



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 1 di 70
Edizione 03 – Settembre 2022
Emittente: C.d.A.

Biscotti P. Gentilini S.r.l.



Gentilini
dal 1890

**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
ai sensi del D. Lgs. 231/2001**

ESTRATTO

Roma (RM), 05 settembre 2022

INDICE

1	<i>I RIFERIMENTI NORMATIVI FONDAMENTALI</i>	6
1.1	Il Decreto Legislativo 231 del 8 giugno 2001	6
1.1.1	Inquadramento del problema	6
1.1.2	I soggetti ed i reati presupposto	8
1.2	Il Decreto Legislativo 81 del 9 aprile 2008	15
1.3	Ulteriori fonti	16
2	<i>LE LINEE GUIDA PER LA REDAZIONE DEL MODELLO</i>	17
3	<i>IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO: SCOPO E CONTENUTO</i>	17
4	<i>IL PROFILO DELLA SOCIETÀ</i>	18
4.1	La storia	18
4.2	La sede aziendale	19
4.3	I prodotti.....	20
4.4	La filiera	21
5	<i>IL SISTEMA DI CORPORATE GOVERNANCE DELLA SOCIETÀ</i>	21
5.1	L'Assemblea dei Soci	22
5.2	Il Consiglio di Amministrazione e il suo Presidente	22
5.3	Il Collegio sindacale	23
5.4	Individuazione dei soggetti in posizione apicale	23
5.4.1	Poteri del Consigliere Delegato	23
5.4.2	Poteri del Consiglio di Amministrazione	24
6	<i>I SISTEMI MANAGERIALI RILEVANTI</i>	25
6.1	Politiche societarie	25
6.2	Il sistema organizzativo	25
6.3	I sistemi di gestione	26
6.4	Il sistema di gestione delle risorse umane	27
6.5	Il sistema informativo	27
6.6	Il sistema dei controlli	28
6.6.1	Principi, requisiti e livelli di controllo	28
6.6.2	Il Controllo sulla gestione economico-finanziaria ed il Controllo Contabile	30
6.7	Il sistema di controllo della salute e sicurezza dei lavoratori	30
6.7.1	Principi e requisiti	30
6.7.2	Organizzazione e ruoli del Servizio Prevenzione e Protezione	31
6.7.2.1	Nomina del Datore di lavoro	32
6.7.2.2	Nomina del Responsabile del Servizio Prevenzione e Protezione	32
6.7.2.3	Nomina dei Dirigenti (del Servizio Prevenzione e Protezione)	32
6.7.3	Monitoraggio	33
7	<i>I PROTOCOLLI</i>	34
7.1	Premessa	34



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 3 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

7.2	Il Protocollo SSL.....	34
7.2.1	Attività di valutazione dei rischi e predisposizione delle misure di prevenzione e protezione	34
7.2.2	Standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, movimentazioni carichi, etc.	35
7.2.3	Gestione delle emergenze.....	36
7.2.4	Aspetti organizzativi (deleghe, nomine di RSPP, RLS, budget e spese)	36
7.2.5	Sorveglianza sanitaria.....	37
7.2.6	Informazione e formazione dei lavoratori	37
7.2.7	Attività di vigilanza e controllo	38
7.2.8	Sistema sanzionatorio	38
7.3	Protocollo per la gestione della contabilità e la formazione del bilancio	39
7.3.1	Livelli autorizzativi definiti e separazione delle funzioni	40
7.3.2	Controllo e monitoraggio specifico	40
7.3.3	Tracciabilità delle operazioni e archiviazione.....	40
7.3.4	Criteri di comportamento	41
7.4	Protocolli in materia di delitti informatici	42
7.4.1	Delitti informatici	42
7.4.2	Potenziale profilo di rischio rispetto al D. Lgs. 231/2001.....	44
7.4.3	Principi deontologici e indicazioni comportamentali di riferimento.....	44
7.5	Protocolli di gestione e controllo	45
7.5.1	Premessa	45
7.5.2	I reati ex art. 24 bis del D. Lgs. 231/2001 – Protocolli comportamentali	46
7.6	La gestione della filiera alimentare	50
7.7	Polices e procedure a presidio dei rischi-reato	50
8	L'ADOZIONE E LA GESTIONE DEL MODELLO.....	52
8.1	Adozione e aggiornamento del Modello	52
8.2	Comunicazione e formazione	53
8.2.1	Comunicazione	53
8.2.2	Formazione.....	53
9	L'ORGANISMO DI VIGILANZA E CONTROLLO	54
9.1	Requisiti e caratteristiche dell'Organismo di Vigilanza	54
9.2	Funzioni, poteri e attività di controllo dell'Organismo di Vigilanza	56
9.2.1	Funzioni e poteri dell'Organismo di Vigilanza	56
9.2.2	Attività di controllo dell'Organismo di Vigilanza	57
9.3	Informativa	57
9.3.1	Informativa all'Organismo di Vigilanza.....	57
9.3.2	Le segnalazioni verso l'Organismo di Vigilanza (whistleblowing)	59
9.3.3	Modalità di trasmissione e valutazione dei flussi informativi e delle segnalazioni.....	59
9.3.4	Obblighi e requisiti del sistema di segnalazione (whistleblowing).....	60
9.3.5	Disciplina del segreto	61
9.3.6	Libri dell'Organismo di Vigilanza	61
9.3.7	Registrazione delle segnalazioni	62
9.3.8	Obblighi di informazione da parte dell'Organismo di Vigilanza	62
10	IL SISTEMA SANZIONATORIO.....	63
10.1	Caratteristiche del sistema sanzionatorio	63
10.2	Criteri di graduazione delle sanzioni.....	63



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 4 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

10.3	Misure nei confronti dei lavoratori dipendenti	64
10.4	Misure nei confronti dei dirigenti.....	66
10.5	Misure nei confronti degli Amministratori e dei componenti l'Organo di controllo.....	66
10.6	Misure nei confronti dei collaboratori esterni.....	67
10.7	Misure nei confronti dei fornitori, partner e consulenti	67
10.8	Rivalsa per risarcimento danni	67
10.9	L'irrogazione delle sanzioni	68
10.9.1	Premessa	68
10.9.2	Lavoratori Dipendenti	68
10.9.3	Dirigenti.....	69
10.9.4	Amministratori e componenti l'Organo di controllo.....	69
10.9.5	Collaboratori esterni	69
10.9.6	Fornitori, partner e consulenti	70
10.10	Conoscibilità	70



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 5 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

Biscotti P. Gentilini S.r.l.



Gentilini
— *dal 1890* —

**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
ai sensi del D. Lgs. 231/2001**

PARTE GENERALE

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 6 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

1 I RIFERIMENTI NORMATIVI FONDAMENTALI

1.1 Il Decreto Legislativo 231 del 8 giugno 2001

1.1.1 Inquadramento del problema

Il Decreto legislativo 8 giugno 2001 n. 231 (in seguito "D. Lgs. 231" o "Decreto") ha introdotto la responsabilità amministrativa "penale" degli enti, i quali possono essere ritenuti responsabili, e di conseguenza sanzionati con pene patrimoniali e interdittive, in relazione a taluni reati commessi o tentati nell'interesse o a vantaggio degli enti stessi da parte degli amministratori, degli altri soggetti apicali o dei dipendenti.

Gli enti possono adottare Modelli di organizzazione, gestione e controllo (di seguito, anche "Modelli") idonei a prevenire i reati stessi.

I reati attualmente più rilevanti, al fine di configurare la responsabilità "penale" degli enti, possono essere ricompresi nelle seguenti categorie:

- delitti contro la Pubblica Amministrazione,
- reati societari,
- reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Gli autori dei reati commessi nell'interesse o a vantaggio dell'ente possono essere sia i soggetti in posizione apicale sia i soggetti sottoposti all'altrui direzione e vigilanza. Si ricorda che ai fini del predetto D. Lgs. 231/2001 si considera soggetto in posizione apicale colui che riveste funzioni di rappresentanza dell'ente (ad esempio il Presidente della Società), di amministrazione o direzione dell'ente (ad esempio gli Amministratori ed i Direttori Generali) ovvero di una sua unità organizzativa dotata di autonomia finanziaria e funzionale (ad esempio institori), nonché coloro che esercitano, anche di fatto, la gestione e il controllo dello stesso.

L'accertamento della responsabilità dell'ente è attribuito al giudice penale mediante :

- la verifica della sussistenza del reato,
- e
- il sindacato di idoneità sul modello organizzativo adottato.

Il Modello è un complesso di principi, regole, protocolli, disposizioni, schemi organizzativi (a partire da organigramma e connessi compiti e responsabilità) funzionale alla prevenzione dei reati previsti dal D. Lgs. 231/2001. Allegate allo stesso, e che quindi ne fanno parte integrante e necessaria, sono le clausole contrattuali.

L'ente si è inoltre dotato di un Codice Etico che prevede le relative sanzioni in caso di violazione.

Il Modello della Biscotti P. Gentilini Srl (di seguito la "Società") è emanazione del Consiglio di Amministrazione, che provvede ad approvarlo così come il Codice Etico.

Essendo il Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6, comma 1, lettera a, del Decreto), le successive modifiche ed integrazioni del Modello, effettuate su indicazione dell'Organismo di Vigilanza (di cui di seguito, indicato anche come O.d.V.) - eventualmente con un supporto esterno - sono rimesse alla competenza del Consiglio di Amministrazione che dovrà procedere alla adozione della versione modificata dello stesso.

Premesso che la modifica del Modello può essere sostanziale o non sostanziale, nei due casi l'approvazione della versione modificata deve avvenire:



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 7 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

- in caso di modifica sostanziale, nel corso della prima riunione utile;
- in caso di modifica non sostanziale, entro sei mesi dall'effettuazione della stessa.

Si considerano modifiche sostanziali del Modello:

- l'introduzione di nuove fattispecie di reato che possono determinare la responsabilità dell'ente ai sensi del Decreto e il conseguente aggiornamento del Modello;
- l'aggiornamento del Sistema di Governance, incluse le modifiche al sistema di deleghe ritenute significative dall'Organismo di Vigilanza;
- l'introduzione di nuovi Sistemi di certificazione;
- la revisione estesa-complessiva della Mappa dei rischi e le relative modifiche al Modello,

nonché ogni altra modifica giudicata sostanziale dall'Organismo di Vigilanza.

Tra le modifiche sostanziali, va annoverato inoltre il recepimento delle proposte formulate dall'Organismo di Vigilanza al Consiglio di Amministrazione per gli eventuali aggiornamenti ed adeguamenti del Modello, ritenuti necessari in seguito a violazioni o elusioni delle prescrizioni che mettano in evidenza l'inefficacia del Modello, significative modifiche dell'assetto organizzativo, variazioni normative o orientamenti giurisprudenziali.

Si considerano invece modifiche non sostanziali del Modello tutte quelle non sopra individuate, tra cui principalmente:

- le variazioni al sistema delle deleghe conferite e riportate nel presente Modello, ad eccezione di quanto sopra;
- la modifica dei presidi esistenti e/o l'introduzione di nuovi presidi;
- l'aggiornamento/modifica/integrazione della Mappa dei rischi, diversa da quella citata tra le modifiche sostanziali;
- l'aggiornamento/modifica/integrazione dei singoli componenti del Modello, i quali sono aggiornati dalle singole funzioni interne competenti, con la supervisione ed il supporto di un soggetto esterno ove ritenuto necessario dall'O.d.V..

Il compito di attuare il Modello è del Consiglio di Amministrazione mediante l'emanazione delle opportune disposizioni interne.

Sono destinatari del Modello tutti coloro che operano per il conseguimento dello scopo e degli obiettivi dell'ente, e pertanto in generale gli esponenti dello stesso, i componenti l'Organismo di Vigilanza, i dipendenti, i collaboratori anche parasubordinati, i consulenti esterni.

Per esponente si intendono, come di volta in volta in carica, il Presidente, i Consiglieri di Amministrazione ed il Direttore Generale, nonché i membri degli altri Organi Sociali dell'ente eventualmente istituiti.

Si intende, inoltre, qualsiasi altro soggetto in posizione apicale che rivesta funzioni di rappresentanza, amministrazione o direzione, gestione, controllo dell'ente, ai sensi del D. Lgs. 231/2001.

A tal fine, si ricorda che, ai fini del predetto Decreto Legislativo, si considera soggetto in posizione apicale colui che riveste funzioni di rappresentanza dell'ente (ad esempio il Presidente della Società), di amministrazione o direzione dell'ente (ad esempio gli Amministratori ed il Direttore Generale), nonché coloro che esercitano anche di fatto la gestione e il controllo dello stesso.

L'adozione del presente Modello Organizzativo è comunicata a tutte le risorse operanti per la Società al momento della sua delibera di approvazione.



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 8 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

Le regole di condotta contenute nel presente Modello si integrano con quelle del Codice Etico adottato dall'ente.

Il Modello è comunicato a ciascun componente degli Organi sociali, a ciascun soggetto apicale e a ciascun responsabile di funzione, i quali sottoscrivono una dichiarazione di conoscenza e adesione al Modello, archiviata dall'Organismo di Vigilanza.

Un Estratto del Modello è messo a disposizione di tutti i collaboratori dell'ente presso gli uffici amministrativi.

Il Codice Etico viene affisso nelle bacheche e viene consegnato a tutti gli apicali, i componenti gli Organi Sociali ed a tutti i dipendenti e collaboratori anche parasubordinati.

I principi e i contenuti del Decreto e del Modello sono divulgati mediante corsi di formazione, ai quali tutti gli apicali, i dipendenti ed i collaboratori in generale sono tenuti a partecipare. I corsi di formazione saranno diversificati in relazione alle funzioni ricoperte dai partecipanti (Componenti l'O.d.V., Amministratori, Apicali, dipendenti e collaboratori).

La formazione verrà effettuata, oltre che contestualmente all'adozione del Modello, anche a seguito di sue variazioni particolarmente significative, dovute ad eventi esogeni (esempio: inserimenti di nuovi reati presupposto e/o modifiche normative attinenti) ed endogeni (modifiche relative alla Società). La partecipazione ai corsi di formazione è obbligatoria e l'O.d.V. vigilerà su tale partecipazione. Il contenuto e la frequenza dei corsi saranno stabiliti dall'O.d.V..

L'impegno al rispetto del Modello 231 della Società da parte di terzi aventi rapporti contrattuali con la stessa è previsto da apposita clausola del relativo contratto (di cui in allegato al presente Modello).

1.1.2 I soggetti ed i reati presupposto

Il Decreto Legislativo 8 giugno 2001, n. 231 (in seguito "D.Lgs. 231" o "Decreto") ha introdotto, nel nostro ordinamento giuridico, la "responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" (definite enti), in conseguenza di reati commessi o tentati nel loro interesse o a loro vantaggio da soggetti che rivestono funzioni di rappresentanza, di amministrazione o direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria (c.d. "soggetti apicali"). Sono soggette alla stessa normativa, altresì, le persone che esercitano anche di fatto la gestione ed il controllo dell'ente (c.d. "soggetti apicali") e le persone sottoposte alla direzione o vigilanza dei predetti soggetti.

La normativa esclude, viceversa, che l'ente risponda se i cosiddetti "reati presupposto" – e cioè i reati richiamati dal Decreto – siano compiuti nell'interesse esclusivo della persona fisica o di terzi.

Il tipo di responsabilità prefigurata dal Decreto si aggiunge alla responsabilità che fa capo alla persona singola ("ex se" considerata).

Per effetto dell'entrata in vigore dell'indicata norma, gli enti possono elaborare ed adottare un sistema di prevenzione che, intervenendo sui processi, concorra a prevenire la commissione di fatti illeciti commessi da propri dipendenti e/o collaboratori, così da fungere da esimente rispetto alle sanzioni previste dal Decreto citato.

Trattasi della prevenzione dei surrichiamati "reati presupposto" commessi, come detto, nell'interesse dell'ente o a suo vantaggio dai soggetti specificamente sopra individuati.

In sintesi, l'art. 5 del Decreto prevede che l'ente sia responsabile relativamente ai reati individuati dallo stesso Decreto, commessi da:

- soggetti apicali, come sopra definiti, ovvero
- persone sottoposte alla direzione o alla vigilanza di un apicale.

Le disposizioni in esame contengono profili di novità e di estrema rilevanza, poiché introducono la possibilità che ad un ente venga ricondotta una responsabilità definita genericamente "amministrativa", ma di fatto di tipo penale, diversa, autonoma e concorrente rispetto a quella delle persone fisiche e conseguente a specifici fatti di reato commessi nell'interesse o a vantaggio dell'ente stesso.

Va, altresì, osservato che tale tipo di responsabilità degli enti non opera "sic et simpliciter" per tutti i reati commessi da coloro che lavorano al loro interno, ma, affinché sussista, occorre che si tratti di uno dei succitati "reati presupposto" previsti dal Decreto stesso, che ha subito le seguenti integrazioni normative, che hanno ampliato il novero dei reati ricompresi nell'ambito di operatività della norma in esame:

- Decreto Legge n. 350 del 25 settembre 2001, convertito con Legge n. 409 del 23 novembre 2001, recante "Disposizioni urgenti in vista dell'introduzione dell'euro, in materia di tassazione dei redditi di natura finanziaria, di emersione di attività detenute all'estero, di cartolarizzazione e di altre operazioni finanziarie", relativo alla "Falsità in monete, in carte di pubblico credito e in valori di bollo";
- Decreto Legislativo n. 61 dell'11 aprile 2002, in materia di false comunicazioni sociali;
- Legge n. 7 del 14 gennaio 2003, in materia di repressione del finanziamento al terrorismo;
- Legge n. 228 dell'11 agosto 2003, "Misure contro la tratta di persone";
- Legge n. 62 del 18 aprile 2005, recante "Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee (Legge comunitaria 2004)", che ha introdotto tra i reati-presupposto i reati di abuso di mercato;
- Legge n. 262 del 28 dicembre 2005 in materia di tutela del risparmio, che ha modificato l'art. 25 ter del D.Lgs. 231/2001 in relazione ai reati societari;
- Legge n. 7 del 9 gennaio 2006, recante "Disposizioni concernenti la prevenzione e il divieto delle pratiche di mutilazione genitale femminile";
- Legge n. 123 del 3 agosto 2007, che ha previsto la responsabilità dell'ente per reati contro la tutela della salute e della sicurezza sul lavoro;
- Decreto Legislativo n. 231 del 21 novembre 2007 che estende la responsabilità dell'ente ai reati di ricettazione, riciclaggio ed impiego di denaro beni o utilità di provenienza illecita;
- Legge n. 48 del 18 marzo 2008 che prevede, tra i reati presupposto, i delitti informatici ed il trattamento illecito di dati;
- Decreto legislativo n. 81 del 8 aprile 2008, che ha modificato l'art. 25 septies del Decreto;
- Legge n. 94 del 15 luglio 2009 che introduce (art. 2, co. 29) Delitti di criminalità organizzata;
- Legge n. 99 del 23 luglio 2009 "Disposizioni per lo sviluppo e internazionalizzazione delle imprese, nonché in materia di energia", che introduce (art. 15, co. 7) i Delitti contro l'industria e il commercio ed i Delitti in materia di violazione del diritto d'autore;
- Legge n. 116 del 3 agosto 2009 che all'art. 4 introduce il reato di "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria";
- Decreto Legislativo n. 39 del 27 gennaio 2010 "Attuazione della direttiva 2006/43/CE, relativa alle revisioni legali dei conti annuali e dei conti consolidati, che modifica le direttive 78/660/CEE e 83/349/CEE". Con tale Decreto viene abrogato l'Art. 2624, e modificato l'Art.2625 del c.c., entrambi richiamati dall'art.25 ter del D.Lgs. 231/2001;

- Legge n. 108 del 2 luglio 2010 che ha modificato alcuni articoli del Codice penale richiamati dal D.Lgs. 231/2001;
- Decreto Legislativo n. 121 del 7 luglio 2011, rubricato “Attuazione della Direttiva 2008/99/CE sulla tutela penale dell’ambiente, nonché della Direttiva 2009/123/CE che modifica la Direttiva 2005/35/CE relativa all’inquinamento provocato dalle navi e all’introduzione di sanzioni per violazioni”.
Tale Decreto prevede, all’art. 2:
 - la diversa numerazione dell’art. 25 novies del D.Lgs. 231/2001 (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria) in art. 25 decies;
 - l’inserimento nel D.Lgs. 231/2001 dell’art. 25 undecies “Reati ambientali”.
- Decreto Legislativo n. 109 del 25 luglio 2012, che ha introdotto l’art. 25-duodecies – “Impiego di cittadini di paesi terzi il cui soggiorno è irregolare”.
- Legge n. 190 del 6 novembre 2012 rubricata “Disposizioni per la prevenzione e la repressione della corruzione e dell’illegalità nella pubblica amministrazione”. Tale norma ha introdotto, tra i c.d. “reati presupposto” il reato di “Induzione indebita a dare o promettere utilità” (art. 319-quater c.p.) e il reato di “Corruzione tra privati” (art. 2635 c.c.) ed ha modificato la portata e/o il trattamento sanzionatorio di alcuni reati contro la Pubblica Amministrazione, quali la “Corruzione per un atto d’ufficio” (art. 318 c.p.), ora rubricata “Corruzione per l’esercizio della funzione”, e la concussione (art. 317 c.p.), in parte confluita nel succitato nuovo reato di “Induzione indebita a dare o promettere utilità” (art. 319-quater c.p.);
- Decreto Legislativo n. 39 del 4 marzo 2014, rubricato “Attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile”, il quale introduce tra i “reati presupposto”, in particolare nell’art. 25-quinquies, l’ “adescamento di minorenni” (art. 609-undecies c.p.);
- Legge n. 186 del 15 dicembre 2014, rubricata “Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di auto riciclaggio”, la quale introduce nell’art. 25-octies del Decreto il reato di autoriciclaggio (art. 648-ter 1 c.p.);
- Legge n. 68 del 22 maggio 2015, “Disposizioni in materia di delitti contro l'ambiente”, la quale aggiunge ai reati-presupposto dell’art. 25-undecies del Decreto: il delitto di inquinamento ambientale (art. 425-bis c.p.), il delitto di disastro ambientale (art. 452-quater c.p.), i delitti colposi contro l’ambiente (art.452-quinquies c.p.), i delitti associativi aggravati (art. 452-octies c.p.), il delitto di traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.);
- Legge n. 69 del 27 maggio 2015, “Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio”, che apporta alcune modifiche agli artt. 24-ter, 25, 25-ter del Decreto.
- Decreti Legislativi n. 7 e n. 8 del 15 gennaio 2016, che hanno introdotto modifiche ai delitti informatici.
- Decreto Legislativo n. 125 del 21 giugno 2016 (Attuazione della direttiva 2014/62/UE sulla protezione mediante il diritto penale dell’euro e di altre monete contro la falsificazione) che ha introdotto modifiche agli articoli del Codice Penale relativi ai delitti di falsità in monete, carte di pubblico credito e valori di bollo (art. 25-bis del D. Lgs. 231)



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 11 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

- Legge n. 199 del 29 ottobre 2016, contenente disposizioni in materia di contrasto ai fenomeni del lavoro nero, dello sfruttamento del lavoro in agricoltura e di riallineamento retributivo nel settore agricolo.
- Decreto Legislativo n. 38 del 15 marzo 2017 (Attuazione della decisione quadro 2003/568/GAI del Consiglio, del 22 luglio 2003, relativa alla lotta contro la corruzione nel settore privato), che ha introdotto modifiche alla Corruzione tra privati (art. 2635 c.c.).
- Decreto Legislativo n. 90 del 25 maggio 2017 che recepisce la Direttiva UE 2015/849 (c.d. IV Direttiva Antiriciclaggio) relativa alla "prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo".
- Legge n.161 del 17 ottobre 2017 che introduce nuovi delitti in relazione all'immigrazione clandestina
- Legge 20 novembre 2017, n. 167 con «Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2017» che introduce nuovi reati per «razzismo e xenofobia»
- Legge 179 del 30 novembre 2017, che introduce nuove "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto pubblico o privato" (il cd. Whistleblowing)
- Decreto Legislativo n. 107 del 10 agosto 2018 che introduce "Norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) n. 596/2014, relativo agli abusi di mercato e che abroga la direttiva 2003/6/CE e le direttive 2003/124/UE, 2003/125/CE e 2004/72/CE".
- Legge n. 3 del 11 gennaio 2018, che introduce modifiche relativamente alla "sperimentazione clinica di medicinali nonché disposizioni per il riordino delle professioni sanitarie e per la dirigenza sanitaria del Ministero della salute".
- Decreto Legislativo n. 21 del 1 marzo 2018, con "Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale a norma dell'articolo 1, comma 85, lettera q), della legge 23 giugno 2017, n. 103."
- Decreto Legislativo n. 21 del 1 marzo 2018, che introduce nuove disposizioni per "Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (art. 604-bis c.p.)".
- Legge n. 39 del 3 maggio 2019, che introduce nuove disposizioni per "Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdecies).
- Legge n. 157 del 19 dicembre 2019 "Conversione in legge, con modificazioni del Dlgs. n. 124 del 26 ottobre 2019, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili" che introduce i reati tributari all'interno del catalogo di cui al D.Lgs. 231 (Art. 25-quinquiesdecies)".
- Decreto Legislativo n. 75 del 14 luglio 2020, che introduce nuove disposizioni per adeguare la disciplina penale italiana alla direttiva (UE) 2017/1371 del Parlamento europeo e del Consiglio, del 5 luglio 2017, in tema di lotta contro la frode che leda gli interessi finanziari dell'Unione (c.d. "direttiva PIF" – direttiva per la protezione interessi finanziari) e che introduce il reato di contrabbando all'interno del catalogo di cui al D.Lgs. 231 (Art. 25-sexiesdecies)
- Decreto Legislativo n. 184 del 08 novembre 2021 in materia di "Delitti in materia di strumenti di pagamento diversi dai contanti" che modifica l'Art. 25-octies.
- Decreto Legislativo n. 195 del 08 novembre 2021 in materia di "Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio" che modifica l'Art. 25-octies
- Legge 23 Dicembre 2021, n.238, "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2019-2020" che ha introdotto alcune modifiche alle previsioni di reato richiamate dal D. Lgs. 231/2001.
- Decreto Legge n. 13 del 25 febbraio 2022, che ha introdotto alcune "Misure di contrasto alle frodi nel settore delle agevolazioni fiscali ed economiche" e conseguenti modifiche alle previsioni di reato richiamate dal D. Lgs. 231/2001:

- Legge n. 22 del 9 marzo 2022, “Disposizioni in materia di reati contro il patrimonio culturale” che ha introdotto l’Art 25 septiesdecies “Delitti contro il patrimonio culturale” e l’Art. 25 duodevicies “Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici”.

Inoltre il Decreto Legislativo n. 58 del 24 febbraio 1998 prevede, per le Società quotate, oltre al reato di abuso di informazioni privilegiate e di manipolazione del mercato, anche l’ipotesi delle corrispondenti fattispecie di illeciti amministrativi, stabilendo per essi specifiche sanzioni e l’applicazione in linea di massima dei principi enunciati dal Decreto Legislativo n. 231/2001.

La Legge n. 146 del 16 marzo 2006 ha previsto un’ulteriore estensione della responsabilità amministrativa degli enti in relazione a determinate ipotesi di reato transnazionale. In questo caso i reati presupposto non sono stati inseriti nel Decreto Legislativo n. 231/2001, ma sono contenuti nella suddetta Legge, che prevede anche le sanzioni e l’applicabilità del Decreto per i conseguenti illeciti.

Il testo attualmente in vigore del Decreto contempla dunque le seguenti fattispecie di reato:

- art. 24 (indebita percezione di erogazioni, truffa in danno dello stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello stato o di un ente pubblico);
- art. 24 bis (delitti informatici e trattamento illecito di dati);
- art. 24 ter (delitti di criminalità organizzata);
- art. 25 (concussione, induzione indebita a dare o promettere utilità e corruzione);
- art. 25 bis (falsità in monete, in carte di pubblico credito e in valori di bollo);
- art. 25 bis.1. (delitti contro l’industria e il commercio);
- art. 25 ter (reati societari);
- art. 25 quater (delitti con finalità di terrorismo o di eversione dell’ordine democratico);
- art. 25 quater.1. (pratiche di mutilazione di organi genitali femminili);
- art. 25 quinquies (delitti contro la personalità individuale);
- art. 25 sexies (abusi di mercato);
- art. 25 septies (omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro);
- art. 25 octies (ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio);
- art. 25 novies (delitti in materia di violazione del diritto d’autore);
- art. 25 decies (induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’autorità giudiziaria);
- art. 25 undecies (reati ambientali);
- art. 25 duodecies (impiego di cittadini di paesi terzi il cui soggiorno è irregolare);
- art. 25-terdecies (Razzismo e xenofobia).
- art. 25-quaterdecies (Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d’azzardo esercitati a mezzo di apparecchi vietati).
- art. 25-quinquiesdecies (Reati tributari)
- art. 25-sexiesdecies (reato di contrabbando)

- art. 25-septiesdecies (delitti contro il patrimonio culturale)
- Art. 25-duodevicies (Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici)

Ad esse si aggiungono altresì i seguenti reati transnazionali, di cui al citato art. 10 della Legge 146/2006, in quanto ai conseguenti illeciti previsti da detto articolo si applicano le disposizioni di cui al Decreto:

- art. 416 c.p. associazione per delinquere;
- art. 416 bis c.p. associazione di tipo mafioso;
- art. 291 quater T.U. D.P.R. 43/73 (materia doganale) associazione per delinquere finalizzata al contrabbando di tabacchi esteri;
- art. 74 del T.U. D.P.R. 309/90 associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope;
- art. 12 commi 3, 3 bis, 3 ter e 5 del T.U. di cui al D.Lgs. n.286/98 disposizioni contro le immigrazioni clandestine;
- art. 377 bis c.p. induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all’Autorità Giudiziaria;
- art. 378 c.p. favoreggiamento personale.

Riprendendo l’esame della responsabilità degli enti, si sottolinea come, per il meccanismo di accertamento di tale tipo di responsabilità, essa venga definita "amministrativa" in omaggio al principio costituzionale della personalità della responsabilità penale, anche se il "modus operandi" la avvicina in più punti ad una responsabilità penale sia per il tipo di processo, sia per le sanzioni comminate, sia ancora per l'autorità giudicante e inquirente (penale) ed infine per la possibilità di adottare misure cautelari.

Il processo cui è fatto riferimento si articolerà quindi in due autonomi giudizi: uno nei confronti del soggetto indagato ed un altro nei confronti dell’ente.

Sono previste sanzioni (ex art. 9 e 10) pecuniarie ed eventualmente, per i casi più gravi, interdittive (l’interdizione dall’esercizio dell’attività, la sospensione o la revoca delle autorizzazioni funzionali alla commissione dell’illecito, il divieto di contrattare con la Pubblica Amministrazione, l’esclusione da agevolazioni o sussidi, il divieto di pubblicizzare beni o servizi), la confisca del prezzo o del profitto del reato, e la pubblicazione della sentenza.

Particolare rilevanza assumono le "sanzioni interdittive", che si applicano in relazione ai reati per i quali sono espressamente previste e quando ricorrono le condizioni indicate dall'art. 13: la loro gravità deriva anche dalla comminabilità in sede cautelare.

Le sanzioni possono essere evitate ove l’ente adotti un modello di comportamento idoneo a prevenire i “reati presupposto”. Trattasi del “Modello di organizzazione gestione e controllo” (il “Modello” o “Modello 231”).

Come stabilito all’art. 6 del Decreto, tale Modello deve rispondere alle seguenti esigenze:

- individuare le attività nel cui ambito possono essere commessi reati;
- prevedere specifici protocolli diretti a programmare la formazione e l’attuazione delle decisioni dell’ente in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell’Organismo deputato a vigilare sul funzionamento e sull’osservanza del Modello;

- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Esso deve inoltre prevedere, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire e ad eliminare tempestivamente situazioni di rischio.

Inoltre, l'efficace attuazione del Modello richiede una verifica periodica e l'eventuale modifica dello stesso quando siano individuate significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività.

L'Ente non risponde se prova che:

1. in caso di reato presupposto commesso dai cosiddetti "soggetti apicali":
 - l'organo dirigente ha adottato (e provato di avere efficacemente attuato) prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi e ha affidato ad un "Organismo di Vigilanza", dotato di autonomi poteri di iniziativa e di controllo, l'onere di vigilare e di curare il suo aggiornamento;
 - le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione ovvero non vi è stata omessa o insufficiente vigilanza da parte dell'"Organismo" di controllo di cui al precedente punto 1 a);
2. in caso di reato presupposto commesso da persone sottoposte alla direzione e alla vigilanza di un apicale, non vi è stata inosservanza degli obblighi di direzione o vigilanza. Tale inosservanza è in ogni caso esclusa se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

Il Decreto, all'art. 6, pone a carico dell'ente l'onere di provare l'avvenuta adozione delle misure preventive solo nel caso in cui l'autore del reato sia un soggetto "apicale" come sopra definito ("inversione dell'onere della prova").

Sulla base dell'interpretazione letterale della norma, si ritiene invece che, nel caso in cui l'autore del reato sia sottoposto all'altrui direzione o vigilanza, l'onere probatorio, relativo alla mancata adozione delle misure preventive, spetti al Pubblico Ministero.

Si ricorda nuovamente che ai fini del Decreto si considera soggetto in posizione apicale colui che riveste funzioni di rappresentanza dell'ente (ad esempio il Presidente del Consiglio di Amministrazione), di amministrazione o direzione dell'ente (ad esempio gli Amministratori ed il Direttore Generale) ovvero di una sua unità organizzativa dotata di autonomia finanziaria e funzionale (ad esempio institori), nonché coloro che esercitano, anche di fatto, la gestione e il controllo dello stesso.

Con riferimento ai reati presupposto di cui sopra, le fattispecie attualmente più rilevanti, in quanto commissibili dalla maggioranza degli enti, possono ricomprendersi:

- reati contro la Pubblica Amministrazione,
- reati societari,
- reati commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
- reati ambientali.
- reati tributari.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 15 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

L'accertamento della responsabilità dell'ente è attribuito al giudice penale mediante la verifica della sussistenza del reato ed il sindacato di idoneità sul modello organizzativo adottato.

1.2 Il Decreto Legislativo 81 del 9 aprile 2008

Il legislatore del D. Lgs. n. 81/2001, tenuto conto della particolarità del contesto di riferimento, all'art. 30 ha inteso individuare più specificamente gli obiettivi ed i contenuti, anche ulteriori rispetto a quelli indicati negli art. 6 e 7 del D. Lgs. n. 231/2001, che devono caratterizzare i Modelli organizzativi perché questi possano essere giudicati idonei ed efficacemente adottati, con conseguente possibilità per l'ente, in tali ipotesi, di beneficiare dell'efficacia esimente ad essi riconosciuta.

In particolare, il Modello organizzativo dovrà essere adottato ed efficacemente attuato, in modo tale da assicurare un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

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

Proseguendo, l'art. 30 richiede espressamente che il modello organizzativo preveda:

- idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui sopra. Tale previsione, da un lato, facilita l'attività investigativa documentale della polizia giudiziaria finalizzata all'accertamento della responsabilità amministrativa dell'ente; dall'altro, offre all'ente la possibilità di "opporre" una preliminare difesa a dimostrazione della assenza di responsabilità;
- per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche ed i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- un idoneo sistema di controllo sull'attuazione del medesimo Modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del Modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

In sede giurisprudenziale, il Tribunale di Trani, con la sentenza in data 29.10.2009, ha statuito la necessità che l'impianto del Modello, allorché non siano coinvolti soggetti dipendenti dell'ente, preveda comunque l'adozione di cautele e regole per evitare che dipendenti di enti terzi possano subire lesioni o

perdere la vita per infrazioni commesse dai loro datori di lavoro nell'esecuzione delle attività lavorative loro assegnate. In particolare, è stato chiarito che il controllo dei rischi non può esaurirsi nell'ambito della struttura organizzativa ed aziendale della società in questione, ma deve essere esteso anche all'osservanza delle medesime regole da parte dei soggetti che con quest'ultima entrano, direttamente o indirettamente, in rapporti lavorativi.

L'adozione e l'efficace attuazione del Modello di verifica e controllo assume, inoltre, particolare rilievo in termini di riconoscimento dell'avvenuto adempimento dell'obbligo di vigilanza nei confronti del delegato da parte del Datore di Lavoro delegante, secondo quanto previsto dall'art. 16, comma 3, del D. Lgs. n. 81/2008. Quest'ultimo stabilisce infatti che tale obbligo di vigilanza si intende assolto in caso di adozione ed efficace attuazione del Modello di verifica e controllo di cui all'articolo 30, comma 4.

In punto di idoneità del Modello, il comma 5 dell'articolo in esame introduce una presunzione di legge secondo cui si considera conforme alle prescrizioni sopra riportate il Modello organizzativo adottato dall'ente definito conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 per le parti corrispondenti.

In merito, inoltre, è previsto, ai sensi del combinato disposto dell'art. 6 e dell'art. 30, comma 5-bis del D. Lgs. n. 81/2008, che la Commissione consultiva permanente per la salute e sicurezza sul lavoro può indicare Modelli di organizzazione e gestione aziendale, nonché elaborare procedure semplificate per l'adozione e l'efficace attuazione dei Modelli di organizzazione e gestione della sicurezza nelle piccole e medie imprese. Tali procedure sono recepite con decreto del Ministero del lavoro, della salute e delle politiche sociali.

Rilevante ai fini che qui interessano è anche la disposizione contenuta all'art. 51, comma 3- bis secondo cui gli organismi paritetici di cui all'art. 2, comma 1, lettera ee), su richiesta delle imprese, possono rilasciare l'asseverazione dell'adozione e dell'efficace attuazione dei Modelli di organizzazione e gestione della sicurezza di cui all'articolo 30.

Si ricorda inoltre che è stato statuito in sede giurisprudenziale (cfr. Tribunale di Trani, sentenza in data 26 ottobre 2009), che i documenti di valutazione dei rischi redatti ai sensi degli artt. 26 e 28 del D. Lgs. n. 81/2008:

- non sono equiparabili al Modello organizzativo e gestionale di cui al D. Lgs. n. 231/2001;
- non assumono valenza nella direzione di assicurare l'efficacia esimente di cui agli artt. 6 e 7.

In merito, occorre rilevare che il sistema introdotto dal D. Lgs. n. 231/2001 impone agli enti di adottare un Modello organizzativo diverso e ulteriore rispetto a quello previsto dalla normativa antinfortunistica, onde evitare in tal modo la responsabilità amministrativa.

Non a caso, mentre i documenti di valutazione dei rischi nel contesto normativo di cui al D. Lgs. n. 81/2008 sono disciplinati dagli artt. 26 e 28, il Modello di organizzazione e gestione di cui al D. Lgs. n. 231/2001 è contemplato dall'art. 30 del citato D. Lgs. n. 81/2008, segnando così una distinzione non solo nominale ma anche funzionale.

1.3 Ulteriori fonti

Ad integrazione dei punti precedenti, sono state impiegate anche le seguenti ulteriori fonti normative, per quanto di interesse 231:

- D. Lgs. 193/2007 – HACCP, "Attuazione della direttiva 2004/41/CE relativa ai controlli in materia di sicurezza alimentare e applicazione dei regolamenti comunitari nel medesimo settore", nonché l'ulteriore normativa nazionale e comunitaria afferente;



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 17 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

- D.P.R. 62/2013, “Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165”;
- Circolare n. 83607/2012 del Comando Generale della Guardia di Finanza - III Reparto Operazioni - Ufficio Tutela Economia e Sicurezza: “Attività della Guardia di Finanza a tutela del mercato dei capitali - Parte IV: Disposizioni comuni”.

Alle suddette fonti normative si è fatto riferimento, nel presente Modello, per la redazione dei protocolli afferenti nonché per la valutazione dei rischi all'interno della fase di Risk Assessment.

Con riferimento alla Circolare della Guardia di Finanza, essa è stata impiegata quale elemento per la definizione dell'Organismo di Vigilanza.

2 LE LINEE GUIDA PER LA REDAZIONE DEL MODELLO

Il Decreto fornisce scarse indicazioni in merito alle modalità di redazione del Modello, nonché ai suoi contenuti, al fine di consentirne l'efficacia esimente.

Infatti, le uniche indicazioni sono reperibili al secondo comma dell'art.6 del Decreto, che stabilisce che i Modelli “devono rispondere alle seguenti esigenze:

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

A miglior specifica, il terzo comma del medesimo articolo statuisce che “I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati.”

Il Modello della Società è stato conseguentemente predisposto sulla base delle “linee guida per la costruzione dei Modelli di organizzazione, gestione e controllo ex D. Lgs. 231/2001” emesse da Confindustria, ultima edizione (31 marzo 2008), approvate in data 2 aprile 2008 dal Ministero della Giustizia, in quanto l'aggiornamento (della precedente edizione del 2002) è stato ritenuto “complessivamente adeguato e idoneo al raggiungimento dello scopo fissato dall'art. 6, comma 3 del D. Lgs. n. 231/2001”.

3 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO: SCOPO E CONTENUTO

Scopo del Modello è quello di fornire indicazioni sui contenuti del Decreto e sul particolare tipo di responsabilità amministrativa degli enti che esso introduce nel nostro ordinamento per i reati commessi, nel loro interesse o vantaggio, dai propri esponenti o dipendenti.

È inoltre volto ad indirizzare le attività interne affinché siano in linea con lo stesso e a vigilare sul suo funzionamento e sulla sua osservanza.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 18 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

In particolare il Modello ha la finalità di:

- generare, in tutti coloro che operano in nome e per conto dell’ente, la consapevolezza di poter incorrere, in caso di violazione delle norme richiamate dal Decreto Legislativo n. 231/2001, in un illecito, passibile di sanzioni nei propri confronti e nei riguardi dell’ente (se questo ha tratto vantaggio dalla commissione del reato, o comunque se quest’ultimo è stato commesso nel suo interesse);
- chiarire che i comportamenti illeciti sono condannati dalla Società in quanto contrari sia alle disposizioni di legge sia ai principi cui essa intende attenersi nell’espletamento della propria missione;
- fissare e rendere noti tali principi, indicandoli nel Modello e nel Codice Etico adottati;
- implementare, in particolare attraverso l’O.d.V., azioni di monitoraggio e controllo interno, indirizzate soprattutto agli ambiti gestionali più esposti in relazione al Decreto Legislativo n. 231/2001, nonché la formazione dei collaboratori al corretto svolgimento dei loro compiti, al fine di prevenire e contrastare la commissione dei reati stessi;
- prevedere delle sanzioni a carico dei destinatari del presente Modello che lo abbiano violato, ovvero abbiano commesso un illecito sanzionabile ai sensi del D. Lgs. 231/2001.

A seguito dell’emanazione del D. Lgs. 231/2001, la Società ha avviato il processo di individuazione ed adozione di tutte le misure necessarie ed opportune, finalizzate ad adeguare la propria organizzazione interna alle disposizioni del Decreto.

Il Modello si compone di una Parte Generale ed una Parte Speciale.

Con riferimento alla presente Parte Generale, essa dunque “descrive la disciplina di riferimento, l’assetto organizzativo dell’ente, il sistema di Governance (tra cui il sistema disciplinare), prevede un’attività di formazione dei dipendenti in relazione alla disciplina della responsabilità degli enti ed elabora i risultati della fase “risk assessment””.

Con riferimento alla Parte Speciale, essa consta dei seguenti capitoli:

- presidi per la gestione del rischio di commissione dei reati, in cui sono analizzati i sistemi di gestione e controllo ed inseriti i protocolli;
- mappatura dei rischi, in cui sono state identificate delle attività che, esclusivamente in relazione ai loro specifici contenuti, potrebbero essere esposte (o maggiormente esposte) al rischio di commissione dei reati contemplati dal D. Lgs. 231/2001.

Per la sua elaborazione, si è proceduto - previa l’opportuna ricognizione - ad associare ai processi organizzativi interni (nel cui svolgimento, in via teorica, potrebbero integrarsi gli estremi di reato di cui alla normativa in esame) le varie fattispecie di reato considerate dal Decreto.

Le aree di rischio individuate sono da intendersi come un complesso in evoluzione, da adeguarsi periodicamente in relazione a modifiche normative e/o a variazioni interne.

4 IL PROFILO DELLA SOCIETÀ

4.1 La storia

Oltre 100 anni di storia raccontano e delineano il profilo della Società Biscotti P. Gentilini Srl che si è trasformata da piccola bottega artigianale in un’azienda solida ed affermata nel panorama nazionale.

La passione della famiglia Gentilini, l’impegno e la continua ricerca della qualità coniugata con il mantenimento degli antichi sapori, sono infatti i principi fondamentali e imprescindibili della Società.



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 19 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

L'azienda fu fondata nel 1890 da Pietro Gentilini, (nato a Vergato nel 1856) che, dopo aver arricchito il proprio bagaglio culturale e professionale alle dipendenze di importanti imprese, si trasferì a Roma, dove aprì il suo primo laboratorio per la produzione di pane e biscotti.

In quegli anni si stava diffondendo in Italia un biscotto secco, di origine anglosassone, denominato Oswego. Pietro Gentilini ne intuì subito il potenziale e passò molto tempo allo studio di una ricetta migliorata e personalizzata. Dopo numerosi tentativi riuscì nell'impresa di creare un biscotto dal sapore semplice, ma allo stesso tempo unico e, per differenziarlo dagli Oswego allora in commercio, lo chiamò Osvego.

Il successo non tardò ad arrivare e nel 1906 in Via Alessandria, nella nascente zona industriale della Roma del risorgimento economico, venne aperta la Fabbrica di Biscotti P. Gentilini, che, per le accresciute esigenze produttive, fu trasferita nel 1958 nell'attuale sede di Via Tiburtina.

Nel corso degli anni accanto agli Osvego e ai biscotti da dessert, Pietro e i suoi discendenti hanno arricchito e diversificato la propria "officina del gusto" con nuove linee di prodotti. Tra questi i Novellini, le Fette Biscottate, i Frollini, il Panettone e la Pizza di Pasqua (dolce tipico romano).

Nel 1987, per soddisfare la crescente richiesta del mercato, a seguito del successo commerciale dei propri prodotti, fu introdotta l'automazione delle linee di produzione. Automazione che ha coniugato la modernità e l'innovazione con l'autenticità e la genuinità che si ritrovano nelle ricette rimaste inalterate da oltre un secolo così come la ricerca e l'utilizzo delle migliori materie prime.

A partire dal 2004 per completare l'offerta di prodotti di qualità, sono stati formalizzati accordi per la commercializzazione, a marchio Gentilini, di prodotti di terzi quali wafer, marmellate, miele, torroni, panettoni e colombe pasquali.

4.2 La sede aziendale

La Sede legale della società è ubicata a Roma in Via Affile, 16/18, mentre gli uffici si trovano, sempre a Roma in Via Tiburtina Valeria, 1302.

Lo stabilimento, è costituito da un edificio industriale articolato su un unico piano di 7 m. di altezza, con struttura in cemento armato, di circa 4.900 mq, destinato alla produzione con annessi magazzini, locali tecnologici, e servizi, e da un edificio distaccato di 9.50 m. di altezza, costituito da un piano seminterrato e due piani fuori terra, con struttura in c.a. di circa 1150 mq di superficie, destinato a deposito prodotti finiti e uffici direzionali.

Di seguito si riporta una descrizione degli ambienti:

Edificio produzione

L'edificio produzione è costituito dal corpo originario della fabbrica di biscotti, di superficie di 3600 mq, e da un corpo di fabbrica aggiunto come ampliamento (per ampliamento linee di produzione biscotti e fette biscottate), costituito da un edificio industriale di tipo prefabbricato ad un unico piano fuori terra con struttura in c.a., di circa 1300 mq di superficie.

L'edificio produzione è articolato nelle seguenti aree funzionali :

- area produzione biscotti e fette biscottate. In questa area sono presenti n. 4 linee di cottura dei biscotti e fette biscottate, delle zone preparazione impasti con relative attrezzature e macchinari, nastri trasportatori, macchine per il confezionamento e una zona di stoccaggio giornaliero dei prodotti.
- area uffici di stabilimento, assistenza tecnica macchinari. In questa area adiacente all'area produzione, sono presenti il locale prove di laboratorio, ufficio controllo qualità, una sala riunioni (al primo piano), gli

uffici dell'area tecnica di primo intervento.

- area magazzino materiale imballaggio. In questa area costituita da tre locali, adiacente all'area produzione, avviene il deposito del materiale di imballaggio costituiti prevalentemente da sacchetti di carta e cartone compattati, necessari ai reparti di confezionamento delle linee di produzione.

Deposito prodotti finiti e uffici direzionali

L'edificio industriale in oggetto con copertura a volta, è costituito da un piano seminterrato e due piani fuori terra, con struttura in c.a. di circa 1150 mq di superficie coperta.

L'edificio è suddiviso in una zona destinata a deposito, articolata su un unico piano di 9.50 m di altezza, e una zona destinata ad uffici direzionali articolata su due piani.

L'edificio in oggetto è articolato nelle seguenti aree funzionali:

- Area deposito prodotti finiti, superficie 850 mq, dove avviene il deposito della produzione, biscotti e fette biscottate, confezionati in scatole di cartone su pallet. La movimentazione dei pallet, avviene mediante impiego di carrelli elevatori elettrici. L'area deposito prodotti finiti comunica al piano seminterrato con la zona uffici ai piani superiori. In quest'area sono presenti complessivamente n. 4 persone.
- Area uffici, superficie 340 mq, articolata su due piani, piano terra e piano primo dell'edificio, in cui vengono svolte tutte le funzioni direzionali, commerciali e amministrative connesse all'esercizio dell'attività aziendali. In quest'area sono presenti complessivamente n. 11 persone.
- Area esterna e parcheggio autoveicoli, detta zona si sviluppa tutta attorno all'edificio in oggetto, ed è destinata essenzialmente al parcheggio di autovetture e allo scarico e carico materiali nell'apposito piazzale antistante l'accesso da Via Tiburtina.

4.3 I prodotti

La P. Gentilini Biscotti Srl produce direttamente fette biscottate e diverse linee di biscotti e commercializza ulteriori prodotti, quali wafer, panettoni, colombe, marmellate e miele realizzati da fornitori terzi. Tutti i prodotti vengono venduti con il marchio Gentilini. Vengono altresì realizzati prodotti a marchio di terzi.

La produzione avviene attraverso l'utilizzo di ricette antiche, pregiate ed uniche, gelosamente custodite e tramandate inalterate dalle varie generazioni sin dal 1890.

La genuinità è garantita dalla scelta e dall'utilizzo di ingredienti naturali accuratamente selezionati. Per la produzione vengono infatti utilizzati soltanto uova e latte freschi, il miele di fioriture spontanee, il burro più cremoso, la farina e lo zucchero di primissima qualità. A questo si aggiungono i minuziosi controlli lungo l'intera filiera produttiva.

Nonostante la presenza di macchinari all'avanguardia presenti nello stabilimento il fattore umano rimane dominante. Nella produzione dei Novellini ancora oggi si utilizzano le trafilè al bronzo che, insieme a mani esperte, fanno sì che non ce ne sia mai uno uguale all'altro.

Il rispetto dei lenti tempi di lavorazione costituisce un'altra componente essenziale nella produzione. Le fette biscottate vengono realizzate, ad esempio, nel pieno rispetto dei più antichi processi artigianali. Sono infatti necessarie ancora oltre 10 ore di lavorazione per ottenere una fetta biscottata.

Per i prodotti commercializzati con il marchio Gentilini, vengono effettuati frequenti controlli per garantire standard qualitativi elevati.



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 21 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

La tradizione artigiana si combina armoniosamente con le nuove tecnologie. Dalla materia prima al prodotto finito ogni attività è costantemente sottoposta a rigorosi controlli che sono alla base del Sistema Qualità Certificato UNI EN ISO 9001:2015 e ISO 22000:2005 che garantiscono un elevatissimo standard qualitativo.

4.4 La filiera

L'affidabilità dei fornitori e la qualità delle materie prime sono da considerarsi fattori distintivi ed imprescindibili per la Società P. Gentilini Biscotti Srl. In merito a standard di conformità sulla sicurezza alimentare, si sottolinea che in Europa esiste una normativa cogente (Reg. 852/04 e 853/04) obbligatoria per tutte le aziende del settore alimentare.

La selezione dei fornitori ed i controlli interni garantiscono standard di qualità, conformi alla politica di approvvigionamento dell'Azienda e al livello qualitativo dei propri prodotti.

Come indicato sopra, la Società P. Gentilini Biscotti Srl si rivolge da sempre a fornitori in grado di garantire alti standard qualitativi, soprattutto per quanto concerne le materie prime, a partire dalla selezione delle farine, degli zuccheri, del burro fino ad arrivare al latte, al miele e agli aromi naturali.

Tutte le fasi del processo di controllo, accettazione e scarico delle materie prime sono monitorate e registrate, rendendo così possibile la futura tracciabilità.

La successiva fase di lavorazione è monitorata da fasi di controllo processo che tengono traccia di tutto il ciclo di lavorazione, dal serbatoio di origine fino al confezionamento del prodotto, registrando tempi di lavorazione, parametri di trattamento e valori quantitativi.

Al termine della fase di lavorazione di ciascun lotto viene effettuato il lavaggio dei macchinari impiegati nel processo produttivo.

Il prodotto finito viene quindi pallettizzato e immediatamente trasferito nei magazzini interni allo stabilimento, in attesa di essere trasferito alla piattaforma logistica di distribuzione finale (esterna all'azienda).

Un software specifico di supervisione e gestione consente a chi effettua la programmazione di mettere in relazione vendite, magazzino e produzione, facendo in modo che la produzione avvenga sulla base delle vendite e dei trend storici e stagionali.

Per garantire la consegna dei suoi prodotti la Società si è dotata di un efficiente sistema logistico distributivo esterno che permette di recapitare in pochissimo tempo dalla produzione e confezionamento i propri prodotti direttamente a tutti i punti vendita.

5 IL SISTEMA DI CORPORATE GOVERNANCE DELLA SOCIETÀ

La Società adotta un sistema di Corporate Governance conforme a quanto delineato dalla legge. Sono organi della Società:

- Assemblea dei Soci;
- Consiglio di Amministrazione
- Presidente del Consiglio di Amministrazione;
- Consigliere/i Delegato/i ove nominato/i
- Direttore Generale ove nominato
- Collegio Sindacale.

5.1 L'Assemblea dei Soci

I Soci decidono sulle materie riservate alla loro competenza dalla legge e dallo statuto, nonché sugli argomenti che uno o più Amministratori o tanti Soci che rappresentino almeno un terzo del capitale sociale sottopongono alla loro approvazione.

Sono attribuite alla competenza dei Soci:

1. Approvazione del bilancio e la distribuzione degli utili;
2. La nomina e la revoca dei membri del Consiglio di Amministrazione e del suo Presidente, e la determinazione del loro compenso;
3. La nomina del Presidente e degli altri membri del Collegio Sindacale, nonché dei Sindaci supplenti, o del revisore.
4. Le modifiche dello statuto sociale;
5. La decisione di compiere operazioni che comportano una sostanziale modificazione dell'oggetto sociale determinato nell'atto costitutivo o una rilevante modificazione dei diritti dei Soci, nonché l'assunzione di partecipazioni da cui derivi responsabilità illimitata per le obbligazioni della Società partecipata;
6. In caso di scioglimento della Società, i Soci nomineranno uno o più liquidatori, determinando:
 - a) Il numero dei liquidatori;
 - b) A chi spetta la rappresentanza della Società;
 - c) I criteri in base ai quali deve svolgersi la liquidazione;
 - d) I poteri, con gli eventuali limiti, dell'organo preposto alla liquidazione.

5.2 Il Consiglio di Amministrazione e il suo Presidente

La società è amministrata da un Consiglio di Amministrazione composto da tre a cinque membri. La nomina del Consiglio di Amministrazione compete ai Soci. I membri del Consiglio di Amministrazione possono essere Soci o non Soci.

Il presidente del Consiglio di Amministrazione esercita i poteri previsti dall'art. 2381, c. I, cc..

Il Consiglio di Amministrazione può delegare proprie attribuzioni ad uno o più Consiglieri. In tal caso si applicano le disposizioni contenute nell'art. 2381, c. III, IV e V, cc..

Il Consiglio si riunisce nella sede sociale o altrove purché in Italia o in un altro Stato membro dell'Unione Europea, quando il Presidente lo giudichi necessario, ovvero su domanda di oltre la metà dei suoi membri o del Collegio Sindacale.

Il Consiglio è convocato dal Presidente con avviso da spedirsi almeno 8 (otto) giorni prima dell'adunanza a ciascun amministratore e sindaco e, nei casi di urgenza, almeno 3 (tre) giorni prima. L'avviso può essere redatto su qualsiasi supporto (cartaceo o magnetico) e può essere spedito con qualsiasi sistema di comunicazione (compresi il telefax e la posta elettronica) che garantisca la prova dell'avvenuto ricevimento. L'avviso deve contenere l'ordine del giorno, nonché il giorno, il luogo e l'ora dell'adunanza.

Per la validità delle deliberazioni del Consiglio si richiede la presenza della maggioranza dei suoi membri in carica.

Le deliberazioni sono prese a maggioranza assoluta di voti dei presenti.

Anche in carenza delle formalità di convocazione stabilite dai commi precedenti, il Consiglio si reputa validamente costituito quando sono presenti tutti i consiglieri in carica ed i Sindaci effettivi, se nominati.

Dalle deliberazioni della seduta si redigerà un verbale firmato dal Presidente e dal Segretario, se nominato, che dovrà essere trascritto nel libro delle decisioni degli Amministratori.

Il Presidente del Consiglio di Amministrazione, ove lo ritenga opportuno, può avvalersi del metodo della consultazione scritta o consenso espresso per iscritto.

Il Consiglio di Amministrazione riserva comunque a sé le seguenti materie:

- investimenti industriali, commerciali e le campagne pubblicitarie di importo superiore a euro 1.000.000 per singolo progetto;
- costituzione di contratti di mutuo a medio e lungo termine per importi superiori a euro 1.000.000;
- costituzione di fidejussioni ed avalli per importi superiori a euro 100.000;
- acquisto e cessioni di partecipazioni in società;
- acquisto, affitto e cessioni di rami di azienda;
- costituzioni di ipoteche sui beni immobili della società;
- acquisti e vendite di immobili anche nella forma del contratto di leasing;
- emissione di cambiali per importi superiori euro 100.000;
- definizione di liti attive e passive ed atti di transazioni per la società di importi superiori a euro 300.000."

La rappresentanza della Società nei confronti dei terzi ed in giudizio e la firma sociale spettano al Presidente del Consiglio di Amministrazione. In caso di assenza o impedimento di quest'ultimo le sue funzioni saranno assunte dal Consigliere Delegato, se nominato, ovvero dal consigliere più anziano.

Il Consiglio di Amministrazione può nominare procuratori alle liti ovvero procuratori per determinati atti ed operazioni o categorie di atti ed operazioni.

5.3 Il Collegio sindacale

Il Collegio Sindacale è composto di 3 (tre) Sindaci effettivi nominati dai Soci, uno dei quali assume le funzioni di Presidente. I Soci nominano altresì due Sindaci supplenti. Tutti i Sindaci devono essere iscritti nel registro dei revisori contabili istituito presso il Ministero di Giustizia.

Il collegio Sindacale esercita anche il controllo contabile sulla Società, salvo il caso in cui i Soci decidano di nominare un revisore.

5.4 Individuazione dei soggetti in posizione apicale

Come in precedenza indicato, il Decreto richiede di individuare i soggetti in posizione apicale.

Fermo restando il dettato normativo di cui all'art. 5 del Decreto e la relativa prassi applicativa, i criteri per individuare tali soggetti possono essere così sintetizzati:

- collocazione gerarchica al vertice della Società o al primo livello di riporto;
- assegnazione di poteri di spesa e di deleghe che consentano di svolgere talune attività, anche verso l'esterno, con un certo margine di autonomia.

I predetti requisiti devono sussistere congiuntamente e non sono alternativi. È pertanto possibile identificare i soggetti apicali avvalendosi dell'organigramma aziendale.

Alla luce dei criteri sopra esposti, allo stato, non risultano soggetti apicali.

5.4.1 Poteri del Consigliere Delegato

Sono conferiti al Consigliere Delegato tutti i poteri per l'amministrazione della Società, ad eccezione di quelli diversamente attribuiti dalla legge, dallo statuto sociale e dalla presente deliberazione. Nell'ambito dei poteri allo stesso conferiti, il Consigliere Delegato, in particolare:

- provvede al controllo della gestione e all'attuazione delle direttive del Consiglio di Amministrazione;
- provvede all'esecuzione delle delibere del Consiglio di Amministrazione;
- provvede alla predisposizione del progetto di bilancio annuale e degli altri documenti contabili periodici (relazioni trimestrali e semestrale), ovvero straordinari, da sottoporre per l'approvazione al Consiglio di Amministrazione;
- definisce l'assetto organizzativo generale della Società, che sottopone all'approvazione del Consiglio di Amministrazione, e provvede alla realizzazione dell'assetto stesso;
- assume e licenzia il personale dirigente e quadri, definisce altresì, gli atti di portata generale riguardanti le modalità di assunzione e la posizione normativa ed economica del personale della società;
- assume determinazioni in merito alle liti attive e passive ed alle transazioni per la società;
- provvede nell'attività di gestione a porre in essere ogni atto in conformità a quanto deliberato dal Consiglio di Amministrazione.

5.4.2 Poteri del Consiglio di Amministrazione

Il Consiglio di Amministrazione riserva comunque a sé le seguenti materie:

- investimenti industriali, commerciali e le campagne pubblicitarie di importo superiore a euro 1.000.000 per singolo progetto;
- costituzione di contratti di mutuo a medio e lungo termine per importi superiori a euro 1.000.000;
- costituzione di fidejussioni ed avalli per importi superiori a euro 100.000;
- acquisto e cessioni di partecipazioni in società;
- acquisto, affitto e cessioni di rami di azienda;
- costituzioni di ipoteche sui beni immobili della società;
- acquisti e vendite di immobili anche nella forma del contratto di leasing;
- emissione di cambiali per importi superiori euro 100.000;
- definizione di liti attive e passive ed atti di transazioni per la società di importi superiori a euro 300.000.

6 I SISTEMI MANAGERIALI RILEVANTI

6.1 Politiche societarie

Sia per scelta strategica, sia in conseguenza del suo posizionamento e della sua visibilità sul territorio regionale, la Società ha sviluppato i propri sistemi manageriali sull'esigenza di prevenire-mitigare l'insorgenza di qualsivoglia rischio reputazionale.

Infatti, tali sistemi sono coerenti con le politiche societarie che richiedono non soltanto l'applicazione più prudentiale e tempestiva delle normative, ma anche la massima attenzione alle metodologie gestionali che garantiscono la qualità del prodotto, dei processi organizzativi, la tutela del consumatore.

Tali politiche si riassumono anche nei seguenti principi adottati formalmente dalla Società:

- consolidare e sviluppare il valore dell'azienda e del marchio;
- promuovere il miglioramento continuo nell'ambito di tutte le attività aziendali;
- rispettare l'ambiente, presidiare la sicurezza e la salute dei lavoratori, garantire la tutela dei consumatori;
- sostenere e valorizzare i rapporti con gli stakeholder e il territorio.

Gli obiettivi che ne derivano sono i seguenti:

- valorizzare il ruolo di "Specialista del Biscotto", garantendo l'offerta di un adeguato mix di tradizione e innovazione;
- adottare tutte le azioni che possono migliorare i parametri qualitativi, produttivi, igienico-sanitari, ambientali, di sicurezza sul lavoro ed etici nelle diverse attività aziendali;
- promuovere lo sviluppo di patti di filiera a tutela del territorio e del consumatore;
- interagire con la società circostante attraverso azioni di marketing sociale.

I Sistemi manageriali adottati dalla Società e di seguito descritti recepiscono pertanto dette petizioni.

6.2 Il sistema organizzativo


Il sistema organizzativo è coerente rispetto ai seguenti principi ispiratori:

- adeguata formalizzazione;
- chiarezza delle linee di dipendenza gerarchica e funzionale;
- pubblicità dei poteri attribuiti, sia all'interno sia all'esterno della Società, per garantirne la conoscibilità;
- chiarezza sul conferimento dei poteri e sulla conseguente allocazione delle responsabilità, così come sulle responsabilità organizzative interne.

Sulla base di quanto sopra, il sistema organizzativo è delineato dal vertice e portato a conoscenza nelle varie articolazioni della struttura tramite Ordini di servizio e Comunicazioni interne, che vengono tempestivamente ed adeguatamente diffuse ai dipendenti.

Nel suo complesso, il sistema organizzativo consta di:

1. **Struttura organizzativa.** È rispecchiata nell'organigramma aziendale, che indica l'articolazione delle funzioni interne ed i relativi responsabili;

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 26 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

2. Sistema delle deleghe (suddivise in deleghe in materia di dirigenza e deleghe in materia di sicurezza), per il quale valgono le considerazioni già svolte;
3. Procedure e Istruzioni operative, che definiscono le modalità operative per lo svolgimento delle diverse attività.

I documenti di cui ai punti precedenti non vengono allegati al presente Modello a causa della loro analiticità e della possibile frequenza di modificazione, ma dato che il Modello vi fa riferimento, vanno considerati sua parte integrante.

L'Organigramma viene mantenuto sempre aggiornato dalla funzione competente e comunicato al personale – anche tramite pubblicazione nell'atrio aziendale – al fine di assicurare una chiara definizione formale dei compiti assegnati ad ogni unità della struttura della Società.

Identica comunicazione dovrà essere inoltrata all'Organismo di Vigilanza (di cui di seguito), anche in caso di variazione delle deleghe, per consentire le valutazioni di competenza di quest'ultimo, al fine di stabilire se le variazioni comportino o meno un'incidenza sulla Parte Generale ovvero sulla Parte Speciale del Modello Organizzativo.

Le procedure e istruzioni operative di cui la Società si è dotata mirano a garantire la correttezza e trasparenza della sua attività, da un lato regolando l'agire della stessa, e dall'altro consentendo i controlli, preventivi e successivi, della correttezza delle operazioni effettuate. Ciò in quanto esse favoriscono l'uniformità di comportamento all'interno dell'azienda, nel rispetto delle disposizioni normative che ne regolano l'attività (in relazione a questo aspetto si rinvia al punto successivo, relativo ai Sistemi di Gestione).

Tutti i dipendenti hanno l'obbligo di essere a conoscenza delle norme procedurali interne di specifico interesse della funzione e di rispettarle nell'esercizio dei compiti loro assegnati.

In caso di sostanziale variazione organizzativa, sarà/saranno la/e funzione/i interessata/e ad informare l'Organismo di Vigilanza affinché quest'ultimo possa effettuare le valutazioni di competenza.

Il costante monitoraggio del sistema organizzativo da parte dell'Organismo di Vigilanza consentirà di adattare nel tempo il Modello alle esigenze specifiche, garantendone la dinamicità.

6.3 I sistemi di gestione

La Società si è dotata di Sistemi di Gestione, che costituiscono un rilevante fattore di mitigazione dei rischi individuati nella Mappa dei rischi (di cui alla Parte Speciale del presente Modello): si tratta del Sistema di Gestione della Qualità UNI EN ISO 9001:2015 che ha il seguente campo di applicazione: "Progettazione, produzione e commercializzazione di prodotti da forno (Biscotti e fette biscottate) e prodotti lievitati da ricorrenza (panettoni, pandori e colombe)" e del Sistema di Gestione UNI EN ISO 22000:2005 che ha il seguente campo di applicazione: "Produzione e confezionamento di prodotti da forno (Biscotti e fette biscottate). Commercializzazione di prodotti lievitati da ricorrenza, prodotti da forno, miele e confetture".

I processi produttivi vengono tenuti sotto controllo dalla Società secondo le modalità previste nello stesso Sistema di Gestione della Qualità e nelle procedure ed istruzioni in esso richiamate.

Tale Sistema di Gestione prevede, tra l'altro, l'effettuazione di audit svolti da un team di personale dipendente, appositamente formato e da consulenti esterni. Gli audit sono sia di prima parte, ovvero sull'azienda stessa, sia di seconda parte, ovvero sui fornitori di beni e servizi.

Inoltre, la tracciabilità del prodotto è assicurata dall'applicazione dell'art. 18 del Regolamento CEE UE 178/2002, cui la Società si attiene.

La Società effettua altresì ulteriori controlli, definiti dai propri piani di campionamento, sui prodotti finiti ricevuti dai fornitori di prodotti a marchio.

6.4 Il sistema di gestione delle risorse umane

Il personale dipendente è inquadrato in base ai seguenti contratti:

- il “contratto collettivo nazionale di lavoro per i lavoratori dell’industria alimentare”, per tutto il personale non dirigente;
- il “contratto collettivo nazionale Dirigenti di aziende produttrici di beni e servizi” per tutti i dirigenti.

Le politiche del personale adottate dalla società si basano, tra l’altro, su una procedura mirata a prevenire casi e situazioni di lavoro irregolare, minorile, di discriminazione, etc.

La selezione del personale avviene nel rispetto di una procedura interna. I candidati vengono selezionati in base alla corrispondenza tra le caratteristiche professionali e personali richieste e quelle possedute.

Adeguata attenzione viene rivolta alla formazione del personale, anch’essa gestita secondo una specifica procedura interna.

6.5 Il sistema informativo

Sono in uso nella Società vari applicativi informatici che supportano l’attività dei principali processi interni.

Per garantire la prevenzione dei delitti informatici di cui al D. Lgs. 231/2001, nonché la conformità a quanto previsto dal D. Lgs. 196/2003, la Società adotta e continuerà ad adottare le seguenti misure previste nel Sistema di Gestione dei Dati Personali (REG. UE 679/2016):

1. Gestione di accessi, account e profili. Con riferimento alla gestione degli accessi:
 - è prevista la definizione formale, individuale ed univoca, dei requisiti di autenticazione ai sistemi per l’accesso ai dati - i codici identificativi (user-id) per l’accesso alle applicazioni ed alla rete;
 - la corretta gestione delle password è definita da linee guida, comunicate a tutti gli utenti per la selezione e l’utilizzo della parola chiave; (no maiuscole-minuscole e numeri)
 - sono definite apposite regole per la creazione delle password di accesso alla rete, delle applicazioni del patrimonio informativo dell’ente e dei sistemi critici o sensibili (ad esempio: lunghezza minima della password, regole di complessità, scadenza, ecc.);
 - sono individuate modalità specifiche per l’assegnazione dell’accesso remoto ai sistemi, sia da parte dei dipendenti sia da parte di soggetti terzi, quali consulenti, fornitori;
 - per quanto concerne l’ambito dei dati sensibili, le applicazioni tengono traccia delle modifiche ai dati compiute dagli utenti.
2. Gestione delle reti di telecomunicazione. Con riferimento alla gestione delle reti, sono effettuate verifiche periodiche sul funzionamento delle reti e sulle anomalie riscontrate.
3. Gestione e sicurezza della documentazione in formato digitale:
 - è regolamentato l’utilizzo della firma digitale nei documenti, disciplinandone responsabilità, livelli autorizzativi, regole di adozione di sistemi di certificazione, eventuale utilizzo ed invio dei documenti, modalità di archiviazione e distruzione degli stessi.
 - vengono effettuate attività di back up dei dati dell’Ente, definendo la frequenza dell’attività, le modalità, il numero di copie ed il periodo di conservazione dei dati;
 - l’accesso ai documenti informatici già archiviati è consentito solo al personale autorizzato.

4. Nell'espletamento delle proprie attività, tutto il personale dipendente di Biscotti P. Gentilini Srl , i collaboratori, i consulenti ed eventuali incaricati di Biscotti P. Gentilini Srl che hanno accesso alla rete aziendale ed ai Sistemi informativi, sono tenuti ad osservare le seguenti linee guida:
- non utilizzare i sistemi informatici aziendali per finalità diverse da quelle richieste per l'espletamento della propria attività lavorativa, ove non sia contemplato dalle policy aziendali l'uso promiscuo del bene, o contraria a quanto previsto dal Codice Etico;
 - evitare l'acquisizione, il possesso e l'utilizzo di software ed hardware, non strettamente necessari per lo svolgimento della propria attività lavorativa, che potrebbero essere adoperati per compromettere la sicurezza dei sistemi informatici;
 - evitare l'accesso ad internet e la navigazione per scopi diversi da quelli strettamente necessari allo svolgimento della propria attività lavorativa;
 - evitare la diffusione di informazioni relative ai sistemi informatici aziendali;
 - non divulgare, fornire o condividere con altri componenti dell'organizzazione o con personale esterno a Biscotti P. Gentilini Srl , le proprie credenziali di accesso alla Rete ed ai sistemi aziendali o informazioni in merito alle procedure di controllo utilizzate da Biscotti P. Gentilini Srl e dai Fornitori per la rete ed i sistemi aziendali.

6.6 Il sistema dei controlli

6.6.1 Principi, requisiti e livelli di controllo

Con il presente Modello la Società tende a migliorare il proprio sistema di controllo interno, in particolare per le attività a rischio individuate e indicate nella Parte Speciale, Mappa dei Rischi, implementando idonei controlli in grado di riportare i rischi emersi ad un livello di accettabilità. Pertanto, la Società si dota di un sistema in grado di:

- accertare l'adeguatezza dei diversi processi organizzativi interni in termini di efficacia, efficienza ed economicità;
- perseguire l'affidabilità e la correttezza delle scritture contabili e la salvaguardia del patrimonio della Società;
- assicurare la conformità degli adempimenti operativi alle normative interne ed esterne ed alle direttive ed indirizzi interni aventi la finalità di garantire una sana ed efficiente gestione.

Vi possono essere tre livelli di controllo:

- Controlli di primo livello: sono controlli operativi e tecnici quali:
 - controlli informatici, segnalazioni di anomalie ed errori, blocco del flusso procedurale, inseriti all'interno di sistemi procedurali informatizzati che consentono la verifica immediata delle elaborazioni e dei dati da parte di chi ne sta effettuando il trattamento;
 - controlli diretti del responsabile organizzativo, che supervisiona la corretta conduzione delle attività.
- Controlli di secondo livello, effettuati da unità diverse da quelle operative e mirati a verificare la regolarità dell'espletamento delle attività ed il rispetto delle procedure. Possono essere effettuati con sistemi informativi automatizzati e rispondono al principio di separatezza delle funzioni.
- Controlli di terzo livello: sono controlli esterni alla funzione, volti ad individuare le anomalie nei processi e le violazioni delle procedure valutando altresì la complessiva funzionalità del sistema dei controlli

interni. Possono essere svolti da soggetti terzi ed indipendenti tra cui l'Organismo di Vigilanza e la Società di Revisione.

A questo sistema di controlli si aggiungono i controlli effettuati da Organismi esterni in modo mirato ed in ambiti specifici. A titolo esemplificativo tali controlli vengono effettuati da NAS, VVF, Agenzia delle Entrate.

Il sistema di controllo interno si sostanzia quindi in:

- "autocontrollo" o "controlli di primo livello", eseguito dalle singole funzioni sui propri processi. Tali attività di controllo sono demandate alla responsabilità primaria degli addetti e costituiscono parte integrante di ogni processo organizzativo interno;
- "controllo di compliance", che comprende i controlli di "secondo" e "terzo" livello, finalizzato a evidenziare e mitigare i rischi di conformità mediante specifiche azioni di monitoraggio.

Il sistema di controllo persegue l'obiettivo di assicurare che siano rispettate le leggi, i regolamenti e le procedure interne, in modo da prevenire la commissione di reati, anche con riferimento alle disposizioni del Decreto. Tale obiettivo viene perseguito mediante:

- la valutazione dell'adeguatezza delle procedure interne a mitigare il "rischio 231", effettuata in sede di redazione della Mappa dei rischi (di cui alla Parte Speciale del presente Modello);
- un costante monitoraggio, da parte dell'Organismo di Vigilanza, della rispondenza ai principi adottati dalla struttura organizzativa interna, nelle sue procedure e nelle attività poste in essere dalle singole funzioni.

Le componenti del Modello organizzativo devono essere integrate con il sistema di controllo interno, implementato dalla Società, che si basa sui seguenti principi ispiratori:

- chiara assunzione di responsabilità, principio in base al quale qualsiasi attività deve fare riferimento ad una persona o funzione che ne detiene la responsabilità. Tale responsabilità deve corrispondere all'autonomia decisionale ed all'autorità conferita;
- separazione di compiti e/o funzioni, principio per il quale ogni operazione rilevante deve svolgersi attraverso fasi diverse (autorizzazione, esecuzione, contabilizzazione, controllo) affidate a soggetti diversi in potenziale contrapposizione di interessi;
- idonea e formale autorizzazione per complessi omogenei di operazioni rilevanti, ovvero per singole operazioni;
- adeguata registrazione e tracciabilità delle operazioni, principio il cui rispetto consente di individuare le caratteristiche e gli attori dell'operazione nelle varie fasi sopra indicate;
- adeguati procedure interne e flussi di reporting atti a rendicontare le operazioni, in particolare se a rischio;
- adeguati controlli "di secondo livello", preventivi o consuntivi, sulla correttezza delle attività attraverso verifiche indipendenti sia da parte di soggetti interni all'organizzazione, ma estranei al processo, sia da parte di soggetti esterni (ad esempio Società di revisione).

Il Sistema di prevenzione deve sostanziarsi nell'adeguatezza e nella conoscibilità delle procedure interne affinché il sistema non possa essere aggirato se non intenzionalmente. Conseguentemente nessuno potrà giustificare la propria condotta adducendo l'ignoranza delle direttive ed il reato non potrà essere causato dall'errore umano (per negligenza o imperizia).

Il Sistema di controllo a consuntivo deve essere in grado di rilevare tempestivamente l'insorgere di anomalie attraverso un adeguato monitoraggio dell'attività svolta.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 30 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

Ciò è in linea con il Decreto, che consente di avvalersi del principio dell'esimente solo in caso di "elusione fraudolenta" per i soggetti apicali; parimenti ed agli stessi fini i controlli interni devono essere implementati in modo tale da garantire in massimo grado l'adempimento degli obblighi di direzione o vigilanza.

6.6.2 Il Controllo sulla gestione economico-finanziaria ed il Controllo Contabile

Le risorse economico-finanziarie sono gestite nel rispetto delle deleghe e sulla base dei documenti programmatici (budget annuale e revisionato) approvati dal Consiglio di Amministrazione nei tempi programmati: sono altresì previsti controlli periodici infrannuali per evidenziare gli scostamenti dalle previsioni e definire gli eventuali interventi correttivi.

Il controllo contabile è esercitato, in ottemperanza a quanto previsto dalla Statuto, dal Collegio Sindacale, così come pure la revisione contabile.

6.7 Il sistema di controllo della salute e sicurezza dei lavoratori

6.7.1 Principi e requisiti

Preliminarmente si specifica che si è provveduto in via sistematica:

- all'identificazione dei rischi ed alla loro valutazione;
- all'individuazione delle misure di prevenzione e di protezione adeguate rispetto ai rischi riscontrati, affinché questi ultimi siano eliminati ovvero, ove ciò non sia possibile, siano ridotti al minimo – e, quindi, gestiti – in relazione alle conoscenze acquisite in base al progresso tecnico;
- alla limitazione al minimo del numero di lavoratori esposti a rischi;
- alla definizione di adeguate misure di protezione collettiva e individuale, fermo restando che le prime devono avere priorità sulle seconde;
- al controllo sanitario dei lavoratori in funzione dei rischi specifici;
- alla programmazione della prevenzione, mirando ad un complesso che integri in modo coerente le condizioni tecniche e produttive dell'ente con l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro, nonché alla successiva realizzazione degli interventi programmati;
- alla formazione, all'addestramento, alla comunicazione ed al coinvolgimento adeguati dei destinatari, nei limiti dei rispettivi ruoli, funzioni e responsabilità, nelle questioni connesse alla SSL;
- alla regolare manutenzione di ambienti, attrezzature, macchine e impianti, con particolare riguardo alla manutenzione dei dispositivi di sicurezza in conformità alle indicazioni dei fabbricanti.

Il sistema prevede la puntuale definizione dei compiti, dei doveri e delle responsabilità spettanti a ciascuna categoria di soggetti coinvolti nel settore della SSL, a partire dal Datore di lavoro fino al singolo lavoratore. In questo senso, sono considerati anche i seguenti profili:

- l'assunzione e la qualificazione del personale;
- l'organizzazione del lavoro e delle postazioni di lavoro;
- l'acquisizione dei beni e dei servizi impiegati dalla Società e la comunicazione delle opportune informazioni a fornitori ed appaltatori;
- la manutenzione ordinaria e straordinaria delle attrezzature, degli impianti, dei mezzi di prevenzione e dei dispositivi di protezione collettiva ed individuale;

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 31 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

- la qualificazione e la scelta dei fornitori e degli appaltatori;
- l'efficiente gestione delle emergenze;
- le modalità da seguire per affrontare le difformità riscontrate rispetto agli obiettivi fissati ed alle previsioni del sistema di controllo.

Inoltre, è stato definito un sistema di flussi informativi che consenta la circolazione delle informazioni all'interno della Società.

Va inoltre rivolta particolare attenzione all'esigenza di predisporre ed implementare, in materia di SSL, un efficace ed efficiente sistema di monitoraggio che, oltre a prevedere la registrazione delle verifiche svolte dalla Società, anche attraverso la redazione di appositi verbali, si sviluppi su un duplice livello, di cui il primo coinvolge tutti i soggetti che operano nell'ambito della struttura organizzativa della Società, ed il secondo è costituito da un controllo esterno affidato all'Organismo di Vigilanza (di cui in seguito).

Per quanto riguarda il controllo di primo livello si rinvia al successivo punto "Monitoraggio", che ne descrive l'attuale articolazione.

Per quanto invece riguarda il secondo livello di monitoraggio, richiamato espressamente dalle Linee Guida di Confindustria, esso deve essere svolto dall'Organismo di Vigilanza, direttamente o tramite soggetti da quest'ultimo delegati.

In ragione della sua idoneità ad assicurare l'obiettività e l'imparzialità dell'operato, nonché l'indipendenza dal settore di lavoro sottoposto a verifica ispettiva, all'Organismo di Vigilanza è assegnato il compito di verificare la funzionalità del complessivo sistema preventivo adottato dalla Società a tutela della salute e della sicurezza dei lavoratori.

Al fine di consentire all'Organismo di Vigilanza di svolgere efficacemente il monitoraggio di secondo livello, è obbligatorio inviare allo stesso copia della reportistica periodica in materia di salute e sicurezza sul lavoro, e segnatamente il verbale della riunione periodica di cui all'art. 35 D. Lgs. n. 81/2008, nonché tutti i dati relativi agli infortuni sul lavoro occorsi nei siti della Società.

I risultati del monitoraggio sono considerati dall'Organismo di Vigilanza ai fini:

- dell'eventuale relazione al Consiglio di Amministrazione per proposte di aggiornamento del Modello, incluso il sistema preventivo adottato dalla Società e le procedure organizzative, in ragione di eventuali inadeguatezze o significative violazioni riscontrate, ovvero di cambiamenti della struttura organizzativa della Società;
- dell'eventuale relazione agli organi/funzioni interne competenti per proposte di irrogazione di sanzioni disciplinari, per l'ipotesi in cui sia riscontrata la tenuta delle condotte indicate nel sistema disciplinare adottato dall'ente ai sensi del Decreto.

Tale complessivo sistema dei controlli applicabili alle attività a rischio, in relazione ai reati in materia di sicurezza e salute nei luoghi di lavoro, è stato definito utilizzando, tra l'altro, le indicazioni contenute nell'art. 30 D. Lgs. n. 81/2008.

6.7.2 Organizzazione e ruoli del Servizio Prevenzione e Protezione

Allo stato attuale, il Servizio di Prevenzione e Protezione istituito presso la Società è gestito da personale dipendente, con il supporto di consulenti esterni, ed è così articolato:

- Datore di lavoro (Consigliere Delegato);
- Responsabile Servizio Prevenzione e Protezione (RSPP), incarico affidato ad un consulente esterno;

- Dirigenti (corrispondenti al personale inquadrato con il CCNL “Dirigenti di Aziende produttrici di beni e servizi”);
- Preposti;
- Rappresentante Lavoratori per la Sicurezza (RLS), individuato – come da norma – all’interno delle RSU;
- Squadra integrata di “Addetti primo soccorso” ed “Addetti prevenzione incendi;
- Medico competente.

Al fine di prevenire e mitigare i rischi connessi alla sicurezza sul lavoro, la Società impiega criteri prudenziali di qualificazione del personale e principalmente:

- tutti i dirigenti, gli impiegati ed alcuni tecnici (in funzione dell’attività svolta) sono classificati “video terminalisti”, con l’applicazione della conseguente sorveglianza sanitaria e formazione specifica;

6.7.2.1 Nomina del Datore di lavoro

Per quanto attiene al Datore di lavoro, questi è nominato dal Consiglio di Amministrazione con la delega di cui al precedente punto “Poteri del Consigliere Delegato”, cui si rinvia.

6.7.2.2 Nomina del Responsabile del Servizio Prevenzione e Protezione

Il RSPP (consulente esterno) è nominato dal Datore di lavoro per l’assolvimento dei seguenti obblighi:

- individuare i Dispositivi di Protezione Individuale da fornire al personale;
- consentire ai lavoratori di verificare, mediante il Rappresentante dei Lavoratori per la Sicurezza, l’applicazione delle misure di sicurezza e protezione della salute;
- consegnare tempestivamente al Rappresentante dei Lavoratori per la Sicurezza, su richiesta di questi e per l’espletamento della sua funzione, copia del documento di cui all’art. 17, lettera a), del D. Lgs. 81/2008;
- elaborare il documento di cui all’art. 26, comma 3 e su richiesta di questi e per l’espletamento della sua funzione, consegnarne tempestivamente copia al Rappresentante dei Lavoratori per la Sicurezza;
- consultare il Rappresentante dei Lavoratori per la Sicurezza secondo le disposizioni dell’art. 50 del D. Lgs. 81/2008;
- convocare la riunione periodica di cui all’art. 35 del D. Lgs. 81/2008;
- aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;

Per eventuali necessità di spesa l’RSPP dovrà sottoporre un relativo piano di spesa al Consigliere Delegato.

6.7.2.3 Nomina dei Dirigenti (del Servizio Prevenzione e Protezione)

Premesso che il D. Lgs. 81/2008 definisce il dirigente come “persona che, in ragione delle competenze professionali e di poteri gerarchici e funzionali adeguati, alla natura dell’incarico conferitogli, attua le direttive del Datore di lavoro organizzando l’attività lavorativa e vigilando su di essa”, allo stato tali Dirigenti sono:

- il Direttore Amministrazione, Finanza e Controllo

Le deleghe conferite ai sopra citati Dirigenti prevedono i seguenti obblighi e poteri:

- nell'affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza;
- vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità;
- prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;
- richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione, con l'impegno a formalizzare il Responsabile Risorse Umane eventuali comportamenti difformi;
- adempiere agli obblighi di informazione, formazione e addestramento di cui all'art.73 del D. Lgs. 81/2008;
- adottare le misure necessarie al fine di ridurre i rischi connessi all'uso delle attrezzature di lavoro, e per impedire che le stesse possano essere utilizzate per operazioni e secondo condizioni per le quali non sono adatte;
- adottare le misure necessarie affinché le attrezzature di lavoro siano oggetto di idonea manutenzione al fine di garantire nel tempo la permanenza dei requisiti di sicurezza di cui all'art. 70 del D. Lgs. 81/2008, e siano corredate, ove necessario, da apposite istruzioni d'uso e libretto di manutenzione;
- fornire al servizio di prevenzione e protezione ed al medico competente le necessarie informazioni in merito a: a) organizzazione del lavoro, programmazione e attuazione delle misure preventive e protettive; b) descrizione degli impianti e dei processi produttivi.

Il Dirigente è altresì tenuto a vigilare in ordine all'adempimento degli obblighi di cui agli articoli 19, 20, 22, 23, 24 e 25 del D. Lgs. 81/2008, ferma restando l'esclusiva responsabilità dei soggetti obbligati ai sensi dei medesimi articoli, qualora la mancata attuazione dei predetti obblighi sia addebitabile unicamente agli stessi e non sia riscontrabile un difetto di vigilanza da parte del Dirigente.

Per eventuali necessità di spesa il Dirigente dovrà sottoporre un relativo piano di spesa al Consigliere Delegato.

Per quanto riguarda inoltre il Direttore Organizzazione e Risorse Umane, la delega prevede i seguenti obblighi ulteriori, in relazione a tutto il personale dipendente dell'Azienda:

- pianificare e verificare l'adempimento degli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37 del D. Lgs. 81/2008;
- garantire gli adempimenti di legge nei confronti dell'INAIL, oltre a consentire al RLS di accedere ai dati relativi agli eventi infortunistici;
- fornire tempestivamente ai dirigenti delegati il giudizio di idoneità alla mansione dei lavoratori visitati a cura del medico competente.

6.7.3 Monitoraggio

Il sistema di monitoraggio attualmente adottato dalla Società coinvolge tutti i soggetti che operano nell'ambito della struttura organizzativa, prevedendo:

- l'auto-controllo da parte dei lavoratori, i quali devono sia utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto, nonché i dispositivi di sicurezza e di protezione messi a loro disposizione, sia segnalare immediatamente le deficienze di tali mezzi e dispositivi nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza;

- il coinvolgimento diretto e costante dei soggetti con specifici compiti in materia di SSL (ad esempio, Datore di lavoro, RSPP, Dirigenti), i quali intervengono, tra l'altro, in materia:
 - di vigilanza e monitoraggio periodici e sistematici sull'osservanza degli obblighi di legge e delle procedure in materia di SSL;
 - di segnalazione di eventuali deficienze e problematiche;
 - di individuazione e valutazione dei fattori di rischio nell'ambito dell'organizzazione in cui i lavoratori prestano la propria attività;
 - di elaborazione delle misure preventive e protettive attuate e richiamate nel Documento di Valutazione dei Rischi, nonché dei sistemi di controllo di tali misure;
 - di proposizione dei programmi di formazione e addestramento dei lavoratori, nonché di comunicazione e coinvolgimento degli stessi.

In proposito, si evidenzia che la Società si è dotata di una procedura specifica, che gestisce la programmazione degli interventi di manutenzione e la relativa effettuazione, con l'acquisizione dei documenti attestanti la realizzazione di dette attività. È previsto che tali documenti debbano essere firmati dallo/dagli operatore/i. Nei casi più rilevanti (ad esempio in relazione agli impianti di confezionamento), è previsto che i controlli debbano essere effettuati congiuntamente da due risorse.

È previsto che, in particolare per quanto riguarda gli impianti antincendio, siano rilasciate apposite relazioni che descrivono la situazione in essere e potenziali situazioni critiche.

7 I PROTOCOLLI

7.1 Premessa

I protocolli seguenti esprimono i fondamentali principi di comportamento e/o di controllo, da integrare nel complessivo Sistema di Gestione, per lo svolgimento di specifiche attività a rischio di commissione di reati presupposto. Tali principi costituiscono pertanto altrettanti elementi che devono essere recepiti nelle procedure e nelle attività aziendali.

7.2 Il Protocollo SSL

7.2.1 Attività di valutazione dei rischi e predisposizione delle misure di prevenzione e protezione

Tutti i rischi cui sono esposti i lavoratori, a causa ed in occasione dello svolgimento delle mansioni attribuite, devono essere oggetto di attenta valutazione.

Il Documento di Valutazione dei Rischi (DVR) deve essere predisposto, approvato ed attuato e, necessariamente, deve contenere:

- una relazione sulla valutazione dei rischi per la sicurezza e la salute connessi all'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;
- l'indicazione delle misure di prevenzione e protezione attuate e dei dispositivi di protezione individuale adottati a seguito della valutazione dei rischi;
- il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;

- l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione all'interno della Società che debbono provvedere;
- l'indicazione del nominativo del Responsabile del Servizio di Prevenzione e Protezione (RSPP) e del Medico competente che ha partecipato alla valutazione del rischio.
- l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Il DVR deve altresì rispettare le indicazioni previste da norme specifiche sulla valutazione dei rischi ove concretamente applicabili.

Il Rappresentante dei Lavoratori per la Sicurezza (RLS), ai fini della redazione del DVR, deve essere in ogni caso previamente consultato.

Il DVR deve essere custodito presso l'unità produttiva o il cantiere a cui si riferisce la valutazione dei rischi ed essere aggiornato costantemente in relazione ai mutamenti organizzativi o produttivi rilevanti ai fini della sicurezza e della salute dei lavoratori.

Il DVR è disponibile presso l'ufficio dell'RSPP e messo a disposizione di chiunque volesse consultarlo. Le misure di prevenzione e protezione adottate devono essere appropriate ed idonee a presidiare i rischi individuati nel DVR.

Le misure di prevenzione e protezione devono essere aggiornate in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e della sicurezza sul lavoro ovvero in relazione al grado di evoluzione della tecnica della prevenzione e della protezione.

Sentito il RSPP, idonei Dispositivi di Protezione Individuale (DPI) devono essere forniti ai lavoratori.

La consegna dei DPI deve essere adeguatamente formalizzata e registrata. I DPI devono essere sottoposti a manutenzione periodica ovvero tempestivamente sostituiti laddove non siano più idonei a garantire adeguata protezione del lavoratore. L'attività di valutazione dei rischi e la predisposizione delle misure di prevenzione e protezione devono essere documentate, tracciate e conservate.

7.2.2 Standard tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, movimentazioni carichi, etc.

Le specifiche procedure adottate devono essere finalizzate a garantire la sicurezza degli impianti, delle attrezzature e dei luoghi di lavoro; in particolare esistono delle indicazioni, prassi e registrazioni per la gestione dei seguenti processi:

- la manutenzione, la pulitura ed il controllo periodico dei luoghi, degli impianti e delle attrezzature di lavoro;
- le norme generali d'igiene nelle aree di lavoro e nelle aree operative;
- le vie di circolazione e le uscite di emergenza;
- i dispositivi antincendio;
- la fuoruscita di sostanze liquide e gassose;
- le misure di primo soccorso;
- l'utilizzo e la manutenzione dei DPI;
- le modalità di archiviazione e di stoccaggio di prodotti e merci.

La manutenzione e le attività di controllo devono essere documentate e archiviate.

Le procedure finalizzate a garantire la sicurezza dei lavoratori debbono essere adottate con riferimento all'esposizione a specifici rischi tra cui:

- videoterminali;
- agenti fisici;
- agenti chimici;
- agenti biologici;
- agenti cancerogeni;
- movimentazione manuale dei carichi.

Tutta l'attività deve essere documentata e tracciata; i relativi documenti devono essere adeguatamente conservati.

7.2.3 Gestione delle emergenze

I piani di intervento, per far fronte a situazioni di emergenza e di pericolo grave per i lavoratori (es. evacuazione, pronto soccorso, gestione incendi, zone di pericolo, etc.), devono essere individuati. La gestione delle cassette di pronto soccorso o dei kit di primo soccorso, con indicazione dei ruoli e delle funzioni, all'interno dei cantieri, deve essere specificatamente regolamentata.

Il materiale di primo soccorso deve essere costantemente reintegrato in modo tale da garantire in ogni momento la completa ed efficace composizione delle dotazioni. I presidi antincendio devono essere allestiti e devono essere idonei ad evitare l'insorgere di un incendio ed a fronteggiare eventuali situazioni di emergenza, ovvero a limitarne le conseguenze qualora esso si verifichi.

I presidi antincendio devono essere soggetti a controlli periodici e sottoposti ad idonea manutenzione. Il piano di evacuazione deve essere predisposto, attraverso la programmazione degli interventi e l'adozione di provvedimenti/istruzioni, affinché i lavoratori possano, in caso di pericolo grave ed immediato che non può essere evitato, cessare la loro attività ovvero mettersi al sicuro abbandonando, immediatamente, il luogo di lavoro.

Tutta l'attività di gestione delle emergenze (es. prove di evacuazione, controlli sui presidi antincendio, etc.) deve essere documentata, tracciata e conservata.

7.2.4 Aspetti organizzativi (deleghe, nomine di RSPP, RLS, budget e spese)

I soggetti destinatari di deleghe nel settore della sicurezza e salute dei lavoratori o comunque coloro cui sono attribuite specifiche responsabilità in materia devono essere formalmente individuati.

L'idoneità tecnica e professionale dei soggetti interni od esterni, cui sono demandati gli adempimenti in materia di sicurezza e salute dei lavoratori, ivi compresa la manutenzione degli impianti, delle attrezzature, dei luoghi di lavoro e dei DPI, deve essere preventivamente verificata.

Nell'ipotesi di affidamento di lavori a soggetti terzi, (imprese appaltatrici e/o lavoratori autonomi), i costi per la sicurezza e salute dei lavoratori devono essere oggetto di apposito ed adeguato budget.

L'affidamento dei lavori a soggetti terzi impone la necessità di cooperazione e di coordinamento, nell'attuazione di misure di prevenzione e protezione dai rischi sul lavoro, nonché dai rischi derivanti dalle interferenze tra i lavori delle diverse imprese coinvolte, nell'esecuzione dell'opera complessiva.

Poteri di spesa adeguati, a far fronte alle esigenze di sicurezza e salute dei lavoratori, conformemente alla struttura e all'organizzazione della realtà della Società complessivamente intesa ovvero dei singoli settori o unità organizzative, vengono conferiti al Consigliere Delegato.

Nei casi di pericolo imminente ed urgenza deve essere espressamente prevista la possibilità, per il soggetto delegato, di adottare tutte le misure necessarie ad evitare danni alle persone o alle cose a prescindere dal limite di spesa, salvo darne comunicazione al Datore di Lavoro.

Un budget destinato alla sicurezza e salute dei lavoratori, conformemente alla struttura e all'organizzazione della realtà della Società complessivamente intesa ovvero dei singoli settori o unità organizzative, deve essere annualmente previsto.

Nei casi di pericolo imminente ed urgenza deve essere espressamente prevista una procedura che consenta di operare anche oltre i limiti del budget predefinito, purché la richiesta di spese extra budget sia adeguatamente e formalmente motivata.

Tutti i documenti relativi al sistema organizzativo in materia di sicurezza e salute (deleghe/procure, organigramma, mansionari, report, etc.) devono essere aggiornati e conservati.

7.2.5 Sorveglianza sanitaria

Un programma generale di accertamenti periodici per verificare lo stato di salute e l'idoneità dei lavoratori, allo svolgimento della mansione affidata, deve essere elaborato.

Un programma di accertamenti periodici per i lavoratori, esposti a rischi specifici, deve essere elaborato.

Uno specifico canale di informazione, verso i singoli lavoratori finalizzato a comunicare tempestivamente il programma individuale di visite, deve essere istituito.

Adeguate misure, nel caso in cui il lavoratore, tempestivamente avvisato, non si sottoponesse alla visita periodica programmata, devono essere previste.

Laddove, a seguito dell'accertamento sanitario, il lavoratore risultasse inidoneo o parzialmente idoneo a svolgere la mansione affidatagli, è assicurata allo stesso la possibilità di prestare la propria attività lavorativa in termini conformi al proprio stato di salute, qualora fosse possibile nel rispetto da un lato delle esigenze interne e dall'altro della normativa vigente.

Gli incontri periodici con il RSPP devono essere pianificati in base ai bisogni rilevati.

Tutta l'attività relativa alla sorveglianza sanitaria deve essere documentata, tracciata e conservata.

7.2.6 Informazione e formazione dei lavoratori

Specifici corsi di formazione aventi ad oggetto la sicurezza e salute dei lavoratori, devono essere organizzati. I corsi di formazione hanno carattere periodico e sono soggetti ad una programmazione annuale (ivi compresi corsi di formazione per i neoassunti). I corsi di formazione devono avere ad oggetto:

- i rischi specifici cui sono esposti i lavoratori in funzione delle mansioni svolte;
- il corretto utilizzo di macchine, attrezzature e dispositivi di protezione individuale;
- le misure di prevenzione e protezione adottate dall'Ente;
- processi produttivi;
- schemi organizzativi;
- norme interne e procedure operative;
- piani di emergenza.

Un sistema di rilevazione delle presenze idoneo a monitorare che la formazione coinvolga tutti i dipendenti, deve essere elaborato.

Specifiche forme di verifica, finalizzate a verificare il grado di apprendimento dei partecipanti, deve essere somministrato al termine del corso di formazione. Ove la verifica di apprendimento dovesse risultare insufficiente devono essere organizzati corsi di formazione di “recupero”.

I lavoratori devono essere informati circa i soggetti responsabili in materia di sicurezza e salute o chiunque altro abbia incarichi specifici al riguardo nonché le modalità di comunicazione con questi ultimi.

Specifici canali di informazione che consentano ai lavoratori, ovvero ai loro rappresentanti, di prospettare eventuali questioni afferenti la sicurezza e salute, devono essere predisposti.

Una opportuna comunicazione deve essere prevista ed altresì rivolta, ai soggetti che occasionalmente accedono presso i luoghi di lavoro ed in particolare al:

- personale esterno (fornitori, committenti, collaboratori esterni);
- pubblico (clienti, visitatori, etc.);
- alle autorità.

Tutta l'attività di formazione ed informazione deve essere documentata, tracciata e conservata.

7.2.7 Attività di vigilanza e controllo

Un piano di verifica annuale, finalizzato a verificare l'adeguatezza dei presidi antinfortunistici, deve essere previsto.

Un piano correttivo qualora, a seguito delle verifiche effettuate, emergessero carenze o, comunque, margini di miglioramento, deve essere definito. Tutte le persone (delegati e preposti) che coordinano l'attività di altri lavoratori devono costantemente verificare:

- la presenza e l'adeguatezza delle misure di prevenzione e protezione;
- il corretto utilizzo dei mezzi di prevenzione e protezione, ove previsti;
- l'adeguatezza nel tempo delle procedure/piani di intervento adottati per la prevenzione infortuni;
- che ai lavoratori siano stati forniti adeguati DPI in relazione alla specifica attività cui sono assegnati;
- che gli stessi utilizzino correttamente i DPI in relazione alla specifica attività cui sono assegnati.

Le segnalazioni fatte dai RLS (Rappresentanti dei Lavoratori per la Sicurezza) devono essere adeguatamente considerate. Qualora, a seguito delle segnalazioni effettuate dai RLS, si ritenessero non necessari interventi correttivi deve essere fornita idonea motivazione a margine della richiesta stessa.

Tutta l'attività di vigilanza e controllo deve essere documentata, tracciata e conservata.

7.2.8 Sistema sanzionatorio

Il non corretto utilizzo dei mezzi di prevenzione e protezione per colpa grave, nonché il mancato utilizzo dei DPI da parte dei lavoratori deve essere specificatamente sanzionato.

Apposite sanzioni per la violazione dei protocolli adottati dalla Società in materia di sicurezza e salute dei lavoratori, devono essere espressamente previste nel sistema sanzionatorio, elaborato a norma del D. Lgs. n. 231/01.

7.3 Protocollo per la gestione della contabilità e la formazione del bilancio

Il presente protocollo ha l'obiettivo di definire i ruoli, le responsabilità operative, i principi di comportamento e di controllo della Società per la gestione della contabilità generale e la predisposizione del bilancio d'esercizio, in conformità con quanto previsto dal D. Lgs. 231/2001.

Quanto definito dal presente protocollo è volto a garantire il rispetto della normativa vigente e dei principi di trasparenza, competenza, correttezza, veridicità, oggettività e tracciabilità nell'esecuzione delle attività inerenti alla gestione della contabilità e della formazione del bilancio.

Il processo di gestione della contabilità e della predisposizione del Bilancio d'esercizio prevede il coinvolgimento secondo le rispettive competenze, di:

- Consiglio di Amministrazione, che provvede all'approvazione del bilancio, approva i criteri di valutazione proposti dal Consigliere Delegato;
- Il Consigliere Delegato, che definisce la documentazione necessaria alla determinazione delle componenti valutative, assicura la corretta applicazione dei Principi Contabili applicabili e della normativa di riferimento. Gestisce i rapporti con l'Organo di controllo, presentando il bilancio d'esercizio preventivamente rispetto al momento in cui sarà sottoposto all'approvazione del Consiglio di Amministrazione. In occasione della seduta del Consiglio di Amministrazione, illustra il Bilancio d'esercizio e lo sottopone all'approvazione del Consiglio di Amministrazione.
- Addetti contabili, che provvedono alla contabilizzazione dei fatti contabili, all'aggiornamento dei registri e dei libri obbligatori di natura contabile ed alla conservazione della documentazione al fine di garantire la tracciabilità delle operazioni svolte; archiviano, controllano e conservano i registri contabili obbligatori (Libro giornale, Libro inventari, Registri IVA, Registro dei beni ammortizzabili), verificano la correttezza di tutti i movimenti IVA, provvedono alla tenuta del Registro IVA e alla liquidazione periodica della stessa.

La tenuta della contabilità e predisposizione del Bilancio deve articolarsi nelle seguenti attività:

A. tenuta della contabilità generale, la quale ricomprende:

- gestione e manutenzione del Piano dei Conti;
- tenuta dei libri contabili obbligatori;
- registrazione e archiviazione delle fatture passive;
- emissione e registrazione delle fatture attive;
- gestione della contabilità generale e altri aspetti contabili (gestione delle operazioni straordinarie sul patrimonio aziendale, gestione della fiscalità, etc.);

B. bilancio d'esercizio, che a sua volta si suddivide in:

- chiusura del periodo contabile ordinario;
- raccolta ed elaborazione dei dati contabili di chiusura;
- valutazione e stima delle poste del bilancio;
- predisposizione del progetto di bilancio;
- approvazione del progetto di bilancio annuale.

Le modalità operative per la gestione delle suddette attività, laddove si renderà necessaria, potranno essere disciplinate nell'ambito di ulteriore apposita normativa interna di dettaglio, che dovrà essere sviluppata ed aggiornata a cura dell'ente.

Il sistema di controllo a presidio del processo in oggetto si basa su i seguenti elementi qualificanti a garanzia dell'oggettività e trasparenza delle scelte effettuate:

- Livelli autorizzativi definiti e Separazione delle funzioni;
- Controllo e monitoraggio specifico;
- Tracciabilità delle operazioni e archiviazione.

7.3.1 Livelli autorizzativi definiti e separazione delle funzioni

Il processo di tenuta della contabilità e predisposizione del Bilancio è articolato in varie attività che prevedono l'intervento di soggetti diversi nelle differenti fasi del processo, a garanzia del principio secondo cui nessuno può gestire in autonomia un intero processo, ed in particolare, nel rispetto dei ruoli e responsabilità.

Tutti i soggetti coinvolti nel processo di tenuta della contabilità e della predisposizione del Bilancio di esercizio sono responsabili della completezza ed accuratezza delle informazioni fornite.

Il livello di responsabilità è commisurato ai ruoli e ai compiti effettivamente svolti e presuppongono una chiara formalizzazione dei livelli autorizzativi per la tenuta della contabilità e la predisposizione del Bilancio coerenti con il sistema dei poteri aziendali, tale per cui:

- si prevede la possibilità di effettuare registrazioni contabili limitatamente alle sole risorse dell'Ufficio amministrativo, autorizzate attraverso un sistema di User Id e Password aggiornate periodicamente secondo le vigenti norme sulla sicurezza;
- la gestione del Piano dei conti e i relativi inserimenti/modifiche/eliminazioni di conti contabili è affidata esclusivamente al Direttore Amministrazione, Finanza e Controllo o a personale dell'Ufficio amministrativo previa autorizzazione formale. Il Direttore Amministrazione, Finanza e Controllo autorizza le ulteriori registrazioni da effettuare successivamente alla chiusura della contabilità;
- il Direttore Amministrazione, Finanza e Controllo, supportato dall'Ufficio amministrativo, redige il Bilancio d'esercizio, da sottoporre a verifica e approvazione del Consiglio di Amministrazione.
- il Consiglio di Amministrazione approva il Bilancio d'esercizio nel suo complesso.

7.3.2 Controllo e monitoraggio specifico

Il sistema informativo contabile è dotato dei requisiti necessari ad assicurare il rispetto delle regole di sicurezza, di segregazione delle funzioni e di tracciabilità delle operazioni registrate.

Il sistema informativo utilizzato mantiene traccia dell'operatore che ha effettuato la registrazione contabile.

Nel sistema contabile sono definiti campi obbligatori per le transazioni (data registrazione, data contabile, importo, ecc.) al fine di assicurare che le transazioni incomplete non vengano registrate.

Inoltre, le regole di validazione del sistema contabile non permettono di inserire registrazioni non quadrate.

L'attività di registrazione contabile prevede che ogni operazione sia supportata da adeguata documentazione al fine di rendere dimostrabili i principi di inerenza e competenza ed assicurare che ogni operazione sia correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua.

Per quanto concerne la registrazione delle fatture passive, all'arrivo della fattura, i dipendenti dell'ufficio amministrativo effettuano la verifica della corrispondenza con la prestazione/fornitura ricevuta, l'ordine di acquisto e la fattura stessa. In caso di prestazione/materiale non conforme, sentito il referente dell'acquisto per eventuali chiarimenti in merito, richiede al fornitore l'emissione di una nota credito parziale o totale.

7.3.3 Tracciabilità delle operazioni e archiviazione



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 41 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

Tutta la documentazione prodotta a supporto dell'alimentazione della contabilità generale e della predisposizione del Bilancio d'esercizio è archiviata e conservata ai sensi di legge presso l'Ufficio amministrativo.

Gli addetti all'Ufficio amministrativo incaricati all'archiviazione provvedono alla conservazione della documentazione relativa alla tenuta della contabilità al fine di garantire la tracciabilità delle operazioni svolte.

Per quanto attiene alla registrazione delle fatture passive, gli addetti all'Ufficio amministrativo provvedono alla timbratura delle fatture con le seguenti informazioni: numero di protocollo, conto di addebito, conto di accredito, data registrazione.

Gli originali delle fatture sono conservati nell'archivio delle fatture passive.

I registri contabili obbligatori sono conservati presso gli archivi dell'Ufficio amministrativo nei termini previsti dalla legge.

Il Direttore Amministrazione, Finanza e Controllo e i soggetti coinvolti nel processo, ciascuno per la parte di propria competenza, provvedono alla conservazione della documentazione relativa alla chiusura contabile ordinaria al fine di garantire la tracciabilità delle operazioni svolte.

7.3.4 Criteri di comportamento

I soggetti che sono coinvolti nella tenuta della contabilità e predisposizione del Bilancio, sono tenuti ad osservare le previsioni del presente Modello nonché le modalità esposte nel presente protocollo e le disposizioni di legge esistenti in materia.

In particolare, nello svolgimento dei compiti assegnati, gli addetti all'Ufficio amministrativo devono attenersi ai seguenti principi di comportamento:

- assicurare che ogni operazione sia, oltre che correttamente registrata, anche autorizzata, verificabile, legittima, coerente e congrua;
- garantire un continuo allineamento tra i profili utente assegnati ed il ruolo ricoperto all'interno dell'ente, assicurando il rispetto delle regole di segregazione dei compiti tra il soggetto che ha effettuato l'operazione, chi la registra in contabilità e chi effettua il relativo controllo;
- garantire la completa tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte, archiviando in maniera corretta e dettagliata i documenti di supporto;
- osservare, nello svolgimento delle attività di contabilizzazione dei fatti relativi alla gestione dell'ente, un comportamento corretto, trasparente e collaborativo;
- procedere alla valutazione e registrazione di elementi economico patrimoniali nel rispetto dei criteri di ragionevolezza e prudenza, illustrando con chiarezza, nella relativa documentazione, i criteri che hanno guidato la determinazione del valore del bene;

Nella predisposizione del Bilancio di esercizio i soggetti coinvolti nel processo:

- devono rispettare puntualmente i principi contabili di riferimento;
- nel procedimento di stima devono attenersi al rispetto del principio di ragionevolezza ed esporre con chiarezza i parametri di valutazione seguiti, fornendo ogni informazione complementare che sia necessaria a garantire la veridicità del documento;
- predisporre un Bilancio nel rispetto del criterio di completezza sotto il profilo dell'informazione societaria contenenti tutti gli elementi richiesti dalla legge;

- sono tenuti a predisporre la relativa documentazione con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando, e comunque segnalando nella forma e nei modi idonei, situazioni di conflitto d'interesse;
- devono consentire la tracciabilità dell'iter decisionale, autorizzativo e delle attività di controllo svolte;
- sono tenuti ad osservare scrupolosamente tutte le norme di legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere;
- assicurano il regolare funzionamento dell'ente e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge;
- devono tenere un comportamento corretto, trasparente e collaborativo nei confronti dell'Organo di controllo allo scopo di permettergli l'espletamento delle attività attribuitegli ex lege soddisfacendo in modo tempestivo e completo le richieste di documentazione avanzate da quest'ultimo nel corso delle attività di verifica;
- In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:
 - porre in essere attività e/o operazioni volte a creare disponibilità extracontabili, ovvero finalizzate alla creazione di "fondi neri" o di "contabilità parallele", anche se per valori inferiori alle soglie di punibilità di cui agli artt. 2621 e 2622 c.c.;
 - porre in essere azioni finalizzate a fornire informazioni fuorvianti non fornendo una corretta rappresentazione della situazione economica, patrimoniale e finanziaria dell'ente;
 - predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta e veritiera della realtà riguardo alla situazione economica, patrimoniale e finanziaria;
 - alterare o distruggere documenti ed informazioni finanziarie e contabili disponibili in rete attraverso accessi non autorizzati o altre azioni idonee allo scopo;
 - omettere di comunicare dati e informazioni imposte dalla legge riguardo alla situazione economica, patrimoniale e finanziaria;
 - ledere l'integrità del patrimonio, in violazione delle disposizioni di legge a tutela dei creditori;
 - occultare documenti ed informazioni richieste dall'Organo di controllo;
 - fornire documenti ed informazioni incompleti o fuorvianti;
 - ostacolare in qualsiasi modo lo svolgimento dell'attività di controllo da parte degli organi di controllo in genere;

7.4 Protocolli in materia di delitti informatici

7.4.1 Delitti informatici

Trattandosi di reati riferibili generalmente alle modalità con le quali vengono non solo realizzate le attività specifiche dell'azienda ma anche la gestione della medesima, è evidente che il rischio di commissione dell'illecito è astrattamente configurabile in qualunque contesto aziendale. È opportuna pertanto la definizione di standard di comportamento condivisi cui dare ampia diffusione all'interno del contesto aziendale al fine di evitare il rischio della commissione dei suddetti reati.

Per comodità di analisi i delitti informatici possono essere raggruppati nelle seguenti cinque tipologie di reato:

1. Le falsità: documenti informatici (art. 491-bis. c.p.).
2. Delitti contro l'inviolabilità del domicilio: accesso abusivo a un sistema informatico o telematico (art. 615-ter c.p.); detenzione o diffusione abusiva di codici di accesso a sistemi informatici a telematici (art. 615-quater c.p.); diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.).
3. Delitti contro l'inviolabilità dei segreti: intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater); installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies).
4. Delitti contro il patrimonio mediante violenza alle cose o alle persone: danneggiamento di informazioni, dati e programmi informatici (art. 635-bis); danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter); danneggiamento di sistemi informatici o telematici (art. 635-quater); danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies)
5. Delitti contro il patrimonio mediante frode: frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies).

Si tratta dei seguenti reati previsti dal Codice Penale:

- Falsità materiale commessa dal pubblico ufficiale in atti pubblici
- Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative
- Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti
- Falsità ideologica commessa dal pubblico ufficiale in atti pubblici
- Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative
- Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità
- Falsità ideologica commessa dal privato in atto pubblico
- Falsità in registri e notificazioni
- Falsità in scrittura privata
- Falsità in foglio firmato in bianco. Atto privato
- Falsità in foglio firmato in bianco. Atto pubblico
- Altre falsità in foglio firmato in bianco
- Uso di atto falso
- Soppressione, distruzione e occultamento di atti veri
- Copie autentiche che tengono luogo degli originali mancanti
- Falsità commesse da pubblici impiegati incaricati di un servizio pubblico
- Accesso abusivo ad un sistema informatico o telematico
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche
- Danneggiamento di informazioni, dati e programmi informatici
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
- Danneggiamento di sistemi informatici o telematici
- Danneggiamento di sistemi informatici o telematici di pubblica utilità
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

7.4.2 Potenziale profilo di rischio rispetto al D. Lgs. 231/2001

I delitti informatici si verificano con comportamenti che realizzano la violazione, il danneggiamento o l'interruzione del sistema informatico interno di Biscotti P. Gentilini Srl, di informazioni, dati e programmi informatici di Biscotti P. Gentilini Srl e l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni relative al sistema informatico di Biscotti P. Gentilini Srl.

In questa prospettiva acquistano rilievo tutti i comportamenti che possono compromettere la sicurezza dei sistemi e dei dati informatici e la continuità del servizio informatico nell'ambito di operatività aziendale.

Appare utile ricordare che l'art. 1 della Convenzione sulla criminalità informatica del Consiglio di Europa fatta a Budapest il 23 novembre 2001, ratificata dall'Italia con la legge n. 48 del 18 marzo 2008 definisce "sistema informatico": "qualsiasi apparecchiatura, dispositivo, gruppo di apparecchiature o dispositivi, interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica di dati".

Si tratta di una definizione molto generale che permette di includere qualsiasi strumento elettronico, informatico o telematico, in rete (gruppo di dispositivi) o anche in grado di lavorare in completa autonomia. In questa definizione rientrano anche dispositivi elettronici che siano dotati di un software che permette il loro funzionamento elaborando delle informazioni (o comandi).

Nel medesimo articolo è contenuta la definizione di "dato informatico" che descrive il concetto derivandolo dall'uso: "qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informativo di svolgere una funzione".

Come conseguenza della violazione dei sistemi informatici acquistano rilievo le problematiche connesse alla tutela dei dati personali trattenuti dall'azienda. L'analisi dei rischi connessi ai delitti informatici è stata condotta pertanto avendo riguardo ai protocolli specifici di sicurezza dettati dal Documento Programmatico sulla Sicurezza (DPS) di Biscotti P. Gentilini Srl che qui si intendono richiamati.

7.4.3 Principi deontologici e indicazioni comportamentali di riferimento

Nello svolgimento delle attività che comportano accesso al sistema informatico di Biscotti P. Gentilini Srl o utilizzo di informazioni e/o dati relativi al sistema informatico di Biscotti P. Gentilini Srl si ispira alle disposizioni di legge e ai regolamenti vigenti.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 45 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

È fatto obbligo ai soggetti coinvolti di non adottare comportamenti a rischio di reato o contrari al Codice di condotta e ai principi di comportamento indicati nel Modello.

In particolare Biscotti P. Gentilini Srl si impegna al rispetto dei seguenti principi comportamentali:

- Biscotti P. Gentilini Srl, consapevole dei continui cambiamenti tecnologici e dell'elevato impegno operativo, organizzativo e finanziario necessario, si impegna a mantenere un efficace sistema di sicurezza informatica, in particolare attraverso (i) la protezione dei sistemi e delle informazioni dai potenziali attacchi, attraverso l'utilizzo di strumenti atti a prevenire e a reagire a fronte delle diverse tipologie di attacchi, e (ii) la garanzia della massima continuità del servizio;
- Biscotti P. Gentilini Srl e tutti coloro che all'interno o all'esterno di Biscotti P. Gentilini Srl sono tenuti a conoscerlo in ragione del loro ufficio (Titolare, Responsabile, Incaricati del trattamento dei dati, oltre a tutti coloro che di fatto trattino dati soggetti alle disposizioni di cui all'art. 34 del D. Lgs. 196/2003) devono uniformare il proprio comportamento alle disposizioni del Documento Programmatico di Sicurezza (DPS) di Biscotti P. Gentilini Srl;
- l'assegnazione e la gestione delle credenziali di autorizzazione personale (username e password) e delle credenziali di accesso alle diverse sezioni del sistema informatico di Biscotti P. Gentilini Srl e i termini di validità delle medesime sono stabilite secondo idonee policy aziendali;
- l'accesso alle diverse sezioni del sistema informatico di Biscotti P. Gentilini Srl e a eventuali dati, informazioni, sistemi informatici e telematici cui Biscotti P. Gentilini Srl abbia accesso è riconosciuto a dipendenti, collaboratori, consulenti e partner nei limiti in cui tale accesso sia funzionale allo svolgimento del relativo incarico e coerentemente con gli obiettivi aziendali;
- le policy aziendali in materia di accesso al sistema informatico, a eventuali dati, informazioni, sistemi informatici e telematici sono definite dal Consigliere Delegato sentito il Direttore Amministrazione, Finanza e Controllo;
- ogni singolo utente è personalmente responsabile riguardo l'utilizzo del sistema informatico di Biscotti P. Gentilini Srl, inclusi eventuali dati, informazioni, sistemi informatici e telematici cui Biscotti P. Gentilini Srl abbia accesso, nell'ambito dei presidi posti da Biscotti P. Gentilini Srl a tutela della sicurezza, integrità e riservatezza dei dati.

7.5 Protocolli di gestione e controllo

7.5.1 Premessa

Il sistema dei controlli preventivi ai fini dei reati identificati si basa sugli elementi della formalizzata attribuzione di deleghe, della responsabilizzazione dei soggetti delegati, della tracciabilità delle azioni.

In particolare, i protocolli specifici introdotti con riferimento all'attività oggetto di analisi sono di seguito descritti:

- le procedure interne identificano con chiarezza ruoli e competenze delle funzioni incaricate della gestione dei sistemi informatici di Biscotti P. Gentilini Srl;
- il Sistema di Gestione dei Dati Personali (REG. UE 679/2016) adottato da Biscotti P. Gentilini Srl identifica i titolari di permessi di accesso agli archivi cartacei e informatici, distinguendo le misure di sicurezza adottate per i documenti cartacei e per i trattamenti informatici; per questi ultimi sono identificate le procedure adottate per l'autenticazione e l'accesso ai sistemi;

- il Sistema di Gestione dei Dati Personali (REG. UE 679/2016) adottato da Biscotti P. Gentilini Srl prevede un sistema di protezione mediante salvataggio automatico del server della rete aziendale di “backup” su base giornaliera;
- il Sistema di Gestione dei Dati Personali (REG. UE 679/2016) adottato da Biscotti P. Gentilini Srl prevede un sistema di protezione mediante strumenti di “disaster recovery” per garantire il ripristino dell’accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici con frequenza almeno settimanale;
- il sistema informatico è protetto dal rischio di intrusione da parte di virus o di altri software maligni attraverso antivirus con aggiornamento automatico, firewall e proxy;
- è fatto esplicito divieto ad amministratori, dipendenti, collaboratori, consulenti e partner che a vario titolo abbiano accesso alla rete aziendale di installare propri software che non rientrino nello scopo per cui il sistema informatico è stato assegnato all’utente, al fine di evitare il rallentamento o il blocco della rete informatica aziendale;
- è fatto esplicito divieto ad amministratori, dipendenti, collaboratori, consulenti e partner che a vario titolo abbiano accesso alla rete aziendale di installare nella rete propri software che possano impedire o interrompere o danneggiare le comunicazioni informatiche aziendali ovvero l’intero sistema informatico aziendale;
- è fatto esplicito divieto ad amministratori, dipendenti, collaboratori, consulenti e partner di operare in maniera illecita su sistemi informativi altrui al fine di sottrarre fraudolentemente dati o informazioni riservate o sensibili;
- i soggetti delegati alla gestione dei sistemi informatici di Biscotti P. Gentilini Srl devono annualmente rilasciare all’OdV una dichiarazione attestante la conformità dei comportamenti tenuti con le prescrizioni comportamentali e procedurali indicate nel Modello;
- è fatto obbligo ai soggetti coinvolti di comunicare immediatamente all’OdV 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 (es. modifiche legislative e regolamenti; mutamenti nell’attività disciplinata, modifica delle struttura e delle funzioni coinvolte, ecc.);
- qualora si verificano circostanze non regolamentate, che si prestano a dubbie interpretazioni, tali da originare difficoltà nell’operatività dell’attività, è obbligo di tutti i soggetti coinvolti di ricorrere al proprio responsabile che, sentito l’OdV, assume le decisioni del caso.

7.5.2 I reati ex art. 24 bis del D. Lgs. 231/2001 – Protocolli comportamentali

Ai fini dell’attuazione delle regole comportamentali e dei divieti elencati nel punto precedente, i Destinatari della presente, oltre a rispettare le previsioni di legge esistenti in materia, i principi comportamentali richiamati nel Codice Etico e quelli enucleati nella Parte Generale del presente Modello, devono rispettare i seguenti protocolli comportamentali qui di seguito descritti, posti a presidio dei rischi-reato sopra identificati (art. 24 bis del D. Lgs. 231/2001) e riferibili alle attività sensibili.

I protocolli comportamentali prevedono obblighi (Area del fare) e/o divieti specifici (Area del non fare) che i Destinatari della presente devono rispettare, uniformando la propria condotta ad essi in corrispondenza delle attività sensibili sopra rilevate. Tali principi riprendono, specificandole o, se del caso, integrandole, le norme del Codice Etico e della Parte Generale del Modello. In forza di apposite pattuizioni contrattuali, i principi in esame si applicano anche ai Soggetti Esterni coinvolti nello svolgimento delle attività sensibili identificate.

Area del Fare



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 47 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

Tutte le attività sensibili devono essere svolte conformandosi alle leggi vigenti, alle norme del Codice Etico, ai principi generali di comportamento del presente Modello, nonché ai protocolli, alle policies e procedure definite e implementate, alle eventuali altre procedure organizzative esistenti poste a presidio dei rischi-reato identificati.

La Società è consapevole del fatto che, per l'attività svolta, la protezione delle infrastrutture IT, dei sistemi informatici/telematici e delle applicazioni, dei dati e delle informazioni ivi contenuti presentano particolare criticità.

In particolare, la Società Biscotti P. Gentilini Srl è consapevole che, per il raggiungimento dei propri obiettivi di business e nell'interesse dei suoi stakeholders, è necessario che, mediante un approccio globale, sia garantita la sicurezza delle informazioni, siano attribuite espressamente e formalmente le responsabilità per la sicurezza delle informazioni, venga valutato il livello di sicurezza dei sistemi informatici/telematici con conseguente valutazione e rivalutazione costante del livello di rischio, gestione del rischio medesimo (con l'obiettivo di eliminarlo, mitigarlo o ridurlo comunque al livello ritenuto accettabile) mediante apposite policies, procedure finalizzate alla prevenzione attiva e di rilevamento degli incidenti di sicurezza informatica, nonché adeguata attività di controllo e monitoraggio.

Tale sistema fornisce un modello per la definizione, l'implementazione, il controllo, il monitoraggio e il miglioramento continuo del livello di affidabilità e di funzionamento dei sistemi informatici/telematici aziendali, della protezione delle infrastrutture IT, del patrimonio informativo aziendale e di tutti i dati, ivi comprese le credenziali di accesso, di dipendenti, clienti/utenti e terzi soggetti.

I vantaggi di implementazione di questo sistema di gestione "olistica" della sicurezza informatica/telematica, rappresentati, come detto, da una riduzione dei rischi in termini di probabilità di verifica e/o di impatto di "incidenti", costituiscono un adeguato presidio anche con riferimento al rischio di commissione dei reati.

Per tale motivo, per il raggiungimento degli obiettivi di prevenzione, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare e attenersi con il massimo rigore a tutte le polizie aziendali e procedure operative.

In particolare:

- la Società definisce, aggiorna, approva formalmente le policies aziendali e le procedure in materia di sicurezza informatica/telematica e ne assicura la divulgazione a tutti gli interessati, a tutti i livelli dell'organizzazione;
- quanto detto al punto precedente, con particolare riferimento a:
 - piano di business continuity, ivi compreso il disaster recovery;
 - back up (modalità, frequenza, etc.);
 - accesso remoto da parte di terzi soggetti;
 - requisiti di autenticazione a tutti i sistemi informatici/telematici, applicazioni e reti (regole per la creazione, modifica, conservazione di password) e formalizzazione e tracciatura di tutte autorizzazioni, registrazioni, modifiche e cancellazioni di profili di autenticazione, ivi compresi quelli di clienti/utenti; divieti o limitazioni di accesso a sistemi informatici/telematici, applicazioni o reti;
 - generazione, protezione e conservazione dei "log" di sistema, di applicazione e di database;
 - concessione di adeguati livelli di privilegio;
 - formale assegnazione di particolari livelli di privilegio e formale assunzione della relativa responsabilità;
 - controllo e tracciatura di variazioni significative (quantitative e qualitative) di dati e informazioni e altri anomali inserimenti, modificazioni o cancellazioni;

- implementazione, gestione e manutenzione di reti (attribuzione di responsabilità; controlli finalizzati a garantire la protezione e la riservatezza dei dati e delle informazioni ivi contenute, o in transito (vulnerability assessment, penetration test etc.);
- monitoraggio del traffico;
- gestione e manutenzione hardware (ivi compresi inventario e divieti o limitazioni di utilizzo);
- installazione, gestione e manutenzione software e banche dati (ivi compresi inventario, verifica di validità, operatività, scadenza e limiti di licenze e certificazioni di software e banche dati di terzi o loro utilizzo in conformità alle norme sul diritto d'autore e altri diritti
- connessi al suo esercizio; divieti o limitazioni di installazione/utilizzo);
- regolamentazione accesso fisico ai locali in cui risiedono le infrastrutture IT (attribuzione di facoltà di accesso, misure di sicurezza e di vigilanza e assunzione della relativa responsabilità);
- creazione, protezione mediante crittografia (ivi compresa la definizione, distribuzione/segretezza, sostituzione e archiviazione dei relativi algoritmi e chiavi), emissione, archiviazione, conservazione, eliminazione, divulgazione, immissione in reti informatiche/telematiche di documenti informatici e manutenzione in genere degli archivi di documenti informatici;
- regolamentazione dell'utilizzo della firma digitale con formale attribuzione e formale assunzione della relativa responsabilità.
- Nomina di amministratore/i di sistema e amministratore/i di database con atto formale, definizione di compiti e attribuzioni ed espressa assunzione della relativa responsabilità;
- Per quanto attiene alla sicurezza dei dati personali di tutti i soggetti con i quali intrattiene rapporti a vario titolo, la Società ha adeguato il suo sistema organizzativo ai principi e obblighi di cui alla normativa vigente in materia e, in particolare, del Sistema di Gestione Privacy Reg. UE 679/2016 e del Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), e garantisce che il trattamento dei dati medesimi si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
- I sistemi informatici/telematici, i programmi informatici, nonché policies e procedure IT della Società garantiscono che il trattamento dei dati personali avvenga nel rispetto dei principi e norme di cui sopra, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Area del Non Fare

E' fatto espresso divieto ai Destinatari di porre in essere comportamenti in violazione o comunque non conformi alle policies e procedure definite e implementate dalla Società, nonché comportamenti tali da integrare, anche solo potenzialmente e anche a titolo di concorso o di tentativo, le fattispecie di reato di cui sopra.

In particolare, premesso che:

- a) la definizione di "concorso" di persone del reato data dal codice penale ricomprende nel "contributo obiettivamente rilevante" ogni forma di collaborazione, anche "morale", idonea, cioè, determinare o a rafforzare il proposito criminoso di altri soggetti (e.g. istigazione),
- b) per documento informatico deve intendersi qualsiasi rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, di natura pubblica o privata, qualora dotato di "efficacia probatoria", cioè con firma elettronica qualificata o emesso nel rispetto di quelle regole tecniche finalizzate a garantirne paternità, provenienza, integrità e immodificabilità,

ai Destinatari è fatto divieto di:



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 49 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

- Formare o concorrere con un pubblico ufficiale o incaricato di pubblico servizio a formare documenti informatici falsi o alterare atti veri;
- Contraffare o alterare o concorrere con un p.u. o i.p.s. nel contraffare o alterare certificati o autorizzazioni amministrative contenute in un documento informatico, o a contraffare o alterare le condizioni richieste per la loro validità;
- Concorrere con un p.u. o i.p.s. a formare e rilasciare una copia in forma legale su documento informatico di un atto pubblico o privato inesistente o una copia diversa dall'originale.
- Contraffare o concorrere con un p.u. o i.p.s. nel contraffare un attestato.
- Concorrere con un p.u. o i.p.s. nella falsa attestazione da parte di quest'ultimo in un documento informatico che un fatto è stato da lui compiuto o che è avvenuto in sua presenza, ovvero nell'attestazione da parte dello stesso in un documento informatico di aver ricevuto dichiarazioni non rese o nell'omissione o alterazione di dichiarazioni da lui ricevute;
- Concorrere con un p.u. o i.p.s. nella falsa attestazione, in atti, in certificati o autorizzazioni amministrative sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità.
- Concorrere con un esercente una professione sanitaria o forense o altro servizio di pubblica necessità nell'attestare falsamente, in un certificato sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità.
- Attestare falsamente, oralmente o per iscritto, ad un p.u. in un atto pubblico, sotto forma di documento informatico, fatti dei quali il documento medesimo è destinato a provare la verità.
- Scrivere o lasciare scrivere false indicazioni nelle registrazioni, sotto forma di documento informatico, soggette all'ispezione dell'Autorità di P.S. o nelle notificazioni, sotto forma di documento informatico, alla stessa Autorità, riguardanti operazioni industriali, commerciali o professionali.
- Formare in tutto o in parte scritte private false, sotto forma di documento informatico, o alterazione di scritte private vere, utilizzandole o lasciando che altri le utilizzino.
- Scrivere o far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto privato produttivo di effetti giuridici diversi da quelli previsti, utilizzandolo o lasciando che altri lo utilizzino.
- Scrivere o far scrivere, ovvero concorrere con un p.u. nello scrivere o nel far scrivere, su documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto pubblico diverso da quello a cui il p.u. stesso era obbligato o autorizzato.
- Distruggere, sopprimere, occultare in tutto o in parte una scrittura privata o un atto pubblico veri, sotto forma di documento informatico.
- Utilizzare abusivamente la firma digitale aziendale o, comunque, in violazione delle procedure che ne regolamentano l'utilizzo.

E'altresì vietato:

- Introdursi abusivamente o permanere contro la volontà espressa o tacita dell'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza.
- Procurarsi, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo.

- Procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare, mettere a disposizione apparecchiature dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico o le informazioni, i dati o i programmi ivi contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale o l'alterazione del suo funzionamento.
- Intercettare illecitamente o abusivamente, impedire, interrompere fraudolentemente o illecitamente comunicazioni informatiche o telematiche.
- Installare illecitamente o abusivamente apparecchiature atte ad intercettare, impedire, interrompere comunicazioni informatiche o telematiche.
- Distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui, o utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- Distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui, ovvero ostacolarne gravemente il funzionamento mediante distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici altrui o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi.
- Distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o introduzione o trasmissione di dati, informazioni o programmi al fine di distruggere, danneggiare, o causare l'inutilizzabilità in tutto o in parte di sistemi informatici o telematici ovvero al fine di ostacolarne gravemente il loro funzionamento.

7.6 La gestione della filiera alimentare

La Società è dotata di un "Piano di autocontrollo HACCP", che è l'insieme delle procedure operative volte a prevenire, o quantomeno a contenere, l'insorgenza dei pericoli lungo la filiera produttiva, attraverso il controllo sistematico delle singole fasi e la successiva registrazione su una specifica documentazione, in ottemperanza alla normativa vigente.

A tale piano viene fatto rinvio per quanto riguarda la prevenzione dei reati inerenti.

7.7 Policies e procedure a presidio dei rischi-reato

La Società ha definito, implementato e diffuso policies e procedure nell'ambito del suo sistema di gestione della sicurezza dei sistemi informatici/telematici.

Tali procedure costituiscono adeguati presidi e strumenti di gestione del rischio con riferimento alle tipologie di reato.

La Società, comunque, definisce, implementa e diffonde un organigramma contenente gli ambiti e le responsabilità di ciascuna funzione, nonché, ove necessario, ulteriori policies e procedure aziendali in materia di sicurezza dei sistemi di cui sopra, ad integrazione di quelle esistenti, che si aggiungono - unitamente alle indicazioni sopra fornite - a costituire il driver per lo svolgimento delle attività sensibili considerate, e di quelle ad esse strumentali o comunque collegate, nonché per i relativi controlli, e, soprattutto, definiscono in dettaglio, ove ciò non sia già previsto, il sistema di riporto e i flussi informativi nei confronti dell'OdV.

In particolare, le procedure esistenti e quelle eventuali integrative devono garantire:

- chiarezza e precisione dei vari ruoli, compiti, attribuzioni, poteri e responsabilità;
- l'individuazione di un responsabile per ciascuna attività sensibile o per ciascuna fase della stessa;
- chiarezza e precisione delle varie linee di riporto;



**MODELLO DI ORGANIZZAZIONE,
GESTIONE E CONTROLLO
AI SENSI DEL D. LGS. 231/2001 E S.M.I.
ESTRATTO**

Pagina 51 di 70

Edizione 03 – Settembre 2022

Emittente: C.d.A.

- segregazione delle funzioni (separazione per ciascun processo tra il soggetto che decide, quello che autorizza, quello che esegue e quello che controlla);
- tracciabilità di tutte le fasi del processo e dei relativi soggetti;
- adeguati controlli (preventivi, concomitanti o successivi; automatici o manuali; continui o periodici; analitici o a campione), di tutte le fasi critiche del processo.
- flussi informativi nei confronti dell'OdV.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 52 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

8 L'ADOZIONE E LA GESTIONE DEL MODELLO

8.1 Adozione e aggiornamento del Modello

Il Consiglio di Amministrazione della Società adotta il presente Modello ed informa di tale adozione con specifica comunicazione affissa in bacheca al momento della sua delibera di approvazione.

Essendo il Modello un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6, comma 1, lettera a, del Decreto), le successive modifiche ed integrazioni del Modello, effettuate a cura dell'Organismo di Vigilanza (di cui di seguito), sono rimesse alla competenza del Consiglio di Amministrazione della Società che dovrà procedere alla adozione della versione modificata dello stesso.

Premesso che la modifica del Modello può essere sostanziale o non sostanziale, nei due casi l'approvazione della versione modificata deve avvenire:

- in caso di modifica sostanziale, nel corso della prima riunione utile;
- in caso di modifica non sostanziale, entro sei mesi dall'effettuazione della stessa.

Si considerano modifiche sostanziali del Modello:

- l'introduzione di nuove fattispecie di reato che possono determinare la responsabilità dell'ente ai sensi del Decreto e il conseguente aggiornamento della Parte Generale del Modello e della Mappa dei rischi;
- l'aggiornamento del Sistema di Corporate Governance conseguente a modificazioni adottate della Società;
- l'introduzione di nuovi Sistemi di gestione, oltre a quelli già descritti nel presente Modello;
- la modifica dei protocolli esistenti e l'introduzione di nuovi protocolli;
- la revisione estesa-complessiva della Mappa dei rischi e le relative modifiche alla Parte Generale del Modello.

Tra le modifiche sostanziali, va annoverato inoltre il recepimento delle proposte formulate dall'Organismo di Vigilanza al Consiglio di Amministrazione per gli eventuali aggiornamenti ed adeguamenti del Modello, ritenuti necessari in seguito a violazioni o elusioni delle prescrizioni che mettano in evidenza l'inefficacia del Modello, significative modifiche dell'assetto organizzativo, variazioni normative o orientamenti giurisprudenziali.

Si considerano invece modifiche non sostanziali del Modello tutte quelle non sopra individuate, tra cui principalmente:

- le variazioni al sistema delle deleghe conferite e riportate nel presente Modello, relative sia alla dirigenza sia alla sicurezza;
- le modifiche ai sistemi di gestione già adottati e descritti nel Modello;
- l'aggiornamento/modifica/integrazione della Mappa dei rischi, diversa da quella citata tra le modifiche sostanziali.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 53 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

8.2 Comunicazione e formazione

8.2.1 Comunicazione

Il Modello (Parte Generale e Parte Speciale) è comunicato a ciascun componente gli Organi sociali, a ciascun soggetto apicale e a ciascun responsabile di funzione, i quali sottoscrivono una dichiarazione di ricevimento, archiviata dall'Organismo di Vigilanza.

Le modalità di diffusione del Modello sono stabilite dall'Organismo di Vigilanza; l'effettiva diffusione è effettuata a cura del Responsabile Risorse Umane.

Un estratto della Parte Generale del Modello:

- viene affisso nella bacheca aziendale;
- viene messo a disposizione di tutti i collaboratori della Società, in forma cartacea presso il Responsabile Risorse Umane ed in formato elettronico nel sistema di archiviazione documentale;
- viene pubblicato sul sito internet della Società.

In generale, sarà cura del Responsabile Risorse Umane informare i terzi che interagiscono con l'ente dell'avvenuta adozione del Modello e in sintesi delle parti per essi rilevanti.

Le stesse modalità informative saranno adottate in caso di aggiornamento del Modello, nel momento in cui ne sarà stata data approvazione da parte del Consiglio di Amministrazione.

8.2.2 Formazione

I principi e i contenuti del Decreto e del Modello sono divulgati mediante corsi di formazione, ai quali tutti i soggetti apicali, i dipendenti ed i collaboratori in generale sono tenuti a partecipare. I corsi di formazione saranno diversificati in relazione alle funzioni ricoperte dai partecipanti (amministratori e sindaci, soggetti apicali, dipendenti e collaboratori).

La formazione verrà effettuata all'adozione del Modello, a seguito di sue variazioni, nonché ogni qualvolta ciò fosse ritenuto indispensabile dall'Organismo di Vigilanza. La partecipazione ai corsi di formazione è obbligatoria e l'Organismo di Vigilanza vigilerà su tale partecipazione.

Il Responsabile Risorse Umane, di concerto con l'Organismo di Vigilanza, garantirà la necessaria formazione stabilendo:

- il contenuto e la durata dei corsi;
- la loro frequenza;
- i partecipanti e l'obbligo di frequenza;
- le modalità con le quali eseguire i controlli che sia stato realizzato tutto quanto stabilito.

In relazione agli aspetti SSL, la Società attiva – nel rispetto delle previsioni normative – dei piani di formazione differenziati per ruoli e responsabilità, al fine di assicurare un'adeguata consapevolezza circa l'importanza sia della conformità delle azioni rispetto al Modello, sia delle possibili conseguenze connesse a violazioni dello stesso; in quest'ottica, particolare rilevanza è riconosciuta alla formazione ed all'addestramento dei soggetti che svolgono compiti in materia di SSL.

L'Organismo di Vigilanza verificherà che la formazione sia tenuta in modo adeguato e che essa sia differenziata nei contenuti, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza dell'ente.

9 L'ORGANISMO DI VIGILANZA E CONTROLLO

9.1 *Requisiti e caratteristiche dell'Organismo di Vigilanza*

In merito all'organo al quale può essere attribuito il ruolo di vigilanza il Decreto legislativo 231/2001 precisa che esso (art. 6, comma 1, lettera b):

- deve essere dotato di autonomi poteri di iniziativa e controllo;
- deve avere compiti di vigilanza sul funzionamento e sull'osservanza del "Modello di organizzazione e gestione";
- deve altresì curarne l'aggiornamento.

Il legislatore non ha tuttavia fornito ulteriori indicazioni circa le caratteristiche specifiche, le responsabilità e la composizione dell'Organismo.

Maggiori indicazioni, sia in merito alla composizione dell'Organismo di Vigilanza che in merito ai requisiti minimi che l'Organismo deve possedere per poter svolgere correttamente i suoi compiti (autonomia e indipendenza, professionalità, e continuità d'azione), sono state fornite dalle linee guida predisposte da alcune associazioni di categoria. I principali requisiti che l'organismo in esame deve possedere, sono stati poi individuati anche in sede giurisprudenziale. Alla luce delle premesse sopra illustrate, nonché della propria struttura, la Società si è dotata di un O.d.V., i cui membri sono designati con delibera consiliare e sono rieleggibili. Con la stessa delibera viene fissata la durata della carica (non inferiore a tre anni) ed il compenso.

L'Organismo di Vigilanza è dotato di autonomi poteri di iniziativa e controllo ed ha una posizione indipendente ed autonoma in quanto si relaziona direttamente con il Consiglio di Amministrazione (terzietà), senza alcun vincolo di subordinazione gerarchica. Per questi motivi, nonché per rispondere al requisito dell'imparzialità, i suoi membri devono essere dotati di onorabilità ed assenza di conflitti d'interesse.

L'autonomia va intesa in senso non meramente formale, nel senso che è necessario che l'O.d.V.:

- sia dotato di risorse (anche finanziarie) adeguate;
- possa avvalersi di strumentazioni, supporti ed esperti nell'espletamento della sua attività di monitoraggio.

L'indipendenza dei componenti dell'Organismo di Vigilanza viene garantita dal fatto che essi non risultino coniugi, parenti od affini entro il quarto grado degli Amministratori della Società, né legati allo stesso da rapporti di natura patrimoniale o professionale. Inoltre non devono trovarsi in una posizione, neppure potenziale, di conflitto di interessi con l'ente né essere titolari all'interno dello stesso di funzioni di tipo esecutivo che, rendendolo partecipe di decisioni ed attività operative, ne minerebbero l'obiettività di giudizio nel momento delle verifiche sui comportamenti e sul Modello.

Il requisito della professionalità dei membri va inteso come capacità specifiche in tema di attività ispettiva e consulenziale, con particolare riferimento alla necessaria competenza legale e di auditing. Tale requisito è infatti riferito al bagaglio di strumenti e tecniche che l'organismo deve possedere per poter svolgere efficacemente l'attività assegnata.

Sul punto si sottolinea che, in sede giurisprudenziale (cfr. G.I.P. presso il Tribunale di Milano, ordinanza in data 20 settembre 2004), proprio il possesso di specifiche competenze in tema di attività ispettiva e di analisi, e delle connesse tecniche, sono stati individuati come indispensabili requisiti dell'O.d.V..

I fondamentali requisiti di autonomia, imparzialità, indipendenza, professionalità sono garantiti dal fatto che il solo Consiglio di Amministrazione può revocare ciascun membro ovvero l'intero Organismo di Vigilanza, e solo quando si verifichi una giusta causa, e cioè:

- l'interdizione o l'inabilitazione ovvero una grave infermità di uno o più dei componenti, che renda l'Organismo di Vigilanza inidoneo a svolgere le proprie funzioni, o un'infermità che, comunque, comporti l'impossibilità a svolgere l'attività per un periodo superiore a sei mesi;
- l'attribuzione ad uno o più dei componenti di funzioni e responsabilità operative incompatibili con i requisiti di autonomia di iniziativa e di controllo, indipendenza e continuità di azione, che sono propri dell'Organismo di Vigilanza;
- un grave inadempimento dei doveri propri dell'Organismo di Vigilanza;
- una sentenza di condanna della Società ai sensi del Decreto, anche in primo grado, ovvero un procedimento penale concluso tramite c.d. "patteggiamento", ove risulti dagli atti "l'omessa o insufficiente vigilanza" da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art.6, comma 1 lett. d del Decreto;
- una sentenza di condanna, a carico dei componenti dell'Organismo di Vigilanza per aver personalmente commesso uno dei reati previsti dal Decreto;
- la condanna, a carico dei componenti dell'Organismo di Vigilanza, per avere commesso un reato con dolo;
- la condanna ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche;
- la perdita dei requisiti di indipendenza così come sopra definiti;
- la presenza di un conflitto di interesse permanente.

Tali giuste cause di revoca costituiscono altresì causa di ineleggibilità o di decadenza, e ciò in quanto è in tal modo garantita l'onorabilità dei componenti l'O.d.V., sia per ragioni di coerenza di sistema, sia per rispondere alle censure che potrebbero essere sollevate in sede giurisprudenziale (cfr. G.I.P. presso il Tribunale di Napoli, ordinanza in data 26.06.2007 e G.I.P. presso Tribunale di Milano, ordinanza in data 09.11.2004).

La rinuncia all'incarico, da parte di ciascun membro dell'O.d.V., potrà avvenire in qualsiasi momento con un preavviso di trenta giorni. In tal caso il Consiglio provvederà in tempo utile alla sua sostituzione.

La decadenza dell'O.d.V. si verifica automaticamente se viene a mancare per dimissioni o altre cause la maggioranza dei componenti.

L'Organismo è dotato di autonomo potere di spesa, al fine di potersi avvalere del supporto di professionalità specialistiche esterne nell'esecuzione dei controlli di competenza. A tali fini potrà altresì utilizzare professionalità interne.

L'O.d.V. è comunque obbligato a rendicontare annualmente al Consiglio di Amministrazione l'utilizzo del Budget assegnatogli.

Le sopra delineate caratteristiche dell'O.d.V., unitamente alla sua stabilità ed alla possibilità di avvalersi di un suo Budget, gli consentono la richiesta continuità d'azione, per soddisfare la previsione di cui all'art. 6, comma 1, lettera d), e quindi per poter dare la garanzia di efficace e costante attuazione di un Modello così articolato e complesso.

Con riferimento all'indipendenza dell'O.d.V., essa è altresì garantita dal Consiglio di Amministrazione dell'ente che si impegna a mantenerlo indenne da rischi di ritorsioni, comportamenti discriminatori o comunque da condotte pregiudizievoli nei suoi confronti per l'attività svolta.

In particolare, qualsiasi atto modificativo o interruttivo nel rapporto con l'ente è sottoposto alla preventiva approvazione del Consiglio di Amministrazione. Gli interventi modificativi o interruttivi del rapporto dovranno essere votati con la maggioranza dei due terzi dei Consiglieri.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 56 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

9.2 Funzioni, poteri e attività di controllo dell'Organismo di Vigilanza

9.2.1 Funzioni e poteri dell'Organismo di Vigilanza

L'O.d.V. non costituisce una sovrapposizione rispetto agli organi di controllo previsti dai diversi sistemi di gestione, anzi imposta un "comportamento" dell'ente all'interno e all'esterno che si integra con gli scopi di una corretta gestione e di un efficiente apparato di controllo, attraverso la giusta previsione di un sistema di scambio incrociato di informazioni tra l'organo amministrativo, quello di controllo (es.: collegio sindacale) e l'organismo di vigilanza.

Il corretto ed efficace svolgimento dei compiti affidati all'O.d.V. sono presupposti indispensabili per l'esonero dalla responsabilità, sia che il reato sia stato commesso dai soggetti "apicali" sia che sia stato commesso dai soggetti sottoposti all'altrui direzione (in tal senso andrebbe letto l'art. 7, comma 4, laddove prevede che l'efficace attuazione del modello richiede, oltre all'istituzione di un sistema disciplinare, una sua verifica periodica, evidentemente da parte dell'organismo a ciò deputato).

A tale organo all'uopo istituito, perché operi costantemente in coordinamento con l'ente, pur risultando soggetto autonomo ed indipendente da esso, sono rimessi la verifica, applicazione ed aggiornamento dei modelli di organizzazione e gestione.

L'Organismo è dunque dotato di tutti i poteri necessari per assicurare una puntuale ed efficiente/efficace vigilanza sul funzionamento e sull'osservanza del Modello nonché per l'espletamento dei seguenti compiti:

- verificare il rispetto, l'efficienza, l'efficacia e l'adeguatezza del Modello mediante verifiche periodiche o a sorpresa;
- curare l'aggiornamento della mappatura delle aree interne sensibili nell'ambito delle quali è ipotizzabile la commissione di reati previsti dal Decreto 231/2001;
- formulare proposte al Consiglio di Amministrazione. per gli eventuali aggiornamenti ed adeguamenti del modello organizzativo ritenuti necessari in seguito a violazioni delle prescrizioni, significative modifiche dell'assetto organizzativo, variazioni normative o orientamenti giurisprudenziali;
- verificare l'attuazione e l'effettiva funzionalità delle modifiche apportate;
- segnalare al Consiglio di Amministrazione le violazioni accertate del modello che comportino una responsabilità dell'ente e vigilare sulla conseguente applicazione delle sanzioni previste;
- raccogliere, elaborare ed archiviare le informazioni rilevanti in ordine al funzionamento ed al rispetto del Modello, nonché la documentazione che compone il Modello medesimo, ivi comprese – inter alia – la mappatura delle aree interne a rischio-reato, i relativi aggiornamenti, le relazioni sull'attività di vigilanza svolta;
- collaborare all'organizzazione di iniziative idonee ad assicurare la massima diffusione e conoscenza delle prescrizioni del Modello, controllando la frequenza ed il contenuto dei necessari programmi di formazione;
- vigilare sull'effettiva e concreta applicazione del Codice Etico e valutarne l'adeguatezza, per gli aspetti di competenza;
- effettuare, direttamente o tramite professionisti, in caso di circostanze particolari (ad esempio, emersione di precedenti violazioni) attività di ricerca e di identificazione di eventuali nuovi rischi.

Coerentemente, all'O.d.V. sono conferiti tutti i poteri necessari per il corretto espletamento dei compiti assegnatigli. Infatti, per poter assolvere in modo esaustivo i propri delicati ed onerosi compiti l'O.d.V. deve essere dotato, come specificano la legge in commento (articolo 6, 1° comma, lett. b) D. Lgs. n. 231/2001) ed

i primi interventi giurisprudenziali, di autonomi poteri di iniziativa e di controllo, ovvero di strumenti adeguati per poter verificare l'idoneità delle procedure codificate per la prevenzione degli illeciti e la puntuale e completa attuazione delle stesse in ciascuna delle aree di rischio individuate in seno all'ente.

Decisiva, in tal senso, è l'autonomia nei confronti degli organi di direzione ed amministrazione dell'ente che deve caratterizzare le fasi dell' "iniziativa" e del "controllo".

In estrema sintesi, l'organismo dovrà essere munito della capacità di decidere cosa, quando, e come esplicitare la propria fondamentale funzione di controllo, agendo in modo indipendente dalle altre funzioni ed organi di vertice dell'ente, in quanto, come si ribadisce, sono essi stessi destinatari dell'attività ispettiva.

Inoltre, molto significativa, evidentemente, è la facoltà di attivarsi (con criteri di autonomia) nella richiesta di informazioni, dati e documenti verso tutte le componenti interne dell'ente.

Ulteriori, fondamentali, prerogative dell'O.d.V. sono da individuare nella facoltà di eseguire interviste e raccogliere segnalazioni.

I compiti ed i poteri dell'O.d.V., unitamente alla nomina dei relativi membri, sono oggetto di specifica comunicazione interna.

Per garantire un efficace ed effettivo svolgimento delle proprie funzioni, oltre alle eventuali disposizioni generali dettate dal Consiglio di Amministrazione, tale Organismo ha la facoltà di stabilire apposite regole operative e adottare un proprio regolamento interno al fine di garantire la massima autonomia organizzativa e d'azione del soggetto in questione.

È necessario che l'O.d.V. provveda a documentare lo svolgimento dei suoi compiti. Infatti, l'attività di documentazione, da svolgersi in modo sintetico, chiaro, approfondito ed obiettivo, non deve essere sottovalutata né considerata come un aggravio burocratico-amministrativo da parte dei suoi componenti posto che:

- dai documenti si può evincere la "sufficiente vigilanza";
- può essere necessario, come nel caso di successiva attività investigativa della polizia giudiziaria finalizzata all'accertamento della responsabilità amministrativa dell'ente, ricostruire, anche ad anni di distanza, l'attività di vigilanza posta in essere dal citato organismo di controllo interno.

Pertanto, l'attività svolta dall'Organismo di Vigilanza deve essere sempre documentata per iscritto e le sedute verbalizzate e sottoscritte dai suoi componenti.

9.2.2 Attività di controllo dell'Organismo di Vigilanza

L'attività di controllo proprie dell'Organismo di Vigilanza si fondano su:

- verifiche dei principali atti e dei contratti di maggior rilevanza conclusi dalla Società in aree di attività a rischio;
- verifiche delle procedure, al fine di monitorarne l'efficacia e l'effettivo funzionamento in modo da prevenire la commissione dei reati di cui al Decreto 231;
- verifiche delle segnalazioni ricevute e delle azioni avviate conseguentemente.

9.3 Informativa

9.3.1 Informativa all'Organismo di Vigilanza

Per quanto sopra indicato assume fondamentale rilevanza il generale obbligo di assoluta ed incondizionata collaborazione incombente su tutti i livelli e le funzioni della società o dell'ente, siano essi operativi ovvero di direzione o di amministrazione.

In tal senso, la legge esplicitamente prevede precisi obblighi di informazione di cui l'organismo di controllo deve risultare destinatario, anche se la relazione illustrativa sul punto non fornisce ulteriori chiarimenti.

L'O.d.V. deve dunque poter disporre di tutte le informazioni necessarie per svolgere efficacemente le proprie funzioni e deve essere tenuto costantemente informato sull'evoluzione delle attività nelle aree a rischio ed avere libero accesso a tutta la documentazione aziendale rilevante, compresi i relativi dati di aggiornamento.

Sarà, inoltre, destinatario di segnalazioni da parte del management circa eventuali situazioni dell'attività aziendale che possano esporre l'ente al rischio di reato nonché di ogni altra informazione, di qualsiasi tipo, proveniente anche da terzi ed attinente all'attuazione del modello nelle aree a rischio.

Ciò comporta che ciascun collaboratore dovrà fornire all'O.d.V. tutte le seguenti informazioni:

- i documenti e le indicazioni relative alle singole attività, ove richiesti;
- le condotte anomale o comunque non in linea con il Modello;
- le notizie relative ad eventuali problematiche nell'effettiva applicazione del Modello nell'ambito delle attività dell'ente;
- tutte le notizie relative ad apparenti violazioni del Modello;
- eventuali richieste od offerte di denaro, doni o altre utilità, anche sotto forma di sconto (eccedenti il valore modico, e cioè in via orientativa Euro 150, secondo quanto previsto dal D.P.R. n. 62/2013), provenienti da, o destinate a, pubblici ufficiali o incaricati di pubblico servizio;
- eventuali omissioni, trascuratezze o falsificazioni nella tenuta della contabilità o nella conservazione della documentazione su cui si fondano le registrazioni contabili;
- in base ad un prudente apprezzamento discrezionale della Direzione le notizie relative ai procedimenti disciplinari in corso e alle eventuali sanzioni irrogate ovvero la motivazione della loro archiviazione;
- ogni situazione di pericolo connesso alla salute ed alla sicurezza sul lavoro.

L'informativa di cui sopra dovrà essere completa ed includere la copia della documentazione relativa; la documentazione di supporto, nel caso in cui non sia in possesso dei dipendenti, è ricercata a cura dell'Organismo di Vigilanza in forza dei suoi poteri ispettivi.

La Società garantisce che ciascun collaboratore potrà liberamente contattare l'O.d.V. per segnalare volontariamente le informazioni sopra indicate, con particolare riferimento ad eventuali irregolarità.

Dette informazioni dovranno essere fornite in forma non anonima; qualora invece giungessero in forma anonima, l'O.d.V. ne valuterà la fondatezza.

L'O.d.V. garantisce la necessaria riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge, ed altresì che il segnalante non subisca alcuna forma di ritorsione, discriminazione o penalizzazione. Tuttavia, gli autori di segnalazioni deliberatamente infondate e/o pretestuose potranno essere assoggettati a sanzioni disciplinari.

L'O.d.V. stabilisce inoltre la tempistica con la quale acquisire:

- verbali del Consiglio di Amministrazione, ove indispensabile;
- bilancio annuale;

- informazioni relative a cambiamenti organizzativi, incluso il sistema di governo e dei poteri, nonché delle procedure interne;
- segnalazioni dell'Organo di controllo relative a possibili carenze dei controlli interni o ad altre problematiche riscontrate;
- informazioni relative ad acquisizione ed utilizzo di contributi e finanziamenti pubblici;
- reportistica periodica in materia di salute e sicurezza sul lavoro, nonché tutti i dati relativi agli infortuni sul lavoro eventualmente occorsi.

Oltre alle segnalazioni sopra descritte, devono essere obbligatoriamente ed immediatamente trasmesse all'Organismo di Vigilanza le informazioni concernenti:

- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati previsti dal Decreto 231 o che interessano, anche indirettamente, la Società, i suoi dipendenti o collaboratori ed i componenti del Consiglio di Amministrazione;
- richieste di assistenza legale inoltrate dai dipendenti o collaboratori e dagli amministratori in caso di avvio di procedimenti giudiziari per i reati previsti dal Decreto 231;
- quando reso noto alla Società, l'avvio di procedimenti giudiziari nei confronti di amministratori, dipendenti, collaboratori;
- rapporti di controllo dai quali potrebbero emergere fatti, atti, eventi o omissioni con profili di criticità rispetto ai reati previsti dal Decreto 231.

La Società rende disponibili i necessari canali informativi per consentire la trasmissione di tutte le suddette informazioni all'O.d.V. e li rende noti a tutti i collaboratori con le modalità più opportune.

La violazione degli obblighi di informativa all'Organismo di Vigilanza costituisce violazione del Modello, sanzionabile secondo quanto previsto nell'apposita sezione: "Il Sistema Sanzionatorio".

9.3.2 Le segnalazioni verso l'Organismo di Vigilanza (whistleblowing)

L'Organismo di Vigilanza deve essere informato da parte dei Destinatari su base occasionale, circa ogni altra informazione, di qualsivoglia genere, proveniente anche da terzi ed attinente l'attuazione e la violazione del Modello nelle Aree a rischio di reato nonché il rispetto delle previsioni del Decreto, che possano risultare utili ai fini dell'assolvimento dei compiti dell'Organismo di Vigilanza ("segnalazioni").

In particolare devono essere segnalate le seguenti circostanze:

- condotte illecite, rilevanti ai sensi del Decreto Legislativo 231/01;
- violazioni del Modello, del Codice etico o di Protocolli preventivi da cui possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto;
- sospetti di violazioni del Modello, del Codice etico o di Protocolli preventivi da cui possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto;
- operazioni societarie o di business per cui si sospetta possa derivare un rischio sanzionatorio per la Società ai sensi del Decreto.

9.3.3 Modalità di trasmissione e valutazione dei flussi informativi e delle segnalazioni

Con riferimento alle modalità di trasmissione delle informazioni/dati/notizie valgono le seguenti prescrizioni.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 60 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

I Flussi informativi debbono pervenire all'Organismo di Vigilanza ad opera dei responsabili delle diverse funzioni aziendali mediante le modalità definite dall'Organismo medesimo, tra cui la posta elettronica alla casella:

odv@biscottigentilini.it

oppure indirizzate tramite posta ordinaria a:

Organismo di Vigilanza ex D.Lgs. 231/2001

C/o Biscotti P. Gentilini Srl

Via Tiburtina 1302

00131 Roma

Le Segnalazioni che hanno ad oggetto l'evidenza o il sospetto di violazioni del Modello, del Codice etico o dei Protocolli Preventivi devono pervenire mediante l'apposito sistema di segnalazione predisposto dalla Società.

Le modalità di valutazione e gestione delle segnalazioni è disciplinata da apposita procedura e dal Regolamento di funzionamento dell'Organismo di Vigilanza.

9.3.4 Obblighi e requisiti del sistema di segnalazione (whistleblowing)

Tutti i Destinatari (quali a mero titolo di esempio: Apicali, Sottoposti e terzi che operano nell'interesse o vantaggio della Società), hanno l'obbligo di presentare, a tutela dell'integrità della Società, segnalazioni circostanziate di eventuali condotte illecite, rilevanti ai sensi del D. Lgs. 231/2001, che in buona fede, sulla base della ragionevole convinzione fondata su elementi di fatto, ritengano essersi verificate o di violazioni del Modello di organizzazione e gestione adottato dalla Società, di cui siano venuti a conoscenza in ragione delle funzioni svolte.

Le segnalazioni dovranno essere circostanziate e fondate su elementi di fatto precisi e concordanti.

Il Sistema di segnalazione whistleblowing è organizzato attraverso specifica procedura e un canale alternativo di comunicazione/segnalazione, diverso dal canale inerente i flussi informativi (questi ultimi interni ai sistemi informatici e telematici aziendali), idoneo a garantire, anche con modalità informatiche, la riservatezza dell'identità del segnalante.

In tale ottica, il canale predefinito è una casella di posta elettronica certificata esterna, a cui potranno accedere solamente i componenti dell'Organismo di Vigilanza.

Destinatari Apicali hanno il divieto di porre in essere atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

Oltre alle segnalazioni sopra descritte, devono essere obbligatoriamente trasmesse all'OdV, tramite i già citati canali di posta elettronica e di posta ordinaria:

- le informazioni espressamente individuate nella Parte Speciale del presente documento;
- le notizie relative ai procedimenti disciplinari e alle sanzioni erogate ovvero ai provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 61 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

9.3.5 Disciplina del segreto

Nelle ipotesi di segnalazione o denuncia effettuate nelle forme e nei limiti di cui al presente Modello 231 e dettagliati dalla procedura in materia di whistleblowing, il perseguimento dell'interesse all'integrità delle amministrazioni pubbliche e private, nonché alla prevenzione e alla repressione delle malversazioni e degli atti illeciti, costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli articoli 326, 622 e 623 del codice penale e all'articolo 2105 del codice civile (come previsto dalla legge vigente).

Quando notizie e documenti che sono comunicati all'organo deputato a riceverli dalla procedura whistleblowing siano oggetto di segreto aziendale, professionale o d'ufficio, costituisce comunque violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori del canale di comunicazione specificamente predisposto a tal fine.

Resta invece fermo l'obbligo di rispettare il segreto professionale e di ufficio per chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale o di assistenza con la Società o gli organi e funzioni preposte alla gestione delle segnalazioni, le quali nel rispetto della vigente procedura whistleblowing (e nell'ambito della propria autonomia e indipendenza) abbiano chiesto pareri specialistici a supporto.

9.3.6 Libri dell'Organismo di Vigilanza

L'OdV stabilisce, tramite il proprio regolamento, le modalità di verbalizzazione delle attività eseguite; tali modalità tengono conto degli obblighi di riservatezza circa i nominativi degli eventuali segnalanti e delle istruttorie di verifica e della facoltà, in capo al Collegio Sindacale ed al Consiglio di Amministrazione, di consultare i soli verbali delle riunioni e le relazioni periodiche.

Ogni informazione, segnalazione, report previsti nel presente Modello sono conservati dall'OdV per un periodo di 10 anni in un'apposita partizione del file server aziendale accessibile dai soli componenti dell'OdV, ovvero in un apposito archivio cartaceo ad accesso selezionato e limitato ai soli stessi componenti dell'OdV.

Le chiavi di accesso all'archivio cartaceo saranno attribuite ai soli componenti dell'OdV, che dovranno restituirle immediatamente al termine del loro incarico per qualsiasi motivo ciò avvenga.

L'accesso ai documenti informatici dell'OdV con poteri di lettura e scrittura dovrà essere consentito esclusivamente ai membri dell'Organismo di Vigilanza stesso.

Interessi dei componenti dell'Organismo di Vigilanza nelle decisioni dell'Organismo stesso

Le modalità di assunzione delle decisioni nel caso in cui uno o più componenti dell'Organismo di Vigilanza siano portatori di un interesse, diretto o indiretto, rispetto ad una decisione da assumere, sono disciplinate all'interno del Regolamento dell'Organismo; per tali casi l'OdV prevede opportuni obblighi di motivazione.

Segnalazioni aventi ad oggetto un componente dell'Organismo di Vigilanza

Le modalità di gestione delle segnalazioni che riguardano uno o più componenti dell'Organismo di Vigilanza sono disciplinate all'interno della procedura whistleblowing.

In tali casi sono previste idonee attività di informazione, verifica ed intervento di altri organi di controllo della Società che assicurano la correttezza dei processi e delle decisioni

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 62 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

9.3.7 Registrazione delle segnalazioni

L'Organismo di Vigilanza stabilisce, tramite il proprio regolamento, le modalità di registrazione delle segnalazioni relative alle violazioni del Modello o di un Protocollo (disciplinate altresì dalla procedura whistleblowing); tali modalità tengono conto degli obblighi di riservatezza circa i nominativi degli eventuali segnalanti e delle istruttorie di verifica, al fine di garantire che tali dati e informazioni non siano consultabili da persone diverse dagli stessi componenti dell'OdV.

9.3.8 Obblighi di informazione da parte dell'Organismo di Vigilanza

Nello svolgimento delle proprie attività, l'Organismo di Vigilanza:

- informa il Presidente ed il Consiglio di Amministrazione nel più breve tempo possibile circa le segnalazioni ricevute e le violazioni rilevate in merito a eventi che potrebbero ingenerare responsabilità della Società ai sensi del D. Lgs. 231;
- presenta al Consiglio di Amministrazione (e dopo avere acquisito gli opportuni riscontri dalle strutture interne) una relazione periodica in ordine alle attività di verifica e controllo compiute e dell'esito delle medesime;
- sottopone all'organo dirigente, in tale occasione:
 - le carenze organizzative o procedurali rilevate e tali da esporre la Società al pericolo che siano commessi reati rilevanti ai fini del Decreto;
 - la necessità di apportare modifiche e/o aggiornamenti al Modello;
 - le azioni correttive, necessarie o eventuali, da apportare al fine di assicurare l'efficacia e l'effettività del Modello;
 - lo stato di attuazione delle azioni correttive precedentemente deliberate;
- informa, con appropriata tempistica, il Presidente del Consiglio di Amministrazione, mediante la presentazione di rapporti scritti concernenti aspetti puntuali e specifici della propria attività, ritenuti di particolare rilievo e significato nel contesto dell'attività di prevenzione e controllo;
- riferisce agli organi sopra menzionati specifici fatti od accadimenti, ogni qualvolta lo ritenga opportuno;
- riferisce al Presidente circa l'eventuale mancata o carente collaborazione da parte delle funzioni interne nell'espletamento dei propri compiti di verifica e/o d'indagine.

Sono rimesse all'Organismo la calendarizzazione e la regolamentazione della propria attività, ai fini di rispettare i requisiti di continuità d'azione richiesti dalla legge.

Le funzioni interne potranno rapportarsi con l'O.d.V. con la tempistica concordata in funzione delle necessità, per riportare in merito a specifici fatti od accadimenti o per discutere di argomenti ritenuti di particolare rilievo nel contesto della funzione di prevenzione di reati.

Gli incontri dell'Organismo di Vigilanza con il Consiglio di Amministrazione devono essere verbalizzati ed i relativi verbali conservati presso l'ente.

10 IL SISTEMA SANZIONATORIO

10.1 Caratteristiche del sistema sanzionatorio

Conformemente alle prescrizioni contenute all'art. 6, punto 2 lett. e) del Decreto ed alle indicazioni di Confindustria, che ha ritenuto nelle proprie Linee Guida l'apparato sanzionatorio quale punto cardine del Modello, è previsto il sistema disciplinare di seguito descritto che prevede apposite sanzioni per la violazione di quanto contenuto nel o richiamato dal Modello, al fine della prevenzione dei reati di cui al Decreto.

Pertanto le norme disciplinari che regolano il rapporto di lavoro a qualsiasi titolo prestato a favore della Società sono integrate da quanto qui previsto.

Ne consegue che saranno considerati come illeciti disciplinari tutte le condotte commissive o omissive, anche colpose, ivi compresa l'omessa informativa all'Organismo di Vigilanza, idonee a ledere l'efficacia del Modello e che a tali condotte saranno applicate le sanzioni di seguito indicate, ferme restando le previsioni di cui alla contrattazione collettiva, ove applicabili.

Il presente sistema sanzionatorio opera nel rispetto delle norme vigenti, incluse quelle previste nella contrattazione collettiva, ove applicabili, ed è aggiuntivo rispetto alle norme di legge o di regolamento vigenti, nonché integrativo delle altre norme di carattere interno, ivi incluse quelle di natura disciplinare.

L'applicazione del sistema è autonoma rispetto allo svolgimento e all'esito del procedimento giudiziario eventualmente avviato presso l'autorità competente.

I soggetti destinatari del presente sistema sanzionatorio potranno esercitare tutti i diritti – ivi inclusi quelli di contestazione o di opposizione avverso il provvedimento disciplinare, ovvero di costituzione di un Collegio Arbitrale – loro riconosciuti da norme di legge o di regolamento, nonché dalla contrattazione, inclusa quella collettiva, e/o dai regolamenti interni.

L'applicazione del sistema sanzionatorio può essere oggetto di richieste di informazioni e di verifiche da parte dell'Organismo di Vigilanza.

Resta inoltre stabilito che il sistema sanzionatorio di seguito riportato è applicabile anche in caso di violazione delle norme in materia di tutela della Salute e della Sicurezza nei luoghi di lavoro; ciò in quanto non siano state previste sanzioni specifiche in caso di violazione delle norme di Prevenzione adottate dalla Società.

Le sanzioni vengono irrogate secondo quanto previsto nel successivo punto, nonché nella contrattazione collettiva, ove applicabile.

10.2 Criteri di graduazione delle sanzioni

L'individuazione del tipo di sanzione e la sua irrogazione avverranno nel rispetto del principio di proporzionalità e di adeguatezza.

Nello stabilire il tipo e l'entità della sanzione verrà tenuto conto:

- dell'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- del comportamento complessivo del lavoratore, con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- delle altre particolari circostanze che accompagnano la violazione disciplinare, quali modalità della condotta e circostanze nel cui ambito si è sviluppata.

La gravità della condotta sarà valutata, in ordine crescente, a seconda che si tratti di:

- violazione del Modello che, oltre l'elemento oggettivo, integra anche l'elemento soggettivo della colpa lieve;
- violazione del Modello realizzata nell'ambito delle aree a rischio reato "minimo" o "contenuto", cioè evidenziate in colore bianco o verde nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave;
- violazione del Modello realizzata nell'ambito delle aree classificate a rischio "moderato" o "critico", cioè evidenziate in colore giallo o rosso nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave;
- violazione del Modello che integra l'elemento oggettivo e quello soggettivo del dolo, che determina il verificarsi di un reato per il quale il Decreto non prevede la comminabilità di sanzioni interdittive (per l'elenco dei reati che non prevedono sanzioni interdittive si rinvia all'allegato 1);
- violazione del Modello che integra l'elemento oggettivo e quello soggettivo del dolo, che determina il verificarsi di un reato per il quale il Decreto prevede la comminabilità di sanzioni interdittive (per l'elenco dei reati che prevedono sanzioni interdittive si rinvia all'allegato 1).

Parimenti, relativamente al settore della salute e sicurezza sul lavoro, la gravità della condotta sarà valutata, in ordine crescente, a seconda che si tratti di:

- violazione del Modello che determini una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione;
- violazione del modello che determini una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione;
- violazione del modello che determini una lesione qualificabile come grave (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione;
- violazione del modello che determini una lesione qualificabile come gravissima (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione, ovvero la morte.

Saranno considerate circostanze aggravanti:

- la recidiva;
- il livello di responsabilità assegnato dall'inquadramento contrattuale e organizzativo;
- il concorso di più persone nella commissione della violazione;
- una condotta che dia luogo a più violazioni, la più grave delle quali sarà oggetto dell'aggravamento della sanzione.

10.3 Misure nei confronti dei lavoratori dipendenti

Le sanzioni irrogabili nei riguardi dei lavoratori dipendenti sono quelle previste dal sistema disciplinare in vigore, in attuazione di quanto disposto dall'articolo 7 della Legge 20 maggio 1970, n. 300 e con riferimento a quanto previsto in materia disciplinare dal CCNL applicato, ovvero il "contratto collettivo nazionale di lavoro per i lavoratori dell'industria alimentare".

Incorre nel provvedimento dell'ammonizione, verbale o scritta, il dipendente, nel caso di:

- inosservanza e/o violazione di norme contrattuali o di direttive ed istruzioni impartite dalla direzione o dai superiori, o in generale dalla Società, con comportamenti quindi non conformi alle prescrizioni del presente Modello;

- negligenza nell'espletamento delle attività lavorative, correlata alle prescrizioni del presente Modello, che comportino la violazione del Modello che, oltre l'elemento oggettivo, integra anche l'elemento soggettivo della colpa lieve, ovvero che determini una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione.

Incorre nel provvedimento della multa di importo fino ad un massimo di 3 ore di retribuzione, il dipendente, nel caso di:

- inosservanza e/o violazione di norme contrattuali o di direttive ed istruzioni impartite dalla direzione o dai superiori, o in generale dalla Società, con comportamenti quindi non conformi alle prescrizioni del presente Modello;
- negligenza nell'espletamento delle attività lavorative, correlata alle prescrizioni del presente Modello, che comportino la violazione del Modello realizzata nell'ambito delle aree a rischio reato "minimo" o "contenuto", cioè evidenziate in colore bianco o verde nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave, ovvero che determini una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione.

Incorre nel provvedimento della sospensione dal lavoro e dalla retribuzione per un periodo non superiore a 3 giorni di effettivo lavoro il dipendente, nel caso di:

- inosservanza e/o violazione di norme contrattuali o di direttive ed istruzioni impartite dalla direzione o dai superiori, o in generale dalla Società, con comportamenti quindi non conformi alle prescrizioni del presente Modello;
- negligenza nell'espletamento delle attività lavorative, correlata alle prescrizioni del presente Modello che comportino la violazione del Modello realizzata nell'ambito delle aree classificate a rischio "moderato" o "critico", cioè evidenziate in colore giallo o rosso nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave, ovvero che determini una lesione qualificabile come grave (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione.

Incorre nel provvedimento del licenziamento senza preavviso ma con trattamento di fine rapporto il dipendente, nel caso di:

- inosservanza e/o violazione di norme contrattuali o di direttive ed istruzioni impartite dalla direzione o dai superiori, o in generale dalla Società, con comportamenti quindi non conformi alle prescrizioni del presente Modello;
- negligenza nell'espletamento delle attività lavorative, correlata alle prescrizioni del presente Modello, che comportino la violazione del Modello che integra l'elemento oggettivo e quello soggettivo del dolo, e che determina il verificarsi di un reato per il quale il Decreto non prevede la comminabilità di sanzioni interdittive (per l'elenco dei reati che non prevedono sanzioni interdittive si rinvia all'allegato 1).
- condotta in violazione del Modello di gravità tale da far venire meno la fiducia sulla quale è basato il rapporto di lavoro e da non consentire comunque la prosecuzione, nemmeno provvisoria, del rapporto stesso per comportamenti non conformi alle prescrizioni del presente Modello, che integra l'elemento oggettivo e quello soggettivo del dolo, che determina il verificarsi di un reato per il quale il Decreto prevede la comminabilità di sanzioni interdittive (per l'elenco dei reati che prevedono sanzioni interdittive si rinvia all'allegato 1), ovvero realizzata in modo da determinare una lesione qualificabile come gravissima (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione, ovvero la morte.

10.4 Misure nei confronti dei dirigenti

Se nell'espletamento di attività il dirigente adotta una condotta ed un comportamento non conformi alle prescrizioni del Modello stesso, ivi compresa l'omessa informativa all'Organismo di Vigilanza, ovvero non esercita un'adeguata direzione e/o vigilanza sui soggetti a lui sottoposti, si provvederanno ad applicare nei confronti del responsabile le misure più idonee, in conformità a quanto previsto dal "contratto collettivo nazionale Dirigenti di aziende produttrici di beni e servizi" e dalle disposizioni di Legge (ad es. artt. 2118 e 2119 del Codice Civile).

In particolare, saranno applicate le seguenti sanzioni, fatte salve eventuali diverse previsioni nell'ambito della contrattazione collettiva applicabile:

- il richiamo verbale, nei seguenti casi:
 - a) in caso di violazione del Modello che, oltre l'elemento oggettivo, integra anche l'elemento soggettivo della colpa lieve, ovvero che determina una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione;
 - b) in caso di violazione del Modello realizzata nell'ambito delle aree a rischio reato "minimo" o "contenuto", cioè evidenziate in colore bianco o verde nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave, ovvero che determini una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione;
- il richiamo scritto, in caso di violazione del Modello realizzata nell'ambito delle aree classificate a rischio "moderato" o "critico", cioè evidenziate in colore giallo o rosso nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave, ovvero che determini una lesione qualificabile come grave (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione;
- il licenziamento, nel caso di condotta in violazione del Modello di gravità tale da far venire meno la fiducia sulla quale è basato il rapporto di lavoro e da non consentire comunque la prosecuzione, nemmeno provvisoria, del rapporto stesso per comportamenti non conformi alle prescrizioni del presente Modello, che integra l'elemento oggettivo e quello soggettivo del dolo, ovvero realizzata in modo da determinare una lesione qualificabile come gravissima (v. art. 583, 1° co., Codice Penale) all'integrità fisica di una o più persone, incluso l'autore della violazione, ovvero la morte.

10.5 Misure nei confronti degli Amministratori e dei componenti l'Organo di controllo

Qualora sia accertata la commissione di una violazione del presente Modello da parte di uno dei soggetti in discorso, saranno applicate le seguenti sanzioni:

- il richiamo scritto, in caso di violazione del Modello che, oltre l'elemento oggettivo, integra anche l'elemento soggettivo della colpa lieve, ovvero che determina una situazione di concreto pericolo per l'integrità fisica di una o più persone, incluso l'autore della violazione;
- la diffida al puntuale rispetto del Modello, in caso di violazione del Modello realizzata nell'ambito delle aree a rischio reato "minimo" o "contenuto", cioè evidenziate in colore bianco o verde nel campo "indice di rischio residuo" (v. Parte Speciale) che, oltre all'elemento oggettivo, integra anche l'elemento soggettivo della colpa grave, ovvero che determini una lesione all'integrità fisica di una o più persone, incluso l'autore della violazione;
- la decurtazione degli emolumenti, o del corrispettivo previsto in favore dell'Organo di controllo, fino al 50%, in caso di violazione del Modello realizzata nell'ambito delle aree classificate a rischio "moderato"

o “critico”, cioè evidenziate in colore giallo o rosso nel campo “indice di rischio residuo” (v. Parte Speciale) che, oltre all’elemento oggettivo, integra anche l’elemento soggettivo della colpa grave, ovvero che determini una lesione qualificabile come grave (v. art. 583, 1° co., Codice Penale) all’integrità fisica di una o più persone, incluso l’autore della violazione;

- la revoca dall’incarico, nel caso di condotta in violazione del Modello di gravità tale da far venire meno la fiducia sulla quale è basato il rapporto e da non consentire comunque la prosecuzione, nemmeno provvisoria, del rapporto stesso per comportamenti non conformi alle prescrizioni del presente Modello, che integra l’elemento oggettivo e quello soggettivo del dolo, ovvero realizzata in modo da determinare una lesione qualificabile come gravissima (v. art. 583, 1° co., Codice Penale) all’integrità fisica di una o più persone, incluso l’autore della violazione, ovvero la morte.

Qualora la violazione sia contestata ad un Amministratore legato alla Società da un rapporto di lavoro subordinato, saranno applicate le sanzioni previste per i dirigenti (vedi sopra).

Se applicata la sanzione del licenziamento, l’amministratore sarà anche revocato dall’incarico.

10.6 Misure nei confronti dei collaboratori esterni

Per collaboratore esterno si intende il personale non dipendente della Società, ma ad esso collegato con rapporto di lavoro parasubordinato.

Le sanzioni previste nei loro confronti sono:

- la diffida al puntuale rispetto del Modello nel caso di violazioni del Modello, ovvero violazioni idonee ad integrare l’elemento oggettivo (fatto) di uno dei reati rilevanti ai sensi del Decreto e l’elemento soggettivo della colpa lieve, ovvero una situazione di concreto pericolo per l’integrità fisica o una lesione all’integrità fisica di una o più persone, incluso l’autore della violazione;
- l’applicazione di una penale in misura pari al 10% del corrispettivo pattuito in favore del collaboratore, nel caso di violazioni idonee ad integrare oltre all’elemento oggettivo (fatto) di uno dei reati rilevanti ai sensi del Decreto anche l’elemento soggettivo della colpa grave, ovvero che determinino una lesione (v. art. 583, 1° co., Codice Penale), all’integrità fisica di una o più persone, incluso l’autore della violazione;
- la risoluzione del rapporto contrattuale nel caso di violazioni idonee ad integrare oltre all’elemento oggettivo (fatto) di uno dei reati rilevanti ai sensi del Decreto anche l’elemento soggettivo del dolo, ovvero che determinino una lesione qualificabile come gravissima (v. art. 583, 1° co., Codice Penale) all’integrità fisica di una o più persone, incluso l’autore della violazione, ovvero la morte.

10.7 Misure nei confronti dei fornitori, partner e consulenti

Ogni violazione delle regole di cui al presente Modello applicabili nei confronti di fornitori, partner e consulenti, ovvero ogni commissione dei reati previsti dal Decreto, è sanzionata secondo quanto indicato nelle specifiche clausole contrattuali da inserirsi nei relativi contratti.

10.8 Rivalsa per risarcimento danni

In ogni caso resta salva l’eventuale richiesta di risarcimento, qualora dai comportamenti sanzionabili derivino danni concreti alla Società, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal Decreto.

10.9 L'irrogazione delle sanzioni

10.9.1 Premessa

Il procedimento di irrogazione delle sanzioni si sviluppa attraverso:

- la fase della contestazione della violazione al soggetto interessato;
- la fase di determinazione e di successiva irrogazione della sanzione.

Si indicano di seguito le procedure di riferimento.

10.9.2 Lavoratori Dipendenti

Fase di contestazione

Il processo sanzionatorio disciplinare ha inizio con la segnalazione effettuata al Responsabile Risorse Umane:

- dall'Organismo di Vigilanza; in questo caso nasce da quanto rilevato a seguito di una sua attività ispettiva o similare o da una segnalazione acquisita;
- dal Responsabile di funzione o da qualsiasi altro superiore gerarchico altrimenti denominato ("Responsabile"): in questo caso il Responsabile Risorse Umane provvede ad informare l'Organismo di Vigilanza, il quale potrà effettuare una eventuale, ulteriore attività ispettiva.

Il valutatore valuta i fatti con il supporto dell'Organismo di Vigilanza, anche sulla base di eventuali informazioni aggiuntive richieste al Responsabile. A seguito di questa valutazione, qualora non sussistano gli estremi, procederà con l'archiviazione; in caso contrario, passerà alla fase della contestazione scritta della violazione.

La comunicazione dovrà contenere la puntuale indicazione della condotta contestata e delle previsioni del Modello oggetto di violazione nonché l'avviso della facoltà di formulare eventuali deduzioni e/o giustificazioni scritte entro cinque giorni dalla ricezione della comunicazione.

Fase di determinazione ed irrogazione


Valutate le eventuali controdeduzioni (sempre con il supporto dell'Organismo di Vigilanza) la Direzione Generale passerà se del caso, in base a informazioni del Responsabile Risorse Umane, alla fase della determinazione e applicazione della sanzione.

Il dipendente ha tempo cinque giorni dal ricevimento della contestazione per le controdeduzioni; la Società, dal ricevimento delle controdeduzioni, ha tempo sei giorni per irrogare il provvedimento disciplinare.

Il Responsabile Risorse Umane verifica l'applicazione della sanzione nel rispetto delle norme di legge e di regolamento, dei regolamenti interni laddove applicabili, nonché delle previsioni di cui alla contrattazione collettiva.

Il dipendente sanzionato avrà facoltà di adire l'autorità giudiziaria ovvero di promuovere la costituzione di un Collegio di conciliazione ed arbitrato. In tal caso la sanzione disciplinare resta sospesa fino alla pronuncia dell'autorità giudiziaria ovvero del Collegio.

L'Organismo di Vigilanza dovrà essere tenuto informato dalla Direzione Generale dell'irrogazione della sanzione e delle eventuali, successive azioni del dipendente.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 69 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

10.9.3 Dirigenti

In tale caso si seguirà la stessa procedura sopra prevista, salvo che le sanzioni saranno deliberate direttamente dal Consiglio di Amministrazione.

Inoltre, qualora il dirigente destinatario dell'eventuale provvedimento sia un soggetto attivo nel procedimento sopra descritto, le attività di cui sopra a lui demandate saranno svolte dal superiore gerarchico ovvero dal Consiglio di Amministrazione.

10.9.4 Amministratori e componenti l'Organo di controllo

Fase della contestazione

Ove un Amministratore non legato alla Società da rapporto di lavoro subordinato violasse il modello, chiunque rilevasse tale violazione deve darne informativa all'Organismo di Vigilanza.

Questi, effettuati i necessari accertamenti nel tempo più breve, trasmetterà al Consiglio di Amministrazione ed all'Organo di controllo una relazione contenente le seguenti indicazioni:

- identificazione del soggetto responsabile;
- descrizione della condotta con cui sarebbe avvenuta la violazione e delle previsioni del Modello violate;
- documentazione raccolta e altri elementi comprovanti la violazione;
- un'eventuale proposta di sanzione.

Il Presidente del Consiglio di Amministrazione – o i suoi componenti, qualora la segnalazione riguardasse il Presidente stesso – deve, entro sette giorni lavorativi dalla ricezione della relazione dell'Organismo di Vigilanza, inviare una comunicazione al soggetto interessato. La comunicazione deve essere effettuata per iscritto e deve contenere gli estremi della condotta contestata e delle previsioni del Modello che sarebbero state violate, dando facoltà all'interessato di formulare rilievi e/o deduzioni di confutazione.

Fase di determinazione ed irrogazione


Il Presidente del Consiglio di Amministrazione deve inoltre convocare il Consiglio, in tempo utile affinché l'adunanza si tenga entro trenta giorni dalla ricezione della relazione dell'Organismo di Vigilanza. Nel corso di questa adunanza, alla quale dovrà essere invitato a partecipare anche l'Organismo di Vigilanza, dovrà essere disposta l'audizione dell'interessato, che potrà anche presentare le proprie controdeduzioni. Qualora non fossero necessari ulteriori accertamenti, e l'esito comprovasse l'avvenuta violazione, il Consiglio determinerà la sanzione da applicarsi e ne fornirà la motivazione; provvederà inoltre a convocare l'Assemblea per le deliberazioni di sua competenza, ove la sanzione consistesse nella decurtazione degli emolumenti o nella revoca dall'incarico.

Qualora necessitassero invece ulteriori accertamenti, il Presidente riconvocherà il Consiglio per un'adunanza da tenersi entro trenta giorni; quest'ultima dovrà concludersi o con l'archiviazione o con l'irrogazione della sanzione.

Il procedimento sopra descritto trova applicazione, *mutatis mutandis*, anche qualora sia riscontrata la violazione del Modello da parte di un componente dell'Organo di revisione, nei limiti consentiti dalle norme di legge applicabili.

10.9.5 Collaboratori esterni

Ove un collaboratore esterno violasse il Modello, chiunque rilevasse tale violazione deve darne informativa all'Organismo di Vigilanza.

	MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL D. LGS. 231/2001 E S.M.I. ESTRATTO	Pagina 70 di 70
		Edizione 03 – Settembre 2022
		Emittente: C.d.A.

Questi, effettuati i necessari accertamenti nel tempo più breve, trasmetterà al Responsabile della funzione che gestisce il rapporto contrattuale in questione ed al Responsabile Risorse Umane, una relazione contenente le seguenti indicazioni:

- identificazione del soggetto responsabile;
- descrizione della condotta con cui sarebbe avvenuta la violazione e delle previsioni del Modello violate;
- la documentazione raccolta e gli altri elementi comprovanti la violazione;
- un'eventuale proposta di sanzione.

Il Responsabile Risorse Umane deve, entro sette giorni lavorativi dalla ricezione della relazione dell'Organismo di Vigilanza, inviare una comunicazione al collaboratore interessato. La comunicazione deve essere effettuata per iscritto e deve contenere gli estremi della condotta contestata e delle previsioni del Modello che sarebbero state violate, dando facoltà all'interessato di formulare rilievi e/o deduzioni di confutazione entro sette giorni dalla ricezione.

Trascorso detto termine, tale funzione, valutate anche le controdeduzioni, comunicherà all'interessato ed all'Organismo di Vigilanza l'esito della procedura e l'eventuale irrogazione della sanzione ritenuta adeguata.

La Direzione Generale provvederà quindi all'effettiva applicazione della sanzione stessa nel rispetto delle norme di legge e di regolamento.

10.9.6 Fornitori, partner e consulenti

La Società applicherà le procedure interne previste in caso di risoluzione contrattuale, ma dell'eventuale irrogazione della sanzione dovranno essere informati, oltre all'Organismo di Vigilanza, anche il Consiglio di Amministrazione e l'Organo di controllo.

10.10 Conoscibilità

Per garantirne la piena conoscenza da parte di ogni destinatario, il presente sistema sanzionatorio:

- viene affisso in bacheca ed è tenuto a disposizione presso il Responsabile Risorse Umane;
- viene consegnato o inviato per via telematica ai soggetti in posizione apicale ed ai componenti gli organi societari;
- per quanto di pertinenza, ne viene data appropriata informativa ai collaboratori, consulenti, partner e fornitori.