentano di ricostruire, a posteriori, le motivazioni dell'operazione e di individuare chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa, è prevista la predisposizione, la registrazione e l'archiviazione di dati/informazioni/stime nonché di tutta la documentazione prodotta ai fini della redazione del bilancio per consentire, sempre, la ricostruzione delle fasi del processo.

1.2.3 Segregazione dei compiti

Per garantire l'applicazione del principio di separazione dei ruoli, è previsto che le attività rilevanti siano organizzate al fine di prevedere la segregazione delle responsabilità tra chi autorizza, chi esegue e chi controlla le operazioni svolte nell'ambito dei processi amministrativi contabili e quelli qui indicati:

- estrazione/rilevazione dei dati contabili e di chiusura contabile;
- predisposizione del bilancio;
- approvazione del progetto di bilancio;
- approvazione del bilancio.

1.2.4 Sistema di procure/deleghe coerente con le responsabilità, ruoli e compiti

Al fine di garantire che i poteri autorizzativi e di firma siano coerenti con le rispettive responsabilità organizzative e gestionali e chiaramente definiti e conosciuti all'interno dell'organizzazione, sono previste procure e deleghe che attribuiscono i poteri per impegnare la Società verso l'esterno, con i limiti e la natura di essi.

2 Attività sensibili alla commissione del delitto di corruzione tra privati

Tenuto conto delle attività aziendali di LOGIC e della sua organizzazione le attività sensibili e i processi a rischio di commissione del reato in oggetto possono essere i seguenti:

- acquisizione e progressione del Personale;
- affidamento di lavori, servizi e forniture;

- affidamento di incarichi per consulenze;
- gestione rimborsi spese e spese di rappresentanza;
- gestione dei procedimenti e dei contenziosi giudiziali e stragiudiziali (civili, penali, amministrativi e tributari) e nomina dei legali;
- omaggi, donazioni, sponsorizzazioni, attività promozionali e erogazioni liberali;
- gestione dei flussi finanziari e delle attività di tesoreria;

2.1 Principi di comportamento

I seguenti principi di comportamento di carattere generale si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività sensibili rispetto al reato in esame.

È vietato porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, la fattispecie di reato di "corruzione tra privati" definita dall'art. 2635 c.c. e richiamata dall'art. 25-ter del Decreto 231.

In particolare, nella gestione dei rapporti con i referenti (apicali o soggetti sottoposti alla direzione e vigilanza degli stessi) di società private è vietato:

- promettere o effettuare dazioni indebite di denaro o riconoscimenti indebiti di altra utilità;
- distribuire omaggi e regali eccedenti le normali pratiche commerciali o di cortesia. Gli omaggi consentiti sono quelli di esiguo valore;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale o comunque non conformi alle specifiche regole aziendali;
- effettuare promesse di assunzione o assunzioni di Personale in favore di soggetti segnalati dall'interlocutore/referente privato al fine di ottenere indebiti benefici o vantaggi derivanti da comportamenti scorretti dell'interlocutore (compimento o omissione di atti in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà alla propria Società di appartenenza).

Questi divieti sono estesi anche a soggetti terzi (ad esempio agenti o distributori) che agiscono nell'interesse della Società.

È vietato:

- favorire, nei processi di acquisto, collaboratori, fornitori, consulenti, intermediari o altri soggetti terzi, in quanto indicati dagli interlocutori/referenti privati;
 - effettuare prestazioni o pagamenti di compensi in favore di collaboratori, fornitori, consulenti, partner, intermediari o altri soggetti terzi che operano per conto della Società che non trovano adeguata giustificazione nel rapporto contrattuale costituito e/o in relazione al tipo di incarico da svolgere.

È obbligo attenersi alle seguenti prescrizioni:

- in caso di conflitti di interesse ovvero di oggettive difficoltà nell'ambito dei rapporti con interlocutori di società terze, il Destinatario deve informare il proprio

Responsabile di Funzione (in caso di dipendente di LOGIC) o il referente interno (in caso di soggetto terzo) e l'Organismo di Vigilanza;

- in casi dubbi sulla corretta attuazione dei principi comportamentali di cui sopra nel corso dello svolgimento delle attività aziendali, il Destinatario deve interpellare tempestivamente il proprio Responsabile (in caso di dipendente LOGIC) o il referente interno (in caso di soggetto terzo) e informare l'Organismo di Vigilanza.

2.2 Controlli

Ogni accordo con terze parti deve essere:

- formalizzato per iscritto con dettagliate condizioni e termini del negozio giuridico;
- sottoscritto dai soggetti aventi i poteri per farlo e a ciò espressamente delegati, secondo il vigente sistema di procure e deleghe;
- sottoposto ad un processo autorizzativo interno basato sul principio di separazione delle funzioni (tra chi propone l'accordo, chi lo verifica e chi lo sottoscrive) e alla corretta verifica dei contenuti e degli impegni economici.

Rispetto ai rischi relativi a questi reati si applicano i seguenti principi.

La Società definisce, con opportune politiche aziendali, le regole e i criteri da applicare alla richiesta, autorizzazione ed erogazione del rimborso di spese sostenute dai dipendenti.

Coloro che richiedono rimborsi spese sono tenuti alla predisposizione della nota spese in modo corretto e vero.

Le spese di rappresentanza sono rimborsate solo se motivate, pertinenti e coerenti con l'attività svolta e validamente documentate.

Premesso che la Società condanna l'utilizzo improprio dello strumento delle liberalità, donazioni e sponsorizzazioni al fine di creare disponibilità finanziarie utili alla commissione di reati di corruzione, nell'eventuale caso di donazioni/elargizioni liberali a enti privati ovvero sponsorizzazione degli stessi, i Destinatari del presente Modello sono tenuti a porre in essere tutti i controlli necessari per assicurare il rispetto dei presenti principi:

- le donazioni e sponsorizzazioni non possono essere effettuate nei confronti di persone fisiche, ma solo a favore di persone giuridiche;
- il potere decisionale per tali iniziative spetta esclusivamente ai soggetti di vertice espressamente delegati;
- la Società si impegna a verificare la natura giuridica dei beneficiari, assicurando che le iniziative vengano realizzate solo nei confronti di soggetti che dimostrino credibilità e buona reputazione con una gestione etica e trasparente;
- in caso di sponsorizzazioni il rapporto deve basarsi sulla congruità tra le prestazioni corrispettive e deve essere formalizzato in un contratto.

I contratti devono:

- essere scritti;
- contenere le clausole "231".

SEZIONE "C"
Art. 24 ter del Decreto 231
Reati di criminalità organizzata

L'art. 24-ter del Decreto 231 inserisce, tra i reati presupposto, quello di:

- **Associazione per delinquere (art. 416 c.p.):** sono punite tre o più persone quando si associano allo scopo di commettere più delitti.

La legge 16 marzo 2006, n. 146, ("Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001") ha esteso, inoltre, la responsabilità amministrativa degli Enti ai reati di "criminalità organizzata transnazionale".

Viste le attività aziendali di LOGIC e della sua organizzazione, le principali attività sensibili e i processi a rischio di commissione dei suddetti reati sono i seguenti:

- gestione dei rapporti con interlocutori terzi - pubblici o privati - nello svolgimento delle proprie attività per conto e/o nell'interesse della Società;
- affidamento di lavori, servizi e forniture;
- partecipazione a gare e commesse nei Paesi esteri;
- gestione dei procedimenti e dei contenziosi giudiziali e stragiudiziali (civili, penali, amministrativi e tributari) e nomina dei legali;
- gestione adempimenti ed operazioni in materia societaria;
- acquisizione e progressione del Personale;
- amministrazione e bilancio;
- gestione relazioni istituzionali.

1 Principi di comportamento

I seguenti principi di comportamento si applicano ai Destinatari del presente Modello che, a qualunque titolo, intrattengano rapporti di tipo commerciale o comunque istituzionale con interlocutori terzi, pubblici o privati, per conto o nell'interesse di LOGIC.

A tali Destinatari è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti idonei ad integrare, direttamente o indirettamente, le fattispecie di reato previste dall'art. 24-ter del Decreto 231.

In particolare, nel rispetto dei principi etici espressi nel Codice Etico di LOGIC e delle regole del presente Modello, è fatto obbligo di:

- tenere un comportamento corretto, trasparente e collaborativo conformemente ai principi stabiliti dalle norme di legge e dalle procedure aziendali interne;
- osservare rigorosamente le norme poste dalla legge a tutela del diritto – costituzionalmente garantito - ad associarsi per scopi e fini che non siano vietati ai singoli dalla legge penale;
- assicurare il regolare funzionamento della Società e degli Organi sociali,

garantendo ed agevolando ogni forma di controllo interno sulle attività societarie, che possano essere strumentali all'attuazione di comportamenti o condotte non conformi ai suddetti principi;

- non ostacolare lo svolgimento di eventuali indagini e iniziative da parte degli Organi sociali, o più in generale da qualsiasi organo/ente ispettivo, finalizzate a rilevare e combattere condotte illecite in relazione all'ipotesi del reato associativo considerato.

Gli obblighi si intendono riferiti non solo ai rapporti instaurati con soggetti privati ma anche con appartenenti alla Pubblica Amministrazione.

Ai propri dipendenti è fatto divieto di adottare con consapevolezza, coscienza e volontà le seguenti condotte:

- promuovere, costituire, organizzare ovvero partecipare ad associazioni di tre o più soggetti con lo scopo di commettere uno o più delitti o, più in generale, tenere condotte direttamente o indirettamente vietate dalla legge penale;
- attuare – anche strumentalizzando attività riconducibili alla comune gestione societaria - condotte che si concretino in un'attiva e stabile partecipazione all'associazione illecita;
- contribuire a creare, e garantire nel tempo, una struttura organizzativa che sia comunque idonea e adeguata alla realizzazione di obiettivi delittuosi nell'interesse dell'associazione illecita;
- predisporre - o contribuire a predisporre - i mezzi attraverso i quali supportare l'attività della associazione illecita;
- promuovere o comunque proporre, la realizzazione di obiettivi delittuosi di volta in volta individuati come utili o necessari nell'ottica del conseguimento di un vantaggio per la Società.

È obbligatorio per i Destinatari di attenersi alle seguenti prescrizioni:

- nel caso in cui si venisse contattati da soggetti interessati ad instaurare un rapporto associativo con la finalità di perseguire scopi delittuosi, il soggetto interessato deve: (i) non dare seguito al contatto; (ii) fornire tempestivamente informativa al proprio Responsabile (in caso di dipendente di LOGIC) o al referente interno (in caso di soggetti terzi) e all'Organismo di Vigilanza;
- in caso di conflitti di interesse che sorgano con soggetti terzi nell'ambito dei rapporti commerciali o comunque istituzionali, il Destinatario deve fornire tempestivamente informativa al proprio Responsabile (in caso di dipendente di LOGIC) o al referente interno (in caso di soggetto terzo) e all'Organismo di Vigilanza;
- in caso di dubbi circa la corretta attuazione dei suddetti principi etici, il Destinatario deve interpellare senza ritardo il proprio Responsabile (in caso di dipendente di LOGIC) o il referente interno (in caso di soggetto terzo) e informare l'Organismo di Vigilanza.

Nei confronti di terze parti contraenti (collaboratori, consulenti, partner, intermediari, fornitori, clienti) che hanno rapporti con interlocutori terzi esterni alla Società per conto o nell'interesse della

stessa, i relativi contratti devono:

- essere scritti;
- contenere le clausole del Decreto 231.

2 Controlli

In relazione ai rischi connessi alla commissione di reati oggetto del presente paragrafo, i principi di comportamento sopra esposti prevedono i seguenti presidi.

2.1.1 *Attribuzione delle responsabilità*

È prevista la definizione dei ruoli e delle responsabilità all'interno di LOGIC per la gestione dei rapporti con interlocutori terzi, pubblici o privati.

2.1.2 *Tracciabilità delle transazioni*

Per ogni operazione relativa alla gestione dei rapporti con terzi - pubblici o privati – è previsto un adeguato supporto documentale per mezzo del quale si possono effettuare i controlli per verificare le caratteristiche e le motivazioni dell'operazione ed individuare chi ha autorizzato, effettuato, registrato e verificato la transazione stessa.

2.1.3 *Segregazione dei compiti*

È contemplata la separazione di funzioni, per cui l'autorizzazione all'effettuazione di un'operazione deve essere di persona diversa da chi esegue operativamente o chi la controlla.

2.1.4 *Sistema di procure/deleghe coerente con le responsabilità, ruoli e compiti*

I poteri autorizzativi e di firma debbono essere coerenti con le responsabilità e gestionali di ognuno, definiti e conosciuti all'interno della Società.

SEZIONE “D”

ART. 25 octies del Decreto 231

Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio

L'art. 25-octies del Decreto contempla i cosiddetti reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio:

- **Ricettazione (art. 648 c.p.):** è punito chi, fuori dei casi di concorso nel reato, al fine di procurare a sé o ad altri un profitto, acquisti, riceva od occulti denaro o cose provenienti da un qualsiasi delitto, o comunque si intrometta nel farle acquistare, ricevere od occultare.
- **Riciclaggio (art. 648-bis c.p.):** è punito chiunque, fuori dei casi di concorso nel reato, sostituisca o trasferisca denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compia in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.
- **Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.):** è punito chiunque, fuori dei casi di concorso nel reato e dei casi previsti dagli articoli 648 e 648 bis, impieghi in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.
- **Autoriciclaggio (art. 648-ter.1 c.p.):** è punito chiunque, avendo commesso o concorso a commettere un delitto non colposo, impieghi, sostituisca, trasferisca, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.

