Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. n. 231 dell'8 giugno 2001

- PARTE GENERALE -

INDICE	

DEFINIZIONI	
Attività a Rischio	Processo, operazione, atto, ovvero insieme di operazioni e atti, che possono esporre Datalogic al rischio di commissione di un Reato
CCNL	Contratti Collettivi Nazionali di Lavoro applicati da Datalogic
Codice di Autodisciplina	Codice di autodisciplina delle società quotate, nell'ultima versione approvata nel 2015, dal Comitato per la *Corporate Governance* e promosso da Borsa Italiana, il cui testo integrale risulta reperibile sul sito web www.borsaitaliana.it
Codice Etico	Codice etico adottato dal Gruppo e approvato dal Consiglio di Amministrazione di Datalogic in data 4 novembre 2009 e relativi aggiornamenti, il cui testo integrale risulta reperibile sul sito web www.datalogic.com
Consulenti	Soggetti che agiscono in nome e/o per conto di Datalogic in forza di un contratto di mandato o di altro rapporto contrattuale di collaborazione professionale
Datalogic	Datalogic S.p.A., con sede in Calderara di Reno (Bologna), Via Marcello Candini n. 2, capitale sociale deliberato, sottoscritto e versato Euro 30.392.175,32, numero di iscrizione al Registro Imprese di Bologna e codice fiscale 01835711209, Repertorio Economico Amministrativo n. BO-391717
Decreto	Decreto Legislativo n. 231 dell'8 giugno 2001, come successivamente modificato
Destinatari	Organi Sociali, Dipendenti, Consulenti, Partner e Fornitori
Dipendenti	Soggetti aventi un rapporto di lavoro subordinato o parasubordinato con Datalogic, ivi compresi i dirigenti
Fornitori	Fornitori di beni e servizi di Datalogic che non rientrano nella definizione di Partner
Gruppo	Datalogic S.p.A. e le società dalla stessa controllate o alla stessa collegate
Illeciti	Illeciti amministrativi di abuso di informazioni privilegiate (art. 187-*bis* TUF) e di manipolazione del mercato (art. 187-*ter* TUF), per i quali è stato rilevato un apprezzabile livello di rischio rispetto alle

	attività esercitate da Datalogic
Modello	Modello di organizzazione, gestione e controllo adottato da Datalogic, ai sensi degli artt. 6 e 7 del Decreto
Organi Sociali	Il Consiglio di Amministrazione e il Collegio Sindacale di Datalogic
Organismo di Vigilanza	Organismo di natura collegiale preposto alla vigilanza sul funzionamento e sull'osservanza del Modello, nonché al relativo aggiornamento in Datalogic
Partner	Controparte contrattuale (inclusi i clienti) con la quale Datalogic ha instaurato un rapporto contrattualmente regolato, destinata a cooperare con Datalogic nell'ambito delle Attività a Rischio
Parte Generale	La parte del Modello contenente, tra le altre cose, la descrizione delle funzioni del Modello e dell'Organismo di Vigilanza, nonché una descrizione di Datalogic e del Gruppo
Parti Speciali	Le parti del Modello dedicate espressamente a ciascun Reato e Illecito, nelle quali vengono previste le relative procedure di prevenzione
Pubblica Amministrazione	La pubblica amministrazione e, con riferimento ai reati nei confronti della pubblica amministrazione, i pubblici ufficiali e gli incaricati di un pubblico servizio
Reati	Le fattispecie di reato alle quali si applica la disciplina prevista dal Decreto sulla responsabilità amministrativa. Nel Modello sono state prese in considerazione solo le fattispecie di reato per le quali è stato rilevato un apprezzabile livello di rischio rispetto alle attività esercitate da Datalogic
TUF	Decreto Legislativo n. 58 del 24 febbraio 1998 - "Testo unico delle disposizioni in materia di intermediazione finanziaria" -, come successivamente integrato e modificato

1. Il D.LGS. n. 231/2001 – *premessa.*

Il Governo italiano, in esecuzione della delega di cui alla Legge 29 settembre 2000, n. 300, con il D.Lgs. n. 231/2001, emanato in data 8 giugno 2001[1], recante la *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"*, ha adeguato la normativa italiana in materia di responsabilità delle persone giuridiche ad alcune Convenzioni Internazionali in precedenza sottoscritte dallo Stato Italiano[2].