Tenuto conto delle attività commerciali svolte da LOGIC, della legge 185 del 1990 e della sua organizzazione interna, le attività sensibili possono essere considerate le seguenti:

- sugli adempimenti e sulle operazioni in materia societaria;
- in relazione ai flussi finanziari e alle attività di tesoreria;
- alla gestione degli acquisti e alla relativa scelta dei fornitori.

In merito al reato di autoriciclaggio, introdotto tra quelli presupposto del Decreto 231 nel 2015, bisogna considerare che potrebbe concretizzarsi anche in presenza di illeciti non previsti dal Decreto 231 (come i reati tributari che non sono indicati nel cd catalogo "231" i cui proventi potrebbero essere oggetto di "autoriciclaggio" quando l'autore del reato sia lo stesso per entrambi gli illeciti penali).

1 Principi di comportamento

I seguenti principi si applicano a tutti i Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività sensibili rispetto ai reati di ricettazione, riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio, con particolare riferimento a coloro che intrattengono rapporti con terze parti per conto o nell'interesse della Società in quanto destinatari di formali procure o deleghe.

Ogni flusso finanziario in entrata e in uscita della Società, sia quelli afferenti ad operazioni ordinarie (incassi e pagamenti) che a quelli riferiti ad esigenze finanziarie (come liquidità, finanziamenti a breve, medio e lungo termine, coperture di rischi) o ad operazioni straordinarie (come acquisti o cessioni di partecipazioni o rami di aziende, liquidazioni, scambi di partecipazioni, liquidazioni, investimenti o cessioni di attività, operazioni sul capitale), deve essere legittimo e

posto in essere nel rispetto delle norme, tracciato, ricostruibile ex post, motivato, autorizzato e consono alle reali esigenze aziendali definite e deliberate dall'organo di vertice o dai soggetti in possesso di specifica procura o delega.

Sono sempre formalizzati: atti o contratti, i rapporti e le operazioni di natura commerciale o finanziaria con terze parti connessi ai flussi finanziari in entrata o in uscita, come pure i rapporti e le operazioni con altre società controllate o con i soci.

Ai Destinatari è fatto tassativo divieto porre in essere, collaborare o dare causa alla realizzazione di condotte volte a impiegare, sostituire, trasferire nell'ambito delle attività d'impresa della Società e dei relativi flussi finanziari, denaro, beni o altre utilità provenienti da illeciti, di qualsiasi natura.

Pertanto, è vietato:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che integrino o possano integrare, direttamente o indirettamente, i reati di ricettazione, riciclaggio, impiego di denaro, beni altre utilità di provenienza illecita, autoriciclaggio;
- impiegare, sostituire, trasferire, in attività economiche, finanziarie, imprenditoriali, il denaro, i beni o le altre utilità provenienti dalla commissione di un reato.

A tali soggetti, in particolare a tutti coloro che, oltre all'Organo di vertice, fanno parte delle Funzioni "Amministrazione/Finanza e Controllo" e "Commerciale" è fatto obbligo di:

- osservare quanto stabilito da norme di legge (in particolare dalla legge 185 del 1990), regolamenti, dal Codice Etico, dal presente Modello 231, dalle procedure aziendali interne, nell'intero processo gestionale dei rapporti commerciali con fornitori/clienti/partner nazionali e stranieri, sia privati che pubblici;
- monitorare le notizie sui soggetti terzi con i quali la Società ha rapporti di natura finanziaria o commerciale, soprattutto allorquando è sorto il sospetto che abbiano commesso attività illecite in genere;
- non intrattenere rapporti con soggetti (fisici o giuridici) dei quali sia anche solo sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della legalità;
- effettuare un costante monitoraggio dei flussi finanziari aziendali;

In caso di dubbio, anche minimo, è fatto obbligo al soggetto interessato di interpellare subito il proprio Responsabile di Funzione (in caso di dipendente della Società) e referente interno (in caso di soggetti terzi) ed inoltrare formale, immediata informazione all'Organismo di Vigilanza, oltre che all'Amministratore Delegato, per le loro valutazioni. Infine, nei confronti di terze parti (come i collaboratori esterni, consulenti, partner, fornitori, clienti) i relativi contratti devono:

- essere scritti, in tutte le loro condizioni e termini;
- contenere le clausole "231".

2 Controlli

In relazione ai rischi connessi ai reati in questione i controlli sono qui di seguito indicati.

2.1 *Attribuzione delle responsabilità*

È prevista la definizione dei ruoli e delle responsabilità di tutte le persone deputate alla gestione dei flussi finanziari e delle attività di tesoreria.

2.2 *Controlli specifici*

Per le attività sensibili in riferimento sono previste/i:

- procedure di gestione dell'anagrafica di clienti e fornitori (ragione/denominazione sociale, indirizzo di fatturazione, indirizzo di spedizione merci, coordinate IBAN, modalità di pagamento) e di corretta gestione contabile dei rapporti contrattuali;
- verifiche costanti della corrispondenza tra registrazioni contabili di ciclo attivo e passivo e flussi di incasso / pagamenti;
- controlli specifici della provenienza dei pagamenti. Per ogni pagamento con bonifico il personale della Funzione "Amministrazione, Finanza e Controllo" che riscontra l'operazione deve immediatamente verificare la corrispondenza dell'identità del soggetto che ha disposto il bonifico con quella del soggetto committente. Nel caso vi sia l'autorizzazione ex L. 185/90 deve altresì essere verificata la corrispondenza con il soggetto nei cui confronti la fornitura è autorizzata. In caso di difformità deve essere data immediata segnalazione all'OdV e all'Amministratore delegato ed il pagamento deve essere respinto in attesa degli approfondimenti.
- modalità formalizzate e autorizzate per la modifica delle coordinate bancarie di pagamento/incasso rispetto a quelle inizialmente concordate in sede contrattuale con la controparte ovvero rispetto a quelle utilizzate in precedenti rapporti contrattuali;
- verifiche di affidabilità commerciale e professionale di fornitori, clienti, partner e intermediari (soprattutto in occasione di nuove controparti) con l'acquisizione di informazioni (come i certificati camerali) e/o, se necessario, con l'ausilio di banche dati elaborate al fine di contrastare il riciclaggio e il finanziamento del terrorismo;
- monitoraggi anche attraverso l'utilizzo dei motori di ricerca nella rete internet;
- accordi negoziali, ove la Società intendesse avere iniziative commerciali di questo tipo, nei confronti di fornitori e partner con sede o residenza in paesi considerati come non cooperativi dal GAFI ovvero residenti negli Stati a fiscalità agevolata (si veda la "black list" costantemente aggiornata dall'Agenzia delle Entrate) solo ed esclusivamente previa verifica dell'attendibilità commerciale e professionale della controparte e comunque nel rispetto delle specifiche normative;
- controlli dei flussi finanziari aziendali in entrata ed uscita; in caso di rapporti con terze parti, tali controlli devono riguardare lo Stato dove è ubicata la sede legale,

amministrativa ed operativa della società controparte (per verificare se sia in un Paese cd paradiso fiscale o Paese a rischio terrorismo), delle sedi degli istituti di credito utilizzati per le transazioni e di eventuali ricorsi a società terze o a consulenti;

- rifiuti di effettuare/ricevere pagamenti in denaro contante e titoli al portatore (assegni, vaglia postali, certificati di deposito) per importi complessivamente superiori alle soglie stabilite dal D. Lgs. 231/07 (e successive modifiche) e sempre che ciò sia autorizzato dal Responsabile della Funzione "Amministrazione, Finanze e Controllo";
- sistemi di gestione dei pagamenti interamente regolati dalle procure e dalle deleghe. Il sistema delle procure e delle deleghe deve costituire un flusso informativo verso l'OdV ogni volta che sono modificate e/o integrate;
- obblighi di tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge, del Codice Etico, del presente Modello e delle procedure in tutte le attività finalizzate alla formazione del bilancio, alla gestione della cassa ed alla tesoreria;
- flussi informativi verso l'OdV relativi alle operazioni straordinarie (come gli acquisti o le cessioni di partecipazioni o rami di aziende, fusioni, scissioni, liquidazioni) per il controllo che: i) siano effettuate nel rispetto delle norme, con particolare ma non esclusivo riferimento alle previsioni del codice civile e dello statuto; ii) prevedano un'adeguata e sufficiente conoscenza della controparte (anche in termini reputazionali), nonché delle prospettive economico-finanziarie dell'operazione; iii) siano gestite fornendo agli organi societari e di controllo (in particolare al Collegio Sindacale) adeguati flussi informativi e documentazione; iv) siano approvate dagli organi di vertice a ciò legittimamente delegati; v) siano effettuate tracciando tutti i flussi finanziari;
- flussi informativi, anche verso l'OdV, atti a garantire che le operazioni connesse alla copertura di esigenze finanziarie o di liquidità, di breve, medio o lungo termine e coperture di rischi con strumenti finanziari, soprattutto quando non vengono poste in essere a mezzo dei canali di credito bancario ma con operazioni di finanziamento da parte di soci o di soggetti terzi, finanziamenti con Società controllate (o partecipate). Tali attività devono essere: i) effettuate nel rispetto della legge; ii) attivate a fronte di effettive necessità finanziarie; iii) prevedano un'adeguata e sufficiente conoscenza delle controparti (quando i finanziamenti non siano effettuati da soci o fra società controllate); iv) siano gestite fornendo agli organi societari e di controllo (soprattutto al Collegio Sindacale) i flussi informativi e la relativa documentazione; v) siano formalizzate in appositi atti o contratti, rispondano a criteri di economicità e sostenibilità dell'operazione, siano autorizzate dagli organi di vertice a ciò legittimamente delegati; vi) sia assicurata la tracciabilità dei flussi finanziari;
- flussi informativi, anche verso l'OdV, atti a garantire che le operazioni sul capitale (come gli aumenti di capitale, anche mediante conferimenti) siano poste in essere in conformità alla legge e allo statuto, fornendo agli organi societari e di controllo (in particolare al Collegio Sindacale) i flussi informativi, deliberate dagli organi di vertice a ciò legittimamente delegati e assicurando la tracciabilità di tutti i flussi finanziari;

- flussi informativi, anche verso l'OdV, tali da garantire che le operazioni connesse ad investimenti, all'acquisto di beni materiali o immateriali, anche quando effettuate attraverso leasing o altri strumenti finanziari siano:
 - effettuate nel rispetto della legge,
 - attivate nel rispetto del principio dell'economicità e sostenibilità dell'operazione rispetto alle esigenze di natura strategica e operativa della Società,
 - gestite fornendo agli organi societari e di controllo (soprattutto al Collegio Sindacale) i flussi informativi e la documentazione,
 - formalizzate in atti o contratti scritti,
 - autorizzate dagli organi societari delegati,
 - poste in essere tracciando i flussi finanziari.

L'Organismo di Vigilanza deve essere informato ogni qualvolta venga posta in essere un'operazione che per caratteristiche, rilevanza o natura rispetto alla normale operatività aziendale, sia configurata come:

- operazione societaria di natura straordinaria;
- attivazione di finanziamenti da parte di soci o terzi di natura non bancaria, ovvero finanziamenti con Società controllate o partecipate;
- operazione sul capitale (come gli aumenti di capitale, anche mediante conferimenti);
- altra operazione di natura straordinaria;
- investimento di particolare rilevanza.

Almeno una volta all'anno, e comunque quando si reputi necessario, l'Organismo di Vigilanza pianifica ed effettua un incontro con il Collegio Sindacale per lo scambio informativo anche sulle operazioni sopra indicate. Gli esiti di questi incontri saranno sempre formalizzati in verbali il cui contenuto sarà poi trasfuso nella relazione annuale dell'OdV al Consiglio di Amministrazione.

Sono tenuti in considerazione, in quanto applicabili anche alla presente area di rischio, i principi di controllo qui si seguito evidenziati.

2.3 Tracciabilità delle transazioni

Ogni operazione deve essere dimostrata da documenti/supporti informatici, per mezzo dei quali si possa procedere, sempre, all'esecuzione di controlli sulle caratteristiche e i motivi dell'operazione e ad individuare, sempre, chi ha autorizzato, effettuato, registrato, verificato.

2.4 Segregazione dei compiti

Il sistema garantisce il rispetto della separazione delle funzioni. Quindi, chi autorizza un'operazione concernente flussi amministrativi, contabili e di tesoreria non sarà lo stesso che la esegue e diverso da chi la controlla.

2.5 Sistema delle procure/deleghe coerente con responsabilità, ruoli e compiti

Nelle operazioni di tesoreria i poteri autorizzativi e di firma devono essere coerenti con le responsabilità assegnate, definite e conosciute all'interno di LOGIC.

SEZIONE "E"

Art.25 bis1 del Decreto231

Reati contro l'industria e commercio

Art. 25 novies del Decreto231

Reati in materia di violazione del diritto d'autore

Art. 25 bis del Decreto231

Per il reato di cui all'Art. 473 del Codice Penale

L'art. 25 novies del Decreto 231 prevede alcune fattispecie inerenti alla violazione del diritto d'autore, tra le quali sono da considerarsi:

- **Mettere a disposizione del pubblico in un sistema di reti telematiche un'opera dell'ingegno protetta o parte di essa (art. 171 l. 633/1941):** è punito chiunque:
 - a. riproduca, trascriva, reciti in pubblico, diffonda, venda o metta in vendita o ponga altrimenti in commercio un'opera altrui o ne riveli il contenuto prima che sia reso pubblico, o introduca e metta in circolazione nello Stato esemplari prodotti all'estero contrariamente alla legge italiana; o metta a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;
 - b. rappresenti, esegua o reciti in pubblico o diffonda con o senza variazioni od aggiunte, un'opera altrui adatta a pubblico spettacolo od una composizione musicale.
 - c. compia i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;
 - d. riproduca un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di produrre o di rappresentare;
 - e. in violazione dell'articolo 79 ritrasmetta su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.
- **Abusiva duplicazione di programmi o predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione per elaborare (art. 171-bis, comma 1, L. 633/1941):** è punito chiunque abusivamente duplichi, per trarne profitto, programmi per elaboratore o ai medesimi fini importi, distribuisca, venda, detenga a scopo commerciale o imprenditoriale o conceda in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori e editori (SIAE).
- **Riproduzione o trasferimento su un altro supporto, distribuzione, presentazione in pubblico del contenuto di una banca dati (art. 171-ter, L. 633/1941):** è punito chiunque a fini di lucro:
 - a. abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;
 - b. abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

- c. pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);
- d. detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;
- e. in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;
- f. introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto.
- g. fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;
- h. abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102- quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

E chiunque:

- a. riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da

- diritti connessi;
- b. in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;
 - c. esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;
 - d. promuove o organizza le attività illecite di cui al comma 1.
- **Delitti in materia di violazione del diritto d'autore (artt. 171 septies e octies, L. 633/1941):** le pene di cui all'art. 171-ter, comma 1, si applichino anche ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi e, salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.

Poi l'art. 25bis.1 disciplina alcune fattispecie inerenti ai reati di turbata libertà dell'industria e del commercio e infine l'art. 25 bis (comma 1, f-bis) i reati di falsità in segni di riconoscimento tra le quali sono da considerarsi rilevanti:

- **Turbata libertà dell'industria o del commercio (art. 513 c.p.):** è punito chiunque adoperi violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio
- **Illecita concorrenza con minaccia o violenza (art. 513bis c.p.):** è punito chiunque nell'esercizio di un'attività commerciale, industriale o comunque produttiva, compia atti di concorrenza con violenza o minaccia, con aumenti di pena se atti di concorrenza riguardano un'attività finanziata in tutto o in parte ed in qualsiasi modo dallo Stato o da altri enti pubblici.
- **Frodi contro le industrie nazionali (art. 514 c.p.):** è punito chiunque, ponendo in vendita o mettendo altrimenti in circolazione, sui mercati nazionali o esteri, prodotti industriali, con nomi, marchi o segni distintivi contraffatti o alterati, cagioni un nocumento all'industria nazionale.
- **Frode nell'esercizio del commercio (art. 515 c.p.):** è punito chiunque, nell'esercizio di un'attività commerciale, ovvero in uno spaccio aperto al pubblico, consegna all'acquirente una cosa mobile per un'altra, ovvero una cosa mobile, per origine, provenienza, qualità o quantità, diversa da quella dichiarata o pattuita.
- **Vendita di prodotti industriali con segni mendaci (art. 517 c.p.):** è punito chiunque pone in vendita o mette altrimenti in circolazione opere dell'ingegno o prodotti industriali, con nomi, marchi o segni distintivi nazionali o esteri atti ad indurre in inganno il compratore sull'origine, provenienza o qualità dell'opera o del prodotto.
- **Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517 ter c.p.):** è punito chiunque potendo conoscere dell'esistenza del

titolo di proprietà industriale, fabbrica o adopera industrialmente oggetti o altri beni realizzati usurpando un titolo di proprietà industriale.

- **Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.):** è punito chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale, contraffà o altera i marchi o segni distintivi, nazionali o esteri, delle opere dell'ingegno o dei prodotti industriali, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati e chi contraffà o altera brevetti, disegni o modelli industriali, nazionali o esteri, ovvero, senza essere concorso nella contraffazione o alterazione, fa uso di tali brevetti, disegni o modelli contraffatti o alterati. Le disposizioni precedenti si applicano sempre che siano state osservate le norme delle leggi interne, dei regolamenti comunitari e delle convenzioni internazionali sulla tutela della proprietà intellettuale o industriale.
- **Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.):** è punito chiunque introduce nel territorio dello Stato, al fine di trarne profitto, prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati.

In considerazione della missione aziendale di LOGIC e della struttura interna, le attività sensibili e i processi strumentali a rischio di commissione dei suddetti reati sono i seguenti:

- utilizzo di beni di natura informatica o telematica ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore;
- gestione degli approvvigionamenti;
- le attività gestite dalle Funzioni della produzione. progettazione e qualità.

1 Principi di comportamento

I seguenti principi di comportamento si applicano ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività sensibili rispetto alla commissione dei reati in materia di violazione del diritto d'autore, contro l'industria e il commercio e di contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli o disegni o di introduzione nello Stato e commercio di prodotti con segni falsi, nell'interesse o a vantaggio della Società.

Ai Destinatari è vietato porre in essere o collaborare alla realizzazione di comportamenti tali che integrino o possano integrare, direttamente o indirettamente, i reati sopra evidenziati.

Questi Destinatari devono:

- osservare le norme di legge, del Codice Etico, del presente Modello e delle procedure aziendali per quanto riguarda i limiti, i termini e le modalità delle attività economico-commerciali della Società;
- avere condotte lineari e trasparenti per garantire le corrette attività commerciali e una libera concorrenza nel mercato;
- astenersi da condotte commerciali finalizzate o comunque idonee a ledere la buona fede del cliente;
- rispettare i diritti di proprietà industriale e intellettuale;

In particolare, è vietato:

- alterare o contraffare marchi o segni distintivi nazionali ed esteri depositati/registrati ovvero fare uso di marchi o segni distintivi alterati oppure contraffatti;
- alterare o contraffare brevetti, disegni, modelli industriali ovvero fare uso di brevetti, disegni o modelli industriali alterati oppure contraffatti;
- importare opere dell'ingegno o prodotti con marchi, segni distintivi e brevetti contraffatti o alterati;
- adottare condotte violente ovvero ricorrere a raggiri o artifici di qualunque tipo, al fine di creare ostacoli al libero commercio ed industria;
- usare violenza o minaccia al fine di ostacolare illecitamente la concorrenza;
- mettere in circolazione, anche attraverso l'immagazzinamento finalizzato alla vendita o allo sdoganamento, opere o prodotti con nomi, marchi o segni distintivi alterati o contraffatti;
- vendere o mettere in circolazione, anche attraverso l'immagazzinamento finalizzato alla distribuzione allo sdoganamento, opere o prodotti con nomi, marchi o segni distintivi altrui, anche se non registrati, al fine di trarre in inganno il cliente;
- produrre o utilizzare oggetti o altri beni, realizzati usurpando o violando il diritto d'autore altrui o brevetti di terzi;
- introdurre nel territorio dello Stato, detenere per la vendita, porre in vendita o comunque mettere in circolazione beni realizzati usurpando il diritto d'autore o brevetti di terzi;
- diffondere - tramite reti telematiche - un'opera dell'ingegno o parte di essa;
- duplicare, importare, distribuire, vendere, diffondere, detenere a scopo commerciale programmi per elaboratori, banche dati protette ovvero qualsiasi opera protetta dal diritto d'autore.

In caso di dubbi nel corso delle attività aziendali, il Destinatario deve interpellare il proprio Responsabile di Funzione (in caso di dipendente di LOGIC) o referente interno (in caso di soggetti terzi) informando, anche tramite il suo Responsabile di Funzione, l'Organismo di Vigilanza.

Nei confronti dei terzi (come i collaboratori, consulenti, partner, fornitori, clienti) i relativi contratti devono:

- essere scritti;
- contenere le clausole "231".

2 Controlli

In relazione ai rischi connessi ai citati reati i principi di comportamento pretendono i seguenti controlli.

2.1 *Attribuzione delle responsabilità*

Definizione dei ruoli e delle responsabilità dei Destinatari coinvolti nell'utilizzo di beni che sono opera dell'ingegno protetta dal diritto d'autore.

2.2 Tracciabilità delle transazioni

Ogni processo relativo all'utilizzo di opere dell'ingegno protette dal diritto d'autore prevede idonea documentazione per consentire, durante e a posteriori, le verifiche delle caratteristiche e delle motivazioni della transazione, di chi ha autorizzato, effettuato, registrato, verificato la transazione stessa.

2.3 Segregazione dei compiti

Il sistema garantisce il principio di separazione di funzioni tra chi ha autorizzato, che ha eseguito e chi ha controllato.

2.4 Sistema delle procure/deleghe coerente con responsabilità, ruoli e compiti

Anche in questa area sensibile i poteri autorizzativi e di firma sono coerenti con le responsabilità organizzative e gestionali, definiti e conosciuti all'interno della Società.

Sono previsti i seguenti ulteriori protocolli preventivi:

- il Responsabile IT tiene aggiornato l'elenco dei produttori di software e esprime la sua valutazione/parere al momento degli acquisti di tali beni;
- è vietata l'effettuazione di copie di software;
- effettuazione di audit, anche a sorpresa, da parte sia dell'organo di vertice sia da parte dell'OdV, sui beni tutelati dai reati sopra evidenziati;
- il Responsabile della Funzione "Progettazione" deve verificare che l'attività di sua competenza si svolga sempre nel pieno rispetto dei diritti alla tutela delle opere dell'ingegno, soprattutto brevetti, marchi, modelli e disegni. Deve controllare se esistono vincoli all'utilizzo dei prodotti come software e hardware. In caso di dubbi deve informare l'Amministratore Delegato per le conseguenti valutazioni ed eventuali richieste di consulenze specifiche e/o per effettuare/far effettuare apposite ricerche;
- il Responsabile della Funzione "Produzione" deve controllare che tutti i materiali utilizzati siano sempre contrassegnati da marchi e/o segni distintivi e che questi risultino conformi alle condizioni di acquisto e che mai i marchi/segni distintivi siano rimossi o alterati;
- il Responsabile della Funzione "Qualità" in caso di sospetto di utilizzo di beni contraffatti o di indebito uso degli stessi in violazione delle norme a tutela dei marchi, brevetti, disegni e dell'ingegno, informa l'Amministratore Delegato e l'OdV.

I suddetti tre Responsabili di Funzione annualmente inviano un report all'OdV contenente gli esiti dei controlli di rispettiva loro pertinenza.

SEZIONE "F"
Art. 24 bis del Decreto 231
Reati informatici e trattamento illecito di dati

L'art. 24 bis del Decreto 231 comprende i reati qui di seguito indicati:

- **Falsità in documenti informatici (art. 491-bis c.p.):** il reato in esame si realizza qualora una delle falsità previste dal Capo III (Falsità in atti) del Titolo VII, Libro II, del Codice riguardi un documento informatico pubblico o privato avente efficacia probatoria. Il sopra menzionato Capo riguarda i delitti contro la fede pubblica, tra i quali si ricomprendono: falsità materiale commessa dal pubblico ufficiale in atti pubblici (art. 476 c.p.); falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative (art. 477 c.p.); falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici e in attestati del contenuto di atti (art. 478 c.p.); falsità ideologica commessa dal pubblico ufficiale in atti pubblici (art. 479 c.p.); falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative (art. 480 c.p.); falsità materiale commessa dal privato (art. 482 c.p.); falsità materiale commessa dal privato in atto pubblico (art. 483 c.p.); falsità in registri e notificazioni (art. 484 c.p.); uso di atto falso (art. 489 c.p.); soppressione, distruzione e occultamento di atti veri (art. 490 c.p.).
- **Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.):** è punito chiunque abusivamente si introduca in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 - quater c.p.):** è punito chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare a altri un danno, abusivamente riproduca, si procuri, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.
- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.):** è punito chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procuri, produca, riproduca, importi, diffonda, comunichi, consegni o, comunque, metta a disposizione di altri apparecchiature, dispositivi o programmi informatici.
- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.):** è punito chiunque fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa, o a chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui sopra.
- **Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.):** è punito chiunque, fuori dai casi consentiti dalla legge, installi apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.
- **Danneggiamento di informazioni, dati e programmi informatici (inclusi quelli utilizzati dallo Stato o altro Ente) (Art. 635-bis e 635 ter c.p.):** è punito chiunque distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui. Se gli stessi sono utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di

pubblica utilità, si applicano le disposizioni di cui all'art. 635 ter c.p., con le relative più afflittive sanzioni.

- **Danneggiamento di sistemi informatici o telematici (incluso quello di pubblica utilità) (Art. 635-quater e 635 quinquies c.p.):** è punito, salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento. Se le stesse condotte sono rivolte verso sistemi informatici o telematici di pubblica utilità o ad ostacolare gravemente il funzionamento di questi ultimi, si applicano le disposizioni, maggiormente afflittive, dell'art. 635 quinquies c.p.
- **Frode informatica del certificatore di firma elettronica (art. 640 quinquies c.p.):** è punito il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé' o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, violi gli obblighi previsti alla legge per il rilascio di un certificato qualificato

In considerazione della specificità della missione aziendale di LOGIC e della sua struttura interna, le principali attività sensibili e i processi strumentali a rischio di commissione dei reati in oggetto possono essere i seguenti:

- utilizzo di risorse e informazioni di natura informatica o telematica ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore;
- adempimenti per la tutela della protezione dei dati personali;
- gestione sicurezza area IT;
- sviluppo e manutenzione IT;
- trattamento informatico dei documenti di progetto, di produzione e di commercializzazione dei beni progettati e/o prodotti;
- controllo logico accessi;
- inventario e gestione delle dotazioni IT.

1 Principi di comportamento

Ai Destinatari del presente Modello che a qualunque titolo siano coinvolti nelle suddette attività sensibili devono:

- osservare rigorosamente tutte le norme poste dalla legge e dalle procedure aziendali interne in merito alla sicurezza dei sistemi informativi della Società ed al trattamento, oltre che dei dati industriali, anche dei dati personali;
- astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, questi reati informatici o il trattamento illecito di dati.

Inoltre, i Destinatari:

- hanno il divieto assoluto di rendere pubbliche tutte le informazioni relative all'utilizzo delle risorse informatiche e all'accesso a dati e sistemi (avendo particolare cura alla

protezione dello username e della password necessari per l'accesso ai sistemi informatici di LOGIC);

- devono attivare ogni misura ritenuta necessaria per la protezione del sistema, evitando che terzi possano avere accesso allo stesso in caso di allontanamento dalla postazione (uscita dal sistema, ovvero blocco dell'accesso tramite password);
- devono accedere ai sistemi informativi unicamente a mezzo dei codici identificativi assegnati al singolo soggetto e provvedere alla modifica periodica della password entro le scadenze indicate;
- devono astenersi dal porre in essere qualsivoglia comportamento che possa mettere a rischio la riservatezza e/o l'integrità dei dati aziendali;
- non devono intraprendere azioni atte a superare le protezioni applicate ai sistemi informativi aziendali;
- non devono installare alcun programma, anche se attinente all'attività aziendale, senza aver prima interpellato il Responsabile IT della Società;
- non devono utilizzare connessioni alternative rispetto a quelle messe a disposizione da parte della Società per l'espletamento della propria attività lavorativa;
- non devono accedere, senza specifica autorizzazione, ai sistemi informativi di terzi (per terzi si intendono anche gli altri dipendenti di LOGIC), né alterarne in alcun modo il funzionamento, al fine di ottenere e/o modificare, senza diritto, dati, programmi o informazioni;
- non devono utilizzare i sistemi informativi aziendali per l'attuazione di comportamenti suscettibili di integrare fattispecie di concorrenza sleale nei confronti di imprese concorrenti di LOGIC o, più in generale, di qualsivoglia altra persona fisica/giuridica;
- non devono connettersi, consultare, navigare, effettuare attività di streaming e download, a siti web che siano considerabili illeciti (come i siti che presentino contenuti contrari alla morale, alla libertà di culto ed all'ordine pubblico, che consentano la violazione della privacy, che promuovano e/o appoggino movimenti terroristici o sovversivi, riconducibili ad attività di pirateria informatica, ovvero violino le norme in materia di copyright e di proprietà intellettuale).

Nei confronti di terze parti contraenti (come i collaboratori, consulenti, partner, fornitori, clienti) coinvolte nello svolgimento di attività a rischio rispetto agli illeciti informatici e al trattamento illecito di dati e che operano per conto o nell'interesse di LOGIC, i relativi contratti devono:

- essere scritti, in tutte le loro condizioni e termini;
- comprendere le clausole "231".

2 Controlli

I suddetti principi di comportamento si legano ai seguenti livelli di controllo.

2.1 *Attribuzione delle responsabilità*

Prevedendo:

- la definizione dei ruoli, delle responsabilità, degli obblighi e dei divieti inerenti alla gestione delle modalità di accesso di utenti interni all'azienda e all'utilizzo dei sistemi informatici;
- la definizione dei ruoli delle responsabilità nella gestione delle eventuali modalità di accesso di utenti esterni all'azienda e gli obblighi dei medesimi nell'utilizzo dei sistemi informatici, nonché nella gestione dei rapporti con i terzi in caso di accesso, gestione, comunicazione, fornitura di prodotti/servizi per l'elaborazione dei dati e informazioni da parte degli stessi terzi. In ogni caso, tali accessi, se motivati, saranno individualmente e preventivamente autorizzati dall'Amministratore Delegato.

Controlli specifici, relativi alle attività sensibili di cui sopra, rappresentati:

- da una policy in materia di sicurezza del sistema informativo aziendale che prevede, fra l'altro:
 - la diffusione delle modalità operative, degli obblighi e dei divieti inerenti all'utilizzo dei sistemi informativi, anche nei confronti di terzi;
 - le modalità di riesame periodico o a seguito di cambiamenti significativi della politica stessa.
 - dalla disciplina aziendale che:
 - dispone l'adozione di controlli (audit periodici e non) al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti, tramite la messa in sicurezza delle aree e delle apparecchiature;
 - assicura la correttezza e la sicurezza dell'operatività dei sistemi informativi. In particolare:
 - il corretto e sicuro funzionamento dell'apparato tecnologico informatico;
 - la protezione da software pericolosi;
 - il back-up;
 - la protezione dello scambio di informazioni con terzi;
 - gli strumenti per effettuare la tracciatura delle attività eseguite sulle applicazioni, sui sistemi e sulle reti e la protezione di tali informazioni contro accessi non autorizzati;
 - una verifica dei log che registrano le attività degli utilizzatori, le eccezioni e gli eventi concernenti la sicurezza informatica;
 - il controllo sui cambiamenti ai sistemi e agli apparati;
 - la gestione di dispositivi rimovibili;
-

- disciplinare gli accessi alle informazioni, ai sistemi informativi, alla rete, ai sistemi operativi, alle applicazioni prevedendo:
 - l'autenticazione individuale degli utenti tramite codice identificativo e password o altro sistema di autenticazione sicura;
 - le modalità di cambiamento della password, a seguito del primo accesso, vietando l'utilizzo di medesime password;
 - la periodicità di modifica delle stesse password, a seconda della frequenza di utilizzo e della criticità dei dati cui si accede;
 - le liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti;
 - la registrazione e la disattivazione per autorizzare e revocare l'accesso a tutti i sistemi e servizi informativi;
 - la rivisitazione dei diritti d'accesso degli utenti secondo intervalli di tempo prestabiliti;
 - la destituzione dei diritti di accesso in caso di cessazione o cambiamento del tipo di rapporto di lavoro o di delega o di procura per i quali era stato concesso l'account;
 - l'accesso ai servizi di rete esclusivamente da parte degli utenti che sono stati specificatamente autorizzati e le restrizioni della capacità degli utenti di accedere a determinati siti o reti;
 - la segmentazione della rete affinché sia possibile assicurare che le connessioni e i flussi di informazioni non violino le norme di controllo degli accessi alle diverse applicazioni aziendali;
 - la chiusura di sessioni inattive dopo un predefinito periodo di tempo;
 - la custodia dei dispositivi di memorizzazione (come le chiavi USB, CD, hard disk esterni) e l'adozione di regole di clear screen per gli elaboratori utilizzati;
- definisce adeguate modalità per il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica. A tal fine, a cura del Responsabile IT:
 - sono predisposti appropriati canali gestionali per la comunicazione degli incidenti e problemi;
 - è effettuata l'analisi periodica di tutti gli incidenti, singoli e ricorrenti, e delle cause di essi;
 - vengono gestiti i problemi che hanno generato uno o più incidenti, fino alla loro risoluzione;
 - sono analizzati i report sugli incidenti per l'individuazione di azioni correttive e preventive per eliminare o attenuare le criticità;
- la procedura prevede anche:
 - la valutazione (prima dell'assunzione o della stipula di un contratto di collaborazione esterna) dell'esperienza e delle capacità tecnico-professionali delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza

dei sistemi informativi e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso;

- specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, se previsto, per i terzi;
- l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (come i pc, telefoni cellulari, chiavi usb, cd, dvd, token) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto;
- l'eliminazione, per tutti i dipendenti e i terzi, di tutti gli accessi alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta;
- l'identificazione di requisiti di sicurezza in fase di progettazione o modifica dei sistemi informativi esistenti;
- la gestione dei rischi di errori, perdite, modifiche non autorizzate di informazioni trattate dalle applicazioni;
- la confidenzialità, autenticità e integrità delle informazioni;
- la sicurezza nel processo di sviluppo dei sistemi informativi.

2.2 Il Codice Etico, il Modello 231 e il Protocollo per la Sicurezza Informatica

Il Codice Etico e il Modello 231 già disciplinano l'utilizzo delle risorse informatiche messe a disposizione dei dipendenti di LOGIC. L'uso di queste risorse è consentito solo per scopi aziendali, a meno che l'Amministratore Delegato non ne approvi altri usi specifici.

Esiste, inoltre, una policy aziendale volta a disciplinare l'utilizzo degli strumenti informatici da parte dei dipendenti della Società. Tale regolamento viene consegnato ad ogni nuovo dipendente al momento dell'assunzione sottoscritto per accettazione. Comunque, lo stesso regolamento viene inserito nella rete intranet aziendale a disposizione di tutto il Personale.

Il processo di gestione degli accessi al dominio e ai sistemi è formalizzato nella predetta policy.

La creazione/modifica/cancellazione di una utenza è sempre autorizzata dal rispettivo Responsabile di funzione mediante compilazione e firma di uno specifico modulo ed inviata all'amministratore di sistema (IT) per l'attuazione. Le abilitazioni dei diversi profili di accesso al sistema degli utenti (profilo solo visualizzazione, profilo per le attività di *front-office* e *back-office*, profili con funzionalità specifiche) vengono concesse solo dopo e-mail di richiesta autorizzazione del Responsabile di funzione.

Tutte le abilitazioni sono trascritte in uno specifico elenco, via via aggiornato, di cui copia viene conservata dall'Amministratore Delegato.

Lo stesso Amministratore Delegato provvederà ad autorizzare i Responsabili di funzione alle abilitazioni necessarie.

2.3 Tracciabilità delle transazioni

Per garantire la tracciabilità dei controlli e dei presidi di prevenzione dei reati informatici e il riscontro delle azioni poste in essere dai Destinatari del Codice Etico e del presente Modello, le

attività effettuate tramite i sistemi informatici sono tutte tracciate e tracciabili.

Compiti della Funzione IT:

- la creazione, modifica e disattivazione dei profili di accesso;
- la manutenzione degli hardware, dei software e delle reti;
- gli audit sulla sicurezza e l'integrità del sistema informativo aziendale;
- la programmazione delle misure di sicurezza del sistema informativo.

La predetta Funzione tiene e conserva le specifiche evidenze delle azioni svolte a mezzo di supporto cartaceo o informatico.

2.4 Segregazione dei compiti

In riferimento ai reati informatici e al trattamento illecito di dati, per garantire l'applicazione del principio di separazione dei ruoli, è previsto che alcune specifiche attività siano organizzate al fine di prevedere la segregazione delle responsabilità tra chi autorizza, chi esegue e chi controlla le attività. Quindi, è previsto che:

- la Funzione IT provvede all'attivazione, modifica o disattivazione degli accessi ai sistemi informatici aziendali ed è diversa da quelle che inoltrano le relative richieste: ogni semestre il Responsabile IT invierà un report all'Amministratore Delegato e all'OdV contenente la sintesi delle attività svolte in questo settore;
- nello stesso report (flusso informativo) il Responsabile IT comunicherà gli esiti degli audit effettuati indicando le eventuali azioni correttive e le aree di miglioramento;
- lo stesso Responsabile avrà cura di proporre all'Amministratore Delegato, se del caso, lo svolgimento di audit da parte di consulenti esterni appositamente selezionati.

Parallelamente alla prevenzione dei reati informatici e al trattamento illecito di dati, LOGIC tutela la protezione dei dati personali disciplinandone il trattamento, con propria policy aziendale, ai sensi del Reg. UE 679 del 2016, applicabile dal 24 maggio 2018 e secondo le norme del D.Lgs. 196 del 2003 così come modificato dal D.Lgs. 101 del 2018.

SEZIONE "G"

Art. 25 septies del Decreto 231

Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

L'art. 25-septies del Decreto 231 riguarda le ipotesi di omicidio colposo e di lesioni colpose gravi o gravissime:

- **omicidio colposo (art. 589 c.p.):** il reato in esame punisce chiunque cagioni per colpa la morte di una persona.
- **lesioni colpose gravi o gravissime (art. 590, co. 3, c.p.):** tale reato punisce chiunque cagioni ad altri per colpa una lesione personale.

Le due fattispecie sopra elencate di reato costituiscono reati presupposto del Decreto se determinati dalla **violazione o attraverso la mancata applicazione delle norme in materia di igiene, sicurezza e salute sul lavoro allorquando ciò determini un interesse o un vantaggio alla Società, per esempio diminuendo i costi necessari all'acquisto di DPI o aumentando la produzione a discapito delle norme sulla salute e sicurezza sul lavoro.**

È importante sottolineare che per la commissione di questi reati è prevista la colpa e non il dolo.

Ciò significa aver avuto la coscienza e volontà dell'azione ma non quelle dell'evento costituito, in questi casi, dalla morte o dalle lesioni gravi o gravissime del lavoratore.

In relazione alle attività di LOGIC e della struttura interna adottata, le principali attività sensibili e i processi strumentali a rischio di commissione dei reati in oggetto sono costituiti dalla gestione degli adempimenti relativi a salute e sicurezza sul luogo di lavoro e dei rapporti con i clienti (pubblici e privati) per il rispetto delle cautele previste da leggi e regolamenti e interessa tutte le funzioni aziendali, ognuna per i rischi correlati alle rispettive attività svolte.

1 Principi di comportamento

Unitamente alle regole che tutti i dipendenti/collaboratori/clienti sono obbligati a rispettare, vengono evidenziati anche le misure di prevenzione che la Società è tenuta a adottare al fine di garantire la salute e la sicurezza dei suoi dipendenti/collaboratori/clienti e, quindi, evitare il verificarsi di qualsivoglia evento che possa comportare l'insorgenza della responsabilità dell'ente ai sensi del Decreto.

Ai Destinatari del presente Modello che, a qualunque titolo, siano coinvolti nelle attività sensibili rispetto ai reati sopra indicati è richiesto di:

- osservare rigorosamente tutte le norme poste dalla legge e dalle procedure aziendali interne in materia di salute, sicurezza ed igiene sul lavoro;
- comunicare tempestivamente al Responsabile per la Sicurezza (RSPP), designato dal Datore di lavoro, e all'Organismo di Vigilanza qualsivoglia informazione relativa ad infortuni e ai mancati infortuni avvenuti a collaboratori/dipendenti/clienti nell'esercizio della propria attività professionale, anche qualora il verificarsi dei suddetti avvenimenti non abbia comportato la violazione del Modello;
- segnalare prontamente al Responsabile per la Sicurezza (RSPP) e all'Organismo di Vigilanza possibili aree di miglioramento e/o eventuali carenze procedurali riscontrate durante la propria lavorativa.

Nell'ambito di tali comportamenti, è vietato porre in essere, in ogni modo, condotte (commissive od omissive) che possano rappresentare una violazione delle norme antinfortunistiche e sulla tutela

dell'igiene e della salute sul lavoro.

È obbligo della Società (e per essa dei soggetti responsabili sopra indicati e più avanti meglio definiti) di:

- elaborare una politica aziendale di individuazione dei rischi inerenti alla sicurezza ed alla salute sui luoghi di lavoro con riferimento alla natura ed all'incidenza degli stessi rispetto alle attività svolte, ai luoghi dove avvengono ed alle dimensioni della Società;
- assicurare il rispetto e l'effettiva attuazione degli adempimenti previsti dal D.Lgs. 81/08 (T.U.) e da altre normative di settore. In particolare per quanto riguarda: la predisposizione ed l'aggiornamento del documento di valutazione dei rischi (il DVR approvato dal Datore di lavoro); l'applicazione dei principi ergonomici nella progettazione e organizzazione delle attività lavorative; l'attenzione all'evoluzione tecnica e all'eventuale obsolescenza degli strumenti, attrezzi e, più in generale, di tutte le apparecchiature utilizzate nell'ambito delle attività lavorative; la programmazione delle attività di prevenzione, di formazione ed informazione dei dipendenti/collaboratori/clienti in materia di salute e sicurezza sul lavoro; la predisposizione di ulteriore documentazione eventualmente prevista da leggi e regolamenti;
- programmare, in aggiunta al controllo di natura tecnico-operativa in capo al Responsabile della Sicurezza (RSPP), un controllo di secondo livello da parte dell'Organismo di Vigilanza che avrà il compito di monitorare i presidi implementati dall'azienda in tema di salute, igiene e sicurezza sul lavoro vigilando sui doveri del Datore di lavoro, dei Dirigenti e Preposti se designati, del RSPP, del Rappresentante dei lavoratori per la sicurezza (RSL), del medico competente;
- prevedere uno scambio informativo tra l'Organismo di Vigilanza ed il Responsabile della Sicurezza (RSPP), anche tramite incontri, garantendo, nel contempo, la riservatezza dei soggetti segnalanti. In particolare, devono essere inviati all'OdV i verbali delle riunioni periodiche di cui all'art. 35 del TU 81 e le comunicazioni relative agli infortuni e i mancati infortuni eventualmente avvenuti.

In caso di dubbi circa la corretta attuazione delle regole di cui sopra è obbligo per il dipendente interessato di interpellare il Responsabile SPP e il Rappresentante per la sicurezza dei lavoratori o il referente interno (per i collaboratori/clienti) informandone per conoscenza l'Organismo di Vigilanza.

Ogni Responsabile di Funzione aziendale è responsabile della veridicità, autenticità ed originalità della documentazione prodotta dalla sua Funzione e delle informazioni rese relative alle attività di propria competenza agli Organi di controllo.

LOGIC assicura risorse umane e finanziarie adeguate a tutelare la salute e la sicurezza sui luoghi di lavoro e per il funzionamento del servizio di prevenzione e protezione, in piena osservanza di quanto stabilito dal TU 81.

Nei confronti dei soggetti non dipendenti della Società (come i collaboratori esterni, consulenti, partner, fornitori, clienti), che operano per suo conto e/o nel suo interesse o che hanno rapporti commerciali con la Società, i relativi contratti, sempre per iscritto, devono contenere le clausole standard al fine del rispetto del Codice Etico e del Modello 231 che comprende anche la Sezione "Salute e Sicurezza sui luoghi di lavoro".

2 Controlli

In merito ai rischi "231" relativi alla salute e sicurezza sul lavoro, i principi di comportamento sopra esposti sono contenuti nei seguenti protocolli che devono essere osservati dai soggetti qui di seguito citati.

2.1 *Attribuzione delle responsabilità*

Definizione di ruoli, responsabilità e disposizioni aziendali in materia di salute e sicurezza sul luogo di lavoro, finalizzata a disciplinare le modalità operative e i controlli in essere per lo svolgimento delle attività sensibili, nonché le modalità di archiviazione della documentazione rilevante.

Di seguito un elenco non esaustivo di obblighi di quei soggetti che, in ambito Logic, rivestono un ruolo di garanzia e responsabilità per quanto riguarda la prevenzione dei reati nell'area salute e sicurezza lavoro.

Il Datore di lavoro:

- nomina il Responsabile del Servizio di Prevenzione e Protezione, in base ai requisiti richiesti dall'articolo 32 del TU 81/2008;
- effettua la valutazione dei rischi presenti in azienda in collaborazione con RSPP e medico competente, previa consultazione del Rappresentante dei lavoratori per la sicurezza (RLS). Il Datore di lavoro provvede inoltre a riesaminare periodicamente tale analisi, al fine di individuare eventuali variazioni dei rischi per la salute e la sicurezza dei lavoratori, rimodulando, se del caso, il Documento di Valutazione dei Rischi (DVR)
- e approva il documento sulla valutazione dei rischi per la sicurezza (DVR) che abbia data certa, specificando i criteri adottati per le valutazioni stesse, le misure di prevenzione e di protezione e i dispositivi di protezione individuale adottati, il programma delle misure ritenute opportune per garantire il miglioramento continuo nel tempo dei livelli di sicurezza, l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché gli altri soggetti dell'azienda che vi debbono provvedere. Il documento indica altresì il nominativo del RSPP, del/degli RLS e del medico competente che hanno contribuito, sulla base delle rispettive competenze, alla valutazione dei rischi e individua le mansioni che eventualmente espongono i lavoratori a rischi specifici e che, pertanto, richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento. Tale documento dovrà necessariamente essere aggiornato:
 - in caso di modifiche ad uno degli elementi della relazione prima citati;
 - in occasione di modifiche significative, ai fini della salute e sicurezza dei lavoratori, riguardanti il processo produttivo o l'organizzazione del lavoro;
 - in relazione all'evoluzione tecnica o della normativa di riferimento o in presenza di specifiche necessità di rafforzamento delle misure di prevenzione e protezione;
 - a seguito di infortuni significativi o quando i risultati della sorveglianza sanitaria ne evidenzino la necessità;
 - in corrispondenza di variazioni dei rischi per la salute e la sicurezza, evidenziati

attraverso la relativa analisi sopra citata.

Si evidenzia che queste anzidette attività sono di esclusiva competenza del Datore di lavoro in quanto non sono delegabili (art. 17 del TU 81).

Il Datore di lavoro e/o soggetto delegato:

- designa preventivamente gli Addetti al Servizio di Prevenzione e Protezione, in base ai requisiti richiesti dall'articolo 32 del TU 81/2008;
- nomina il Medico Competente per l'effettuazione della sorveglianza sanitaria, in base ai requisiti di cui all'articolo 38 del D.Lgs. 81/2008, monitorando le attività svolte dallo stesso, nell'ambito del piano di sorveglianza sanitaria;
- convoca le riunioni con i soggetti aventi specifiche responsabilità in materia di salute e sicurezza sul lavoro (RSPP, Medico Competente, RLS e ogni altro soggetto con conoscenze o responsabilità inerenti al tema della riunione) tra cui la riunione annuale obbligatoria prevista dall'art. 35 del TU 81;
- in relazione agli obblighi connessi ai contratti svolge le attività necessarie alla predisposizione, se necessario, del Documento Unico di Valutazione dei Rischi da Interferenza (DUVRI), condiviso con i soggetti terzi con cui la Società andrà a realizzare il progetto e la produzione;
- consegna, tramite i suoi delegati, ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il Responsabile del servizio di prevenzione e protezione e il medico competente;
- garantisce l'implementazione e l'aggiornamento delle misure di prevenzione, in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza sul lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione, prevedendo un adeguato sistema di vigilanza sul rispetto delle procedure e delle misure di sicurezza da parte dei lavoratori;
- cura, direttamente o tramite i suoi delegati, le attività di verifica e manutenzione delle macchine e delle attrezzature di lavoro, affinché siano conformi alle disposizioni di legge in materia antinfortunistica;
- assicura che sia fornita adeguata formazione a tutto il Personale in materia di sicurezza, sia in occasione dell'assunzione che del trasferimento ad altre mansioni. In ogni caso, la formazione deve essere adeguata agli eventuali rischi specifici della mansione cui il lavoratore è in concreto assegnato. A riguardo, prende appropriate misure affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio specifico. In merito a questa specifica formazione si sottolinea che deve comprendere anche quella relativa al Codice Etico, al Modello 231 e all'OdV con lo scopo di illustrare a tutto il Personale come la Società, adottando il Modello 231, abbia inteso presidiare anche le aree aziendali dove potenzialmente potrebbero essere commessi, seppur per colpa, i reati di cui all'art. 25 septies del Decreto 231;
- adotta adeguate misure (come per esempio il monitoraggio, le verifiche, le indicazioni) che comportino l'osservanza, da parte dei singoli lavoratori, delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza del lavoro e utilizzo dei mezzi di protezione collettivi e dei dispositivi di protezione individuali;

- si assicura che siano adottate le misure necessarie alla prevenzione incendi, all'evacuazione dei luoghi di lavoro, in caso di pericolo grave e immediato, e al monitoraggio di eventuali situazioni a rischio per la salute e la sicurezza dei lavoratori (con appropriate verifiche sui luoghi di lavoro);
- in caso di emergenze che comportino un pericolo grave, immediato ed inevitabile, dà istruzioni affinché i lavoratori abbandonino il posto di lavoro o la zona pericolosa, informandoli del rischio stesso e delle disposizioni prese o da prendere in materia di protezione;
- cura la corretta tenuta del registro infortuni, facendo in modo che tutti gli infortuni (e mancati infortuni) siano registrati in modo corretto, chiaro e veritiero;
- provvede affinché siano comunicati all'INAIL, per fini statistici e informativi, i dati relativi agli infortuni sul lavoro, nonché i nominativi dei Rappresentanti dei Lavoratori per la Sicurezza, avendo cura di trasmettere all'Ente medesimo informazioni corrette, documentate e veritiere;
- consulta il Rappresentante dei Lavoratori per la Sicurezza nelle ipotesi indicate dall'art. 50 del TU 81;
- provvede all'adozione delle misure necessarie affinché gli ambienti di lavoro e l'organizzazione dei processi produttivi garantiscano le condizioni di igiene e salubrità necessarie per svolgere efficacemente le attività aziendali, fermo restando il rispetto delle disposizioni di legge;
- vigila affinché i lavoratori, per i quali vige l'obbligo di sorveglianza sanitaria, non siano adibiti alla mansione lavorativa specifica senza che il medico competente abbia espresso il proprio giudizio di idoneità;
- cura la gestione dei rapporti con gli Enti incaricati di effettuare verifiche e ispezioni, nonché con gli enti e le organizzazioni che si occupano di studi, ricerche e dell'erogazione dei finanziamenti o contributi alle imprese in materia di salute e sicurezza sul lavoro;
- adotta provvedimenti disciplinari, in conformità alle disposizioni contrattuali e legislative, nei confronti dei lavoratori che non osservino le misure di prevenzione e le procedure di sicurezza mettendo in pericolo, attuale o potenziale, la propria o altrui sicurezza. A tal fine, si evidenzia che, come disciplinato dall'art. 30 del TU 81 con il rinvio ai Modelli di organizzazione previsti dal Decreto 231, questo Modello prevede, nella Parte Generale, anche il sistema disciplinare che sarà attivato in caso di violazione del Modello stesso. Tra le violazioni, sono comprese anche quelle eventualmente commesse in relazione alle regole del sistema salute e sicurezza sul lavoro. Tutti i procedimenti disciplinari attivati per questi illeciti saranno comunicati all'OdV se non hanno avuto origine dall'OdV medesimo.

Il Responsabile SPP:

- collabora con il Datore di lavoro all'individuazione e la valutazione dei fattori di rischio al fine di individuare le misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente;
- elabora, per quanto di competenza, le misure preventive e protettive di cui all'art. 28 del TU 81 e i sistemi di controllo di tali misure;

- elabora le procedure di sicurezza per le attività aziendali;
- propone programmi di informazione e formazione dei lavoratori;
- partecipa alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica ai sensi dell'articolo 35 del D.Lgs. 81/2008;
- fornisce ai lavoratori le informazioni relative a:
 - rischi generali e specifici connessi all'attività di LOGIC, alle procedure di primo soccorso e antincendio, alle misure di prevenzione e protezione adottate;
 - nominativi del medico competente, del Responsabile del Servizio di Prevenzione e Protezione, degli Addetti al Servizio di Primo Soccorso e di Prevenzione Incendi, degli altri Addetti al Servizio di Prevenzione e Protezione eventualmente designati;
 - gli altri punti indicati dall'art. 36 del più volte citato TU.

Il Medico Competente:

- collabora con il Datore di Lavoro e con il Responsabile della Sicurezza, Prevenzione e Protezione alla predisposizione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori;
- svolge l'attività di sorveglianza sanitaria attraverso l'effettuazione di visite mediche preventive e periodiche previste dalla legge e da programmi di prevenzione opportunamente stabiliti;
- esprime il giudizio di idoneità/inidoneità specifica alla mansione;
- collabora all'attività di informazione e formazione dei lavoratori e alla predisposizione del servizio di pronto soccorso;
- partecipa alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica ai sensi dell'articolo 35 del TU.

I Preposti, se nominati:

- sovrintendono e vigilano sull'osservanza, da parte dei singoli lavoratori, dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro, di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale, informando il Delegato del Datore di Lavoro (il Dirigente se designato) in caso di persistenza della condotta errata;
- verificano che solo i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
- si assicurano che i lavoratori osservino le misure previste in caso di emergenze o situazioni che presentino rischi per la Salute e la Sicurezza, dando istruzioni affinché gli stessi abbandonino il posto di lavoro o la zona pericolosa in caso di pericolo grave, immediato e inevitabile;
- segnalano tempestivamente al Delegato del Datore di Lavoro (Dirigente) le carenze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro.

I Rappresentanti dei Lavoratori per la Sicurezza (art. 50 del TU 81):

- accedono ai luoghi di lavoro, verificando che siano state adottate le misure necessarie per la tutela della Salute e la Sicurezza dei lavoratori;
- sono consultati preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive;
- sono consultati sulla designazione del RSPP, degli ASPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso;
- sono consultati in merito all'organizzazione delle attività formative;
- sono informati di eventuali visite e verifiche effettuate dalle autorità competenti, formulando a riguardo le proprie osservazioni, nel caso in cui lo ritengano necessario;
- avvertono il Datore di lavoro dei rischi individuati nel corso della loro attività e promuovono l'elaborazione, l'individuazione a l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei Lavoratori;
- partecipano alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica ai sensi dell'articolo 35 del TU 81;
- possono far ricorso alle autorità competenti qualora ritengano che le misure di prevenzione e protezione dai rischi adottate dal Datore di lavoro o dai Dirigenti ed i mezzi impiegati per attuarle non siano idonei a garantire la sicurezza e la salute durante il lavoro.

2.2 Controlli specifici

In relazione ai rischi connessi alla potenziale commissione dei reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, gli standard di controllo specifici sono enucleati nell'ambito delle aree che costituiscono i fattori qualificanti del Sistema di Salute e Sicurezza quali:

- la pianificazione;
- l'attuazione e il funzionamento;
- controllo e azioni correttive;
- attività di riesame.

2.2.1 Pianificazione

Per le attività di pianificazione del sistema di gestione della salute e sicurezza sono stabiliti i seguenti standard di controllo:

- esistenza di un documento formalizzato che definisca gli indirizzi e gli obiettivi generali in tema di salute e sicurezza che LOGIC stabilisce di raggiungere e che:
 - sia formalmente approvato dal Datore di lavoro;
 - contenga l'impegno al rispetto delle vigenti leggi in materia di salute e sicurezza applicabili;
 - preveda l'impegno alla prevenzione degli infortuni e delle malattie professionali e al miglioramento continuo della gestione e delle prestazioni del sistema di salute e sicurezza;

- sia adeguatamente diffuso ai dipendenti ed ai terzi eventualmente coinvolti;
- sia periodicamente riesaminato per assicurare che gli obiettivi in esso indicati siano idonei a mitigare i rischi presenti nell'organizzazione e allineati ai nuovi regolamenti e leggi.

2.2.2 Attuazione e funzionamento

Per le attività di attuazione e funzionamento del sistema di gestione della salute e sicurezza sul lavoro sono stabiliti i seguenti standard di controllo:

- esistenza di un sistema integrato di procedure in materia di sicurezza, igiene e salute sul lavoro. In particolare, tali procedure riportano anche le modalità di gestione, archiviazione e conservazione della documentazione prodotta;
- sussistenza di una disciplina aziendale che identifichi ruoli, responsabilità e modalità per lo svolgimento, approvazione ed aggiornamento della valutazione globale e documentata di tutti i rischi presenti nell'ambito dell'azienda.

In particolare tale disciplina: i) identifica ruoli, autorità, requisiti di competenza e necessità di addestramento del personale responsabile dell'identificazione dei pericoli, l'identificazione del rischio ed il controllo del rischio; ii) identifica modalità, tempistiche e criteri dei processi di identificazione dei pericoli e valutazione del rischio; iii) prevede, laddove necessario, la tracciabilità dell'avvenuto coinvolgimento del medico competente nel processo di identificazione dei pericoli e valutazione dei rischi; iv) prevede la valutazione delle diverse tipologie di sorgenti di rischio: pericoli ordinari o generici, ergonomici, specifici, di processo e organizzativi e una individuazione di aree omogenee in termini di pericolo all'interno dell'azienda; v) prevede l'individuazione delle mansioni rappresentative dei lavoratori; vi) prevede il censimento e la caratterizzazione degli agenti chimici e delle attrezzature e macchine presenti; vii) prevede esplicita definizione dei criteri di valutazione adottati per le diverse categorie di rischio nel rispetto della normativa e delle prescrizioni vigenti;

- attribuzione formale di ruoli, compiti e responsabilità organizzative e di controllo mediante:
 - individuazione della figura del Datore di lavoro (DDL), in relazione alla struttura organizzativa della Società e al settore di attività di produttiva;
 - nomina del Responsabile del Servizio Prevenzione e Protezione (RSPP) / Addetti del Servizio di Prevenzione e Protezione (ASPP) / Medico Competente / Incaricati delle Emergenze e del Pronto Soccorso;
 - individuazione dei compiti, delle responsabilità e dei poteri dei Dirigenti e dei Preposti laddove designati.

A tal fine è necessario che *i*) siano tracciabili le verifiche svolte in ordine al possesso dei requisiti specifici disposti dalla legge; *ii*) sia documentabile l'attività di verifica sul personale effettuata per comprenderne le capacità e le disponibilità temporali necessarie per ricoprire tali specifici ruoli; *iii*) sia comprovabile la formale accettazione dell'incarico;

- elaborazione del Documento di Valutazione dei Rischi (DVR) redatto secondo le disposizioni definite e contenente almeno: i) il procedimento di valutazione, con la specifica dei criteri adottati; ii) l'individuazione delle misure di prevenzione e di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione; iii) il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei

livelli di sicurezza;

- definizione di una normativa aziendale che provveda a determinare le modalità di qualifica dei fornitori e altri soggetti esterni con cui la Società entri in relazione. In relazione a ciò il Sistema Qualità che LOGIC già ha adottato e applicato potrà essere di valido supporto;
- inserimento nei contratti, se del caso, di clausole riguardanti anche i costi della sicurezza;
- regolamentazione delle modalità operative per l'affidamento di compiti e mansioni ai lavoratori. In particolare, è necessario prevedere: i) i criteri di affidamento delle mansioni ai lavoratori in base alle capacità e alle condizioni degli stessi in rapporto alla loro salute e alla sicurezza e a quanto emerso dai risultati degli accertamenti sanitari eseguiti; ii) le modalità di pianificazione delle visite periodiche; iii) le misure organizzative per la partecipazione del Medico Competente e del RSPP nella valutazione dell'idoneità dei lavoratori alle specifiche mansioni;
- adozione dei dispositivi di protezione individuale (DPI) adatti per le lavorazioni effettuate in ambito aziendale. In particolare, è necessario individuare DPI idonei a tutelare il lavoratore, definire le modalità per la verifica dei necessari requisiti quali resistenza, idoneità e mantenimento in buon stato di conservazione ed efficienza dei DPI, formalizzare le attività di gestione, distribuzione e mantenimento in efficienza dei DPI e prevedere la tracciabilità delle attività di consegna e verifica della funzionalità dei DPI;
- regolamentazione delle azioni da intraprendere per la gestione delle emergenze, atte a mitigare gli effetti sulla salute e sicurezza del Personale aziendale, di coloro che non appartengono alla Società e sull'ambiente esterno. E' necessario: i) individuare le misure per il controllo di situazioni di rischio in caso di emergenza; ii) definire e diffondere adeguatamente le modalità di abbandono del posto di lavoro o della zona pericolosa in cui persiste un pericolo grave e immediato; iii) definire le modalità di intervento dei lavoratori incaricati dell'attuazione delle misure di prevenzione incendi, di evacuazione dei lavoratori in caso di pericolo grave ed immediato e di pronto soccorso; iv) individuare i provvedimenti per evitare rischi per la salute del Personale e di coloro che, per qualsiasi motivo si trovino nelle aree aziendali e per evitare danni all'ambiente esterno; v) indicare le modalità e la tempistica/frequenza di svolgimento delle prove di emergenza;
- formalizzazione delle modalità operative per la gestione del rischio incendio. In particolare, è necessario: i) disciplinare il monitoraggio delle attività da svolgersi al fine della richiesta di rilascio e rinnovo (quando necessario) del Certificato di Prevenzione Incendi; ii) indicare le modalità di informazione ai lavoratori sulle norme di comportamento da attuarsi in caso di incendio; iii) indicare le modalità di tenuta ed aggiornamento del registro incendio;
- svolgimento di attività di consultazione e comunicazione mediante:
 - la definizione di un calendario che preveda riunioni periodiche di tutte le figure competenti per la verifica della corretta gestione delle tematiche riguardanti salute e sicurezza e l'adeguata diffusione delle risultanze delle riunioni all'interno dell'organizzazione;
 - tracciabilità delle riunioni periodiche e della diffusione delle risultanze delle

riunioni all'interno dell'organizzazione;

- raggiungimento di uno standard di comunicazione/informativa in tema di salute e sicurezza, tale da garantire a tutti i livelli aziendali conoscenze utili all'identificazione, riduzione e gestione dei rischi sul lavoro.
- svolgimento di attività di formazione e sensibilizzazione nel rispetto di una disciplina aziendale che regolamenti le modalità, tempi e criteri di erogazione della formazione e definisca l'ambito, i contenuti e le modalità della formazione, in considerazione del ruolo assunto all'interno della struttura organizzativa (Dirigenti, Preposti, RLS, ASPP). A tal proposito, è prevista:
 - l'elaborazione di un piano di formazione annuale e di un programma di formazione pluriennale.
 - adeguata informazione a Dirigenti e dipendenti circa l'adozione di eventuali procedure sulla sicurezza, mediante consegna di copia cartacea ovvero pubblicazione sulla intranet aziendale o attraverso modalità informativa analogia;
- effettuazione e regolamentazione delle verifiche periodiche di adeguatezza e di integrità degli asset aziendali e di conformità ai requisiti normativi applicabili.

2.2.3 Azioni correttive e di miglioramento

Per le attività di controllo e azioni correttive del sistema di gestione della salute e sicurezza del lavoratore è stabilito il seguente protocollo:

- programmazione ed esecuzione di attività di audit, con riferimento al rispetto delle procedure e delle istruzioni di lavoro impartite ai lavoratori, elaborando un sistema che preveda chiaramente ruoli e responsabilità, indicatori del sistema di sicurezza, prevenzione e protezione, tempistica per la programmazione delle attività e modalità di registrazione e gestione dei risultati degli audit. Al termine dell'attività di monitoraggio viene elaborato un verbale che attesti eventuali carenze e indichi le azioni correttive da intraprendere, nonché le modalità di comunicazione dei risultati dell'audit al Datore di Lavoro ed ai Dirigenti se delegati.

Inoltre è necessario prevedere: i) le competenze necessarie per il personale coinvolto nelle attività di audit, nel rispetto del principio dell'indipendenza dell'auditor rispetto all'attività che deve essere soggetta ad audit; ii) le modalità di individuazione e l'applicazione di azioni correttive nel caso siano rilevati scostamenti rispetto a quanto prescritto dal sistema di gestione della salute e sicurezza in azienda o dalla normativa; iii) le modalità di verifica dell'attuazione e dell'efficacia delle suddette azioni correttive;

- misura e monitoraggio delle prestazioni in relazione a
 - **infortuni:** con documentazione aziendale da cui risultino:
 - a) ruoli, responsabilità e modalità di rilevazione, registrazione, investigazione interna degli infortuni e delle malattie professionali;
 - b) ruoli, responsabilità e modalità di tracciabilità ed investigazione degli incidenti occorsi e dei "mancati incidenti";
 - c) modalità di comunicazione degli infortuni/incidenti occorsi da parte dei responsabili operativi al datore di lavoro e al responsabile del servizio di

prevenzione e protezione;

- **sorveglianza sanitaria, sicurezza degli impianti e delle macchine, utilizzo di sostanze chimiche pericolose:** con documentazione aziendale da cui risultino ruoli, responsabilità e modalità di registrazione e monitoraggio (anche attraverso l'uso di indicatori) per i dati riguardanti la sorveglianza sanitaria, la sicurezza degli impianti e delle macchine, l'utilizzo di sostanze e preparati pericolosi;
- **cause/controversie:** con documentazione aziendale da cui risultino ruoli, responsabilità e il monitoraggio delle controversie/contenziosi pendenti relativi agli infortuni occorsi sui luoghi di lavoro, al fine di identificare le aree a maggior rischio infortuni.

2.2.4 Attività di riesame dell'Alta Direzione

Per le attività di riesame da parte del Datore di lavoro, ovvero dei soggetti delegati alla gestione del sistema di controllo e prevenzione della salute e sicurezza, è prevista una documentazione da cui risultino ruoli, responsabilità e modalità di conduzione del processo di riesame sull'efficacia e l'efficienza del sistema di gestione della salute e sicurezza in azienda.

Tale documentazione assicura la tracciabilità dello svolgimento delle seguenti attività: i) analisi degli eventuali scostamenti tra i risultati ottenuti e gli obiettivi programmati; ii) analisi dei risultati degli audit; iii) analisi dei risultati sul monitoraggio della performance del sistema di gestione della salute e sicurezza (infortuni, altri dati); iv) stato di avanzamento di eventuali azioni di miglioramento definite nel precedente riesame; v) individuazione degli obiettivi di miglioramento per il periodo successivo e della necessità di eventuali modifiche ad elementi del sistema di gestione della salute e sicurezza.

Il verbale del riesame della Direzione viene inviato, annualmente, all'OdV.

2.3 Tracciabilità delle transazioni

Al fine di garantire un'adeguata tracciabilità delle azioni riguardanti il sistema di controllo e prevenzione in materia di salute e sicurezza sul lavoro e di consentire l'esecuzione di verifiche sulla solidità dello stesso e sul rispetto delle relative disposizioni normative ed aziendali, è fatto obbligo che tutti i soggetti coinvolti provvedano alla corretta archiviazione, su supporto cartaceo o informatico, della documentazione inerente alla gestione della sicurezza quale le cartelle sanitarie, il registro infortuni, il documento di valutazione dei rischi, la gestione delle controversie in materia di salute e sicurezza.

2.4 Segregazione dei compiti

In riferimento ai reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, per garantire l'applicazione del principio di separazione dei ruoli (uno dei principi cui si devono conformare i Modelli 231), è previsto che alcune specifiche attività siano organizzate al fine di prevedere la segregazione delle responsabilità tra chi autorizza, chi esegue e chi controlla le seguenti attività:

- pianificazione del sistema di controllo e prevenzione della salute e sicurezza sul lavoro;
- attuazione e funzionamento del sistema di controllo e prevenzione della salute e sicurezza

sul lavoro;

- controllo e azioni correttive;
- attività di riesame.

2.5 Sistema di procure/deleghe coerente con responsabilità, ruoli e compiti

Al fine di garantire che i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative e gestionali assegnate, nonché chiaramente definiti e conosciuti all'interno dell'organizzazione, è previsto un sistema di procure che attribuiscono poteri e deleghe in modo coerente con le mansioni ricoperte ed in linea con le attività effettivamente svolte.

Per quanto attiene al sistema di deleghe, oltre ad evidenziare che esso è dettagliatamente disciplinato dall'art. 16 del Testo Unico 81/2008, si sottolinea che:

- i delegati devono possedere tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;
- la delega deve attribuire tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate, nonché un'autonomia di spesa necessaria allo svolgimento delle predette funzioni;
- alla delega di funzioni deve essere data adeguata e tempestiva pubblicità;
- la delega deve risultare da atto scritto recante data certa e deve essere accettata dal delegato per iscritto. Il soggetto delegato può, a sua volta, delegare specifiche funzioni in materia purché ciò sia previsto, nei termini e modalità, dalla stessa delega del DDL. Il soggetto al quale viene conferita tale delega non può, a propria volta, delegare le funzioni delegategli;
- le deleghe di funzioni non escludono l'obbligo di vigilanza in capo al soggetto delegante.

Infine, si evidenzia che la previsione dell'art. 30 del TU 81, con la quale il legislatore fa interagire il sistema della tutela della salute e della sicurezza sui luoghi di lavoro con quello previsto per la prevenzione dei reati (Decreto 231) prevede proprio l'adozione di un sistema integrato di controllo interno alla Società nel quale siano presenti sia i presidi di prevenzione previsti dal suddetto Decreto 231 sia quelli disciplinati dal TU 81.

SEZIONE "H"
Art. 25 undecies del Decreto 231
Reati ambientali

L'art. 25 undecies del Decreto prevede, quali reati presupposto della responsabilità dell'Ente, alcuni reati ambientali. In relazione all'attività svolta dalla Società ed ai rischi ad essa connessi sono state ritenute potenzialmente rilevanti per la Società le seguenti fattispecie di reato:

- **Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art.258 D.Lgs. 152/06, TU Ambiente):** è punita la mancata adesione a SISTRI da parte di imprese di raccolta e trasporto rifiuti e che effettuano il trasporto senza compilare il formulario, oltre a prevedere la sanzione penale per chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto.
- **Attività di gestione di rifiuti non autorizzata (art.256 TU):** è punito chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione.
- **Discarica non autorizzata (art.256 TU):** è punito chiunque realizza o gestisce una discarica non autorizzata.
- **Traffico illecito di rifiuti (art.259 D.Lgs. 152/06):** l'illecito penale è commesso da chi effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 2 del regolamento (CEE) 1° febbraio 1993, n. 259, o effettua una spedizione di rifiuti elencati nell'Allegato II dello stesso regolamento.
- **Sistema informatico di controllo della tracciabilità dei rifiuti – SISTRI (art.260 bis, TU):** l'illecito penale si realizza quando sono integrate condotte finalizzate a: fornire false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico- fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti ovvero inserire un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti; usare un certificato falso durante il trasporto; usare una copia cartacea della scheda SISTRI - AREA Movimentazione fraudolentemente alterata durante il trasporto.
- **Superamento valori limite di emissione e di qualità dell'aria (art.279 TU):** il reato consiste nella condotta di chi, nell'esercizio di uno stabilimento, viola i valori limite di emissione o le prescrizioni stabilite dall'autorizzazione, dalla normativa vigente, dai piani e dai programmi o imposte dall'autorità competente.
- **Violazioni in tema di impiego di sostanze lesive dell'ozono e dell'ambiente (art. 3 l. 549/93):** il reato si concretizza quando sono integrate condotte finalizzate a violare quanto disposto dai Ministeri competenti in materia di sostanze lesive per l'ozono e per l'ambiente o a produrre, utilizzare, commercializzare, importare ed esportare sostanze di cui alle tabelle A e B allegate alla legge 549/1993.
- **Scarichi sul suolo (art.103, TU):** è punito chiunque effettui scarichi sul suolo al di fuori di un elenco di ipotesi in cui gli stessi, a determinate condizioni, sono consentiti.
- **Scarichi nel sottosuolo e nelle acque sotterranee (art.104, TU):** l'illecito penale si realizza quando viene scaricato direttamente nelle acque sotterranee e nel sottosuolo senza la necessaria autorizzazione dell'autorità competente o in violazione delle prescrizioni della stessa.
- **Scarichi di sostanze pericolose in reti fognarie (artt.107, 108, 137 TU):** viene sanzionato

chiunque scarichi sostanze pericolose oltre i limiti di quantità massima prescritti dalle necessarie autorizzazioni previste dagli artt. 107 e 108 del decreto.

- **Scarichi di acque reflue industriali contenenti sostanze pericolose (art.137 TU):** commette reato chi effettua scarichi di acque reflue industriali senza autorizzazione o dopo che l'autorizzazione sia stata sospesa o revocata, sono previste pene più afflittive in caso di acque reflue industriali contenenti sostanze pericolose.
- **Scarichi di acque reflue industriali contenenti sostanze pericolose oltre i valori limite (art.137 TU):** è punito chiunque, nell'effettuazione di uno scarico di acque reflue industriali o di scarico sul suolo, superi i valori limite fissati dalla normativa o dall'autorità competente, con aggravati di pena connessi alle sostanze pericolose contenute negli scarichi.
- **Divieto di miscelazione di rifiuti pericolosi (art.187 TU):** è reato laddove siano miscelati rifiuti pericolosi aventi differenti caratteristiche di pericolosità ovvero rifiuti pericolosi con rifiuti non pericolosi nonché in caso di diluizione di sostanze pericolose in assenza della prescritta autorizzazione o comunque in assenza di specifiche condizioni previste dalla norma. A questi fini la miscelazione va definita come l'operazione consistente nella mescolanza, volontaria o involontaria, di due o più tipi di rifiuti aventi codici identificativi diversi, in modo da dare origine ad una miscela per la quale non esiste uno specifico codice identificativo.
- **Bonifica dei siti (art.257 TU):** è punito chi, avendo cagionato l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio, non provveda alla bonifica in conformità al progetto approvato dall'autorità competente.
- Inoltre, si evidenzia che:
 - **l'art. 192, comma 4, del TU Ambiente (divieto di abbandono di rifiuti)** prevede una responsabilità solidale della persona giuridica (in questo caso la LOGIC) quando la responsabilità sia da addebitare ai suoi amministratori o ai suoi rappresentanti;
 - **l'art. 256 bis dello stesso TU (combustione illecita di rifiuti)** prevede per le Società anche sanzioni interdittive ai sensi del Decreto 231.

In considerazione delle attività aziendali svolte da LOGIC e della struttura interna adottata, importante è il conseguimento della certificazione UNI EN ISO 14001:2015 ottenuta nel 2017.

Le procedure di certificazione rappresentano un determinante supporto al sistema di prevenzione dei reati 231 in materia ambientale sempreché siano sempre osservati i principi di comportamento del Codice Etico, i protocolli e le procedure del presente Modello di organizzazione, gestione e controllo affinché sia assicurata l'implementazione del sistema integrato di controllo della Società con i presidi di prevenzione alla commissione dei reati ambientali.

In relazione alla gestione dei rifiuti le deleghe di funzioni devono essere giustificate in base alle dimensioni di LOGIC e/o alle sue esigenze organizzative.

Per attribuirsi rilevanza penale all'istituto della delega di funzioni in materia ambientale (per la quale non è prevista la delega così come è invece regolata in materia di salute e sicurezza sui luoghi di lavoro all'art. 16 del TU 81) è necessaria la compresenza di alcuni requisiti:

- a. la delega deve essere puntuale ed espressa;
- b. il delegato, e l'eventuale subdelegato, devono essere tecnicamente idonei e

- professionalmente qualificati per lo svolgimento dei compiti loro affidati;
- c. il trasferimento delle funzioni delegate deve essere giustificato in base alle dimensioni dell'impresa o, quantomeno, alle esigenze organizzative della stessa;
 - d. la delega deve riguardare non solo le funzioni ma anche i correlativi poteri decisionali e di spesa;
 - e. l'esistenza della delega, una volta accettata formalmente, deve essere provata in modo certo. L'esistenza deve riguardare non solo le funzioni ma anche i poteri.

Circa la rilevanza delle deleghe di funzione nel sistema "231" può soccorrere la sentenza della Cassazione n. 9132 del 24 febbraio 2017: in caso di responsabilità da reati ambientali, nell'apprezzamento del modello organizzativo dell'ente e nella valutazione della sua idoneità, il primo elemento da considerare è la predisposizione di un adeguato sistema di deleghe: l'assenza di deleghe di funzioni è fatto che di per sé prova la mancanza di un efficace modello organizzativo adeguato a prevenire la consumazione del reato da parte dei vertici societari.

Le principali attività sensibili e i processi strumentali a rischio di commissione dei reati in oggetto sono i seguenti:

- gestione di attività e processi rilevanti ai fini ambientali anche in rapporto con terze parti;
- gestione flussi documentali relativi al processo di raccolta e trattamento dei rifiuti;
- gestione dei rapporti con interlocutori terzi - pubblici o privati - nello svolgimento delle proprie attività lavorative per conto e/o nell'interesse della Società - monitoraggio delle attività esternalizzate;
- gestione del servizio raccolta e conferimento rifiuti alle imprese autorizzate;
- gestione degli adempimenti relativi ai rapporti con la Pubblica Amministrazione;

Si evidenzia che i rischi di carattere ambientale sono presidiati anche:

- dalle verifiche della qualità e relativa certificazione UNI EN ISO 14001:2015, ottenuta nel 2017;
- controlli da parte del Responsabile ambientale coadiuvato dai suoi eventuali delegati.

1 Principi di comportamento

La Società è impegnata nell'attuazione di un valido sistema di gestione ambientale, nella prospettiva di un miglioramento continuo dello stesso, secondo un approccio operativo e gestionale, che prenda in considerazione gli elementi necessari, di seguito sintetizzati, ad una gestione strutturata delle tematiche ambientali con la:

- definizione di una struttura organizzativa, responsabile di gestire e monitorare, a livello aziendale, il complessivo sistema di gestione ambientale, identificare gli scostamenti rispetto agli obiettivi e le attività pianificate, nonché supervisionare l'efficacia, l'efficienza e il mantenimento nel tempo del sistema di procedure e regolamenti posti in essere in materia ambientale;
- definizione di specifiche disposizioni organizzative e di un sistema di *job description*, adeguando il sistema di deleghe e procure, al fine di specificare le figure professionali

- preposte alla gestione delle attività di natura ambientale e le rispettive responsabilità assegnate, ivi incluse le modalità di coordinamento tra i soggetti deputati al controllo;
- previsione nell'ambito dei contratti con fornitori esterni che svolgono attività con impatto ambientale di specifiche clausole contrattuali che impegnino il fornitore al rispetto di tutte le norme ambientali nello svolgimento delle proprie attività;
 - analisi e valutazione degli aspetti e degli impatti ambientali, con riferimento all'analisi dei rischi ambientali e all'identificazione delle misure di prevenzione, protezione e mitigazione connesse;
 - definizione delle modalità operative per la gestione e il mantenimento in efficienza delle misure di prevenzione, protezione e mitigazione ambientali;
 - definizione delle modalità operative per la gestione delle emergenze in materia ambientale;
 - gestione e monitoraggio degli adempimenti normativi ambientali relativi a fornitori di attività che hanno impatto in materia ambientale;
 - definizione delle modalità operative per la misura, la sorveglianza e il monitoraggio delle prestazioni in materia ambientale e degli incidenti ambientali intervenuti;
 - pianificazione, gestione e consuntivazione degli impegni di spesa in materia ambientale (scadenze, risorse, rendicontazione e tracciabilità delle spese);
 - gestione dell'aggiornamento delle informazioni riguardo alla legislazione rilevante e alle altre prescrizioni applicabili in materia di ambiente;
 - consultazione, comunicazione e formazione in merito alle tematiche ambientali;
 - definizione delle modalità di gestione, archiviazione e tracciabilità della documentazione del sistema di controllo in merito alle tematiche ambientali;
 - definizione delle modalità operative per la gestione degli audit e del relativo reporting sulle tematiche ambientali;
 - esecuzione di specifici audit in materia ambientale;
 - conduzione del processo di riesame da parte dell'Amministratore Delegato in relazione all'efficacia e all'efficienza del sistema di controllo in materia di ambiente.

I seguenti principi di comportamento si applicano ai destinatari del presente Modello che, a qualunque titolo, siano/saranno coinvolti nelle attività sensibili rispetto alla commissione dei reati ambientali, per conto o nell'interesse della Società.

A tutti i Destinatari del Codice Etico e del Modello è richiesto di:

- osservare rigorosamente tutte le norme poste dalla legge e dai regolamenti interni a tutela dell'ambiente e tenere un comportamento corretto, trasparente e collaborativo ad esse conforme;
- assicurare il regolare funzionamento della Società e degli Organi sociali, garantendo ed agevolando ogni forma di controllo interno sulle attività societarie che possa essere strumentale alla salvaguardia di comportamenti o condotte non conformi ai principi normativi di cui all'art. 25-undecies del Decreto 231 che individua il titolo della presente sezione della parte speciale;

- tenere condotte volte a minimizzare qualsiasi rischio di inquinamento ambientale, evitando qualsiasi azione che, anche solo potenzialmente, possa comportare il rischio di cagionare compromissioni o deterioramenti delle acque, dell'aria, di porzioni del suolo o del sottosuolo, di ecosistemi, della biodiversità, della flora o della fauna, ovvero l'alterazione irreversibile dell'equilibrio di un ecosistema, l'alterazione dell'equilibrio di un ecosistema la cui eliminazione risulti particolarmente onerosa o l'offesa alla pubblica incolumità;
- astenersi dal porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie previste nell'ambito dei reati ambientali (art. 25-undecies del Decreto 231).

Per quanto riguarda gli scarichi idrici, è previsto il divieto di attivare o effettuare:

- nuovi scarichi di acque reflue industriali contenenti le sostanze pericolose normativamente individuate dalle tabelle 3, 3A, 4 e 5 di cui all'Allegato 5, parte terza del Testo Unico Ambiente e successive modificazioni, in assenza di autorizzazione ovvero qualora la stessa sia sospesa o revocata ovvero in violazione delle prescrizioni presenti nell'autorizzazione, o delle altre prescrizioni delle Autorità competenti;
- scarichi di acque reflue industriali contenenti le sostanze pericolose di cui sopra con superamento dei limiti normativamente individuati dal suddetto TU ovvero dei limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente;
- gli scarichi di acque nel suolo, sottosuolo e acque sotterranee al di fuori dei casi normativamente previsti.

Per la bonifica, è previsto il divieto di omettere:

- gli interventi di bonifica ovvero violare le disposizioni inerenti al progetto di bonifica approvato dall'autorità competente nel caso di eventi inquinanti del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio, in violazione di quanto previsto dall'articolo 242 del TU;
- la comunicazione dell'evento inquinante alle Autorità competenti, ai sensi della norma di cui al punto precedente.

In relazione alla gestione delle emissioni atmosferiche, è previsto il divieto di:

- compiere/omettere azioni o interventi che possano determinare il superamento dei valori limite di qualità dell'aria mediante la violazione dei valori di emissione stabiliti dall'autorizzazione o imposte dall'Autorità competente, ovvero i valori normativamente individuati;
- violare le disposizioni previste dalla normativa sulla tutela dell'ozono in caso di produzione, consumo, importazione, esportazione, detenzione e commercializzazione delle sostanze considerate lesive ai sensi del Reg. CEE 3093/94.

Circa la gestione dei rifiuti, è previsto il divieto di:

- effettuare attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione ovvero in violazione di alcuni dei requisiti normativamente previsti per lo svolgimento di dette attività;
- effettuare attività non autorizzata di miscelazione dei rifiuti o di discarica di rifiuti;

- predisporre ovvero utilizzare per il trasporto un certificato di analisi dei rifiuti fornendo false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti, ovvero inserire un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti, ovvero utilizzare una copia cartacea della scheda SISTRI fraudolentemente alterata;
- ricevere ovvero effettuare spedizioni di rifiuti da e verso uno o più paesi dell'area comunitaria, in mancanza della notifica alle Autorità competenti, ovvero della autorizzazione delle stesse, ovvero in caso di autorizzazioni ottenute fraudolentemente e in tutti gli altri casi costituenti traffico illecito;
- predisporre un certificato di analisi dei rifiuti fornendo false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti ovvero inserire un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti;
- immettere nel suolo o sottosuolo sostanze che possano compromettere o deteriorare l'equilibrio ambientale o che ne possano comportare l'alterazione irreversibile.

In caso di dubbi circa la corretta attuazione dei principi etico - comportamentali di cui sopra nel corso dello svolgimento delle attività aziendali, è fatto obbligo al soggetto interessato di interpellare il proprio Responsabile (in caso di dipendente della Società) o referente interno (in caso di soggetti terzi) informandone l'Organismo di Vigilanza.

È fatto obbligo ai soggetti coinvolti di comunicare immediatamente all'Organismo di Vigilanza l'impossibilità di attuare gli obblighi previsti indicandone la motivazione e ogni anomalia significativa riscontrata, nonché ogni evento suscettibile di incidere sull'operatività ed efficacia dell'attività (come per esempio, le modifiche legislative e regolamentari, circostanze non regolamentate, mutamenti nell'attività lavorativa, modifica della struttura aziendale).

È obbligatorio in tutti i casi di:

- violazioni presunte o effettive delle prescrizioni normative ovvero di quelle di cui al presente paragrafo;
- verifiche e ispezioni da parte delle Autorità competenti, anche per quelle che terminano senza rilievi a carico della Società;
- apertura e chiusura di procedimenti sia penali che amministrativi,

venga data immediata e tempestiva comunicazione all'Organismo di Vigilanza.

Per quanto riguarda le ispezioni delle Autorità Pubbliche l'informazione all'OdV sarà inviata entro lo stesso giorno di inizio dell'attività ispettiva.

Allo stesso OdV sarà trasmesso, annualmente, il verbale del riesame della Direzione.

LOGIC, inoltre, al fine di evitare il proprio coinvolgimento in attività suscettibili di concretizzare uno o più reati ambientali, si impegna a svolgere responsabilmente la propria attività secondo modalità che garantiscano il rispetto dell'ambiente ed in particolare a:

- raccogliere e valutare dati relativi ad eventuali incidenti derivanti dalla gestione delle diverse attività e processi che abbiano avuto o possano avere impatti sull'ambiente;
- pianificare eventuali azioni volte a migliorare le performance di processo, indicando modalità, tempi e soggetti coinvolti;
- attuare idonea politica di formazione ed informazione nei confronti del personale dipendente a vario titolo coinvolto nelle attività rilevanti;

- garantire una condotta trasparente nei confronti della Pubblica Amministrazione per quanto attiene alla gestione degli adempimenti di natura tecnico-normativa relativamente all'ottenimento di autorizzazioni, licenze, concessioni o permessi ovvero alla gestione di verifiche e ispezioni inerenti attività e processi di natura ambientale. Quindi la Società adotta processi e sviluppa attività di controllo volte a:
 - assicurare che tutte le informazioni trasmesse agli Enti di riferimento in forma verbale, scritta o attraverso l'uso di sistemi info-telematici siano predisposte nel rispetto della specifica normativa che regola l'attività sottostante e siano complete, veritiere e corrette nonché ricostruibili, in termini di tracciabilità dei flussi informativi e dei dati che le hanno generate;
 - evitare di omettere indicazioni o informazioni che, se taciute, potrebbero ingenerare nella controparte pubblica erronee rappresentazioni o decisioni inopportune;
 - non esibire documenti e dati falsi o alterati;
- evitare condotte ingannevoli che possano indurre la Pubblica Amministrazione in errore di valutazione tecnico-amministrativa sulle autorizzazioni, licenze, concessioni o permessi richiesti ovvero che possano impattare sull'esito di eventuali ispezioni e verifiche svolte da parte delle Autorità competenti;
- rispettare quanto stabilito dalla normativa vigente per le emissioni in atmosfera con riferimento ai punti di emissione degli impianti e alle emissioni convogliabili, in base alle migliori tecniche disponibili;
- evitare di impiegare nella produzione nonché di consumare, importare, esportare, detenere e commercializzare sostanze considerate come lesive dell'ozono dalla normativa vigenti;
- assicurare che tutti i dati riportati all'interno dei registri di carico e scarico dei rifiuti, formulari, schede di movimentazione SISTRI, certificati di analisi rifiuti siano completi, corretti e veritieri; garantire, anche tramite le associazioni imprenditoriali interessate o società di servizi di diretta emanazione delle stesse, la corretta tenuta - anche in termini di numerazione e vidimazione, e la corretta archiviazione del registro di carico e scarico, riportante tutte le informazioni sulle caratteristiche qualitative e quantitative dei rifiuti;
- garantire la corretta tenuta - anche in termini di numerazione e vidimazione, e la corretta archiviazione dei formulari relativi al trasporto dei rifiuti ovvero della copia della scheda del sistema di controllo della tracciabilità dei rifiuti (SISTRI);

Infine, nei confronti di terze parti contraenti (come i collaboratori esterni, consulenti, partner, fornitori, clienti), identificate anche in funzione di specifici criteri di importo e significatività della fornitura, coinvolte nello svolgimento di attività a rischio rispetto ai reati ambientali e che operano per conto o nell'interesse della Società, i relativi contratti, secondo precisi criteri di selezione stabiliti nel presente Modello, devono:

- essere definiti per iscritto, in tutte le loro condizioni e termini;
- comprendere le clausole relative al Decreto "231".

2 Controlli

In relazione ai rischi connessi alla potenziale commissione di reati ambientali, i principi del sistema di controllo devono evidenziare:

2.1 *Attribuzione delle responsabilità*

Definizione dei compiti, dei ruoli e delle responsabilità così come statuiti dall'organigramma aziendale, dal sistema autorizzativo, dagli ordini di servizio, dalle procedure e da ulteriori documenti organizzativi che regolamentano:

- la gestione delle attività che generano scarichi idrici industriali;
- la gestione delle attività che generano emissioni in atmosfera;
- la gestione delle attività che possono dare luogo a bonifiche, ovvero all'identificazione degli eventi che potenzialmente possano contaminare il suolo, il sottosuolo, le acque superficiali e/o le acque sotterranee;
- la gestione delle attività aziendali connesse alla raccolta, al trasporto, al recupero e allo smaltimento dei rifiuti;
- la gestione degli adempimenti connessi al SISTRI.

2.2 *Protocolli specifici*

Ottenimento, modifica e/o rinnovo delle autorizzazioni, è previsto di:

- identificare la necessità di richiesta di una nuova autorizzazione o di modifica di autorizzazioni preesistenti;
- predisporre l'idonea documentazione prevista dall'iter autorizzativo e alla formalizzazione delle attività necessarie;
- comunicare l'avvenuto ottenimento dell'autorizzazione, la sua modifica e/o il rinnovo al Responsabile Ambientale;
- tracciare l'iter autorizzativo dalla raccolta dei dati, fino alla comunicazione dell'esito dello stesso.

Gestione delle emissioni atmosferiche, è previsto di:

- identificare e aggiornare i punti di emissione e i punti di campionamento;
- definire il programma dei campionamenti e delle analisi delle emissioni, in linea con quanto previsto dalle prescrizioni autorizzative e dalla normativa vigente;
- monitorare i dati riguardanti le emissioni, ivi compresi i certificati analitici delle analisi e i campionamenti effettuati;
- implementare sistemi manuali e automatizzati di controllo e di monitoraggio continuo delle emissioni in atmosfera, in modo da garantire che non vengano superati i limiti normativamente individuati ovvero gli eventuali limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente al

momento del rilascio delle autorizzazioni;

- intervenire in caso di valori anomali rilevati dalle determinazioni analitiche effettuate sui punti di emissione.

Esistenza di un sistema di poteri coerente con le responsabilità organizzative individualmente assegnate.

In riferimento ai reati ambientali, al fine di garantire che i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative e gestionali, chiaramente definiti e conosciuti all'interno dell'organizzazione, è previsto che il sistema delle procure/deleghe attribuiscono poteri per impegnare la Società anche verso l'esterno, in modo coerente con le mansioni ricoperte ed in linea con le attività effettivamente svolte.