Il Legislatore Delegato ha, dunque, introdotto nell'ordinamento giuridico italiano un sistema di responsabilità autonomo degli enti per gli illeciti conseguenti alla commissione di reati (che si aggiunge a quella della persona fisica che lo ha materialmente realizzato), caratterizzato da presupposti e conseguenze distinti da quelli previsti per la responsabilità penale della persona fisica.

L'ente, pertanto, può essere ritenuto responsabile se, prima della commissione del reato da parte di un soggetto ad esso funzionalmente collegato (vedi *infra*), non aveva adottato ed efficacemente attuato un proprio modello di organizzazione e gestione idoneo a evitare reati della specie di quello verificatosi.

In particolare, l'ente può essere ritenuto responsabile dell'illecito se il reato è stato posto in essere:

(i) da persone fisiche che rivestano funzioni di rappresentanza, di amministrazione o di direzione degli enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli enti medesimi *(c.d. soggetti in posizione apicale)*, nonché

(ii) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti indicati al punto sub (i) *(c.d. soggetti in posizione subordinata).*

Tale responsabilità si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto.

Perché possa configurarsi la responsabilità in capo alla società è inoltre necessario che la condotta illecita ipotizzata sia stata posta in essere dai soggetti individuati "nell'interesse o a vantaggio della Società[3], mentre tale responsabilità è espressamente

---

[1] Entrato in vigore il 4 luglio 2001.

[2] Convenzione OCSE (Organizzazione per la cooperazione e lo sviluppo economico) del 17 dicembre 1997 sulla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali. Convenzioni OCSE e Unione Europea contro la corruzione nel commercio internazionale e contro la frode ai danni della Comunità Europea. L'art. 11 della legge delega (legge 29 settembre 2000 n. 300), in particolare, delegava il Governo a disciplinare questo tipo di responsabilità.

[3] In tema di responsabilità da reato delle persone giuridiche e delle società, l'espressione normativa, con cui se ne individua il presupposto nella commissione dei reati "nel suo interesse o a suo vantaggio", non contiene un'endiadi, perché i termini hanno riguardo a concetti giuridicamente diversi, potendosi distinguere un interesse "a monte" per effetto di un indebito arricchimento, prefigurato e magari non realizzato, in conseguenza dell'illecito, da un vantaggio obiettivamente conseguito con la commissione del reato, seppure non prospettato ex ante, sicché l'interesse ed il vantaggio sono in concorso reale. Cassazione Penale Sez. II, 20.12.2005 n. 3615. Certamente il requisito dell'interesse o vantaggio dell'Ente, quale criterio di imputazione oggettiva della responsabilità dell'ente stesso, può essere integrato anche dal vantaggio

esclusa nel caso in cui il reato sia stato commesso "nell'interesse esclusivo proprio o di terzi".

Più precisamente la Corte di Cassazione ha affermato che l'Ente non risponde dell'illecito amministrativo dipendente da reato allorquando il fatto è commesso dal singolo nell'interesse esclusivo proprio o di terzi, non riconducibile nemmeno parzialmente all'interesse dell'Ente, ossia nel caso in cui non sia possibile configurare una immedesimazione fra la società ed i suoi organi. Ad eccezione di quanto sopra esposto, l'Ente non risponde per quanto ha commesso il suo dipendente/rappresentante se dimostra di avere adottato le misure necessarie per impedire la commissione dei reati del tipo di quello realizzato (adozione ed efficace attuazione del Modello).

La giurisprudenza ha poi sottolineato che la responsabilità prevista in capo all'Ente dal D. Lgs. 231/2001 discende da una "colpa nell'organizzazione" della persona giuridica (ex plurimis, Cass. pen. Sez. VI, 18-02-2010 - 16-07-2010, n. 27735). La mancata adozione del Modello, in presenza dei presupposti oggettivi e soggettivi sopra indicati (reato commesso nell'interesse o vantaggio della società e posizione apicale dell'autore del reato) è sufficiente a costituire quella rimproverabilità di cui alla Relazione Ministeriale al Decreto Legislativo e ad integrare la fattispecie sanzionatoria, costituita dall'omissione delle previste doverose cautele organizzative e gestionali idonee a prevenire talune tipologie criminose. In tale concetto di rimproverabilità è implicita una nuova forma "normativa" di colpevolezza per omissione organizzativa e gestionale, avendo il legislatore ragionevolmente tratto dalle concrete vicende occorse in questi decenni, in ambito economico ed imprenditoriale, la legittima e fondata convinzione della necessità che qualsiasi complesso organizzativo costituente un ente ex art 1 comma 2 D.lgs. 231/01, adotti modelli organizzativi e gestionali idonei a prevenire la commissione di determinati reati che l'esperienza ha dimostrato essere funzionali ad interessi strutturati e consistenti[4]. Tale "colpa di organizzazione" assume specifica rilevanza nell'ambito del cd. gruppo di società.

1.1 (segue): l'adozione del modello quale possibile esimente della responsabilità.

L'art. 6 del Decreto, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede, tuttavia, una forma specifica di esonero da detta responsabilità qualora l'ente dimostri che, in caso di reato commesso da soggetti *c.d. in posizione apicale:*

a) l'organo dirigente dell'ente ha adottato ed **efficacemente attuato**[5], prima della commissione del fatto, un modello di organizzazione e di gestione idoneo a prevenire i *reati presupposto* della specie di quello verificatosi;

---

indiretto, inteso come acquisizione per la società di una posizione di privilegio sul mercato derivante dal reato commesso dal soggetto apicale. Nondimeno, proprio la natura di criterio di imputazione della responsabilità riconosciuto dalla legge richiede la concreta e non astratta affermazione dell'esistenza di un tale interesse o vantaggio, da intendersi rispettivamente come potenziale o effettiva utilità, ancorché non necessariamente di carattere patrimoniale, derivante all'ente dalla commissione del reato presupposto. Tribunale di Milano – ordinanza 28.04.2008.

[4] Cassazione Penale Sezione VI – 9.07.2009 n. 36083.

[5] Requisito indispensabile perché dall'adozione del modello derivi l'esenzione da responsabilità dell'ente è che esso venga efficacemente attuato.

b) il compito di vigilare sul funzionamento e sull'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo;

c) le persone che hanno commesso i *reati presupposto* hanno agito eludendo fraudolentemente il suddetto modello;

d) non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla precedente lett. b).

Nel caso di reato commesso da soggetti in posizione subordinata, invece, l'adozione e l'efficace attuazione del modello importa che l'ente sia chiamato a rispondere solo nell'ipotesi in cui il reato sia stato reso possibile dall'inosservanza degli obblighi di direzione e vigilanza.

Il Decreto prevede, inoltre, che i modelli di cui alla lettera a), debbano rispondere alle seguenti esigenze:

a) individuare le attività nel cui ambito esiste la possibilità che vengano commessi i Reati e gli Illeciti;

b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai Reati e agli Illeciti;

c) individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali Reati e Illeciti;

d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;

e) introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

L'art. 7, commi 3 e 4, del Decreto introduce, infine, due principi che appaiono rilevanti e decisivi ai fini dell'esonero della responsabilità dell'ente, nel momento in cui viene espressamente previsto che:

a) il modello deve prevedere misure idonee sia a garantire lo svolgimento dell'attività nel rispetto della legge, sia a scoprire tempestivamente situazioni di rischio, tenendo in considerazione il tipo di attività svolta nonché la natura e la dimensione dell'organizzazione;

b) l'efficace attuazione del modello richiede una verifica periodica e la modifica dello stesso qualora siano scoperte significative violazioni delle prescrizioni di legge o qualora intervengano significativi mutamenti nell'organizzazione o normativi.

Si precisa, da ultimo, che, sotto un profilo meramente formale, l'adozione ed efficace attuazione di un modello non costituisce un obbligo, ma unicamente una facoltà per gli enti. Tuttavia, per le società le cui azioni risultino essere quotate presso il Segmento Titoli con Alti Requisiti (S.T.A.R.) del Mercato Telematico Azionario (M.T.A.) organizzato e gestito da Borsa Italiana S.p.A. (così come risultano essere le azioni di Datalogic),

l'adozione ed efficace attuazione di un modello è considerato un requisito fondamentale per la quotazione presso tale segmento.

1.2 (segue): i c.d. reati presupposto.

Non tutti i reati commessi dai soggetti sopra indicati implicano una responsabilità amministrativa riconducibile all'ente, atteso che ai sensi del Decreto sono individuate come rilevanti solo specifiche tipologie di reati *(c.d. reati presupposto)*. Deve considerarsi, inoltre, che il "catalogo" dei reati presupposto rilevanti ai sensi del Decreto è in continua espansione.

Per il dettaglio analitico dei reati presupposto attualmente in vigore si rimanda al quadro normativo di riferimento, pubblicato sulla Gazzetta Ufficiale (www.gazzettaufficiale.it).

Si sottolinea, tuttavia, come nelle Parti Speciali del presente Modello siano stati presi in considerazione solo i *reati presupposto* per i quali sia stato rilevato un apprezzabile livello di rischio rispetto alle attività esercitate da Datalogic e come sia in ogni caso demandato al Consiglio di Amministrazione di Datalogic il compito di integrare il presente Modello con ulteriori Parti Speciali relative ad altre tipologie di reati presupposto qualora, sulla base delle periodiche verifiche effettuate, risulti opportuno procedere in tale direzione.

1.3 (segue): le sanzioni.

Nell'ipotesi in cui i soggetti di cui alla premessa commettano uno dei *reati presupposto*, l'ente potrà essere soggetto alle seguenti sanzioni amministrative:

a) sanzioni pecuniarie;

b) sanzioni interdittive, quali:

   i) l'interdizione dall'esercizio dell'attività;

   ii) la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

   iii) il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;

   iv) l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

   v) il divieto di pubblicizzare beni e servizi.

c) confisca;

d) pubblicazione della sentenza.

Tali sanzioni interdittive possono essere adottate anche in sede cautelare.

L'Autorità Giudiziaria può, altresì, disporre:

1. il sequestro preventivo delle cose di cui è consentita la confisca;

2. il sequestro conservativo dei beni mobili e immobili dell'ente qualora sia riscontrata la fondata ragione di ritenere che manchino o si disperdano le garanzie per il pagamento della sanzione pecuniaria, delle spese del procedimento o di altre somme dovute allo Stato.

1.4 (segue): idoneità del Modello

Ai fini della redazione del modello e della conseguente valutazione di idoneità dello stesso è opportuno tenere conto della giurisprudenza (ancora assai scarsa) sul punto e dei criteri dalla stessa fissati; in particolare la Corte di Cassazione (andando di contrario avviso al GUP di Milano in data 17.11.2009 e alla Corte d'Appello di Milano in data 21.03.2012) ha statuito, in sintesi, che "un modello è idoneo quando le procedure a sostegno dello stesso sono idonee a evitare la commissione del reato presupposto".

È altresì importante sottolineare quanto statuito dal G.I.P. di Milano (dott. D'Arcangelo) novembre 2010. La pronuncia ha fissato il principio secondo il quale *"l'agire in conformità a legge è sottratto alla discrezionalità dell'imprenditore ed il rischio di non conformità non può rientrare tra i rischi accettabili da parte degli amministratori".*

Nella suddetta pronuncia si legge che *"il giudice chiamato a deliberare la idoneità di un modello organizzativo deve far riferimento alla disciplina di un determinato settore con riferimento al tempo della condotta criminosa in contestazione e verificare quali cautele organizzative siano state adottate dall'ente per scongiurare un dato fatto criminoso e come le stesse in concreto siano state attuate con riferimento al miglior sapere tecnico disponibile all'epoca" […] "il modello cautelare idoneo è, infatti, (come si desume, sul piano metodologico, anche dal contenuto precettivo dell'art. 30 del D.Lgs. 9.4.2008 n. 81) quello forgiato dalle migliori conoscenze, consolidate e condivise nel momento storico in cui è commesso l'illecito, in ordine ai metodi di neutralizzazione o di minimizzazione del rischio tipico".*

2. STRUTTURA DEL GRUPPO – *premessa*.

Il Gruppo Datalogic opera a livello mondiale nei mercati dell'acquisizione automatica dei dati e di automazione industriale. In particolare, l'azienda è specializzata nella progettazione e produzione di lettori di codici a barre, mobile computer, sensori per la rilevazione, misurazione e sicurezza, RFID, sistemi di visione e marcatura laser, con l'obiettivo di aumentare l'efficienza e la qualità dei processi nei settori grande distribuzione, manifatturiero, trasporti e logistica e sanità, lungo l'intera catena del valore.

La Struttura Organizzativa del Gruppo, prevede le seguenti società, incluse nel perimetro di applicazione del D.Lgs. 231/2001, direttamente o indirettamente controllate da Datalogic S.p.A.:

- **Datalogic S.r.l.**;
- **Datasensing S.r.l.;**
- **Datalogic IP TECH S.r.l..**

2.1 (segue): Datalogic S.r.l.

La società Datalogic S.r.l. svolge attività di progettazione, fabbricazione (anche su licenza), commercializzazione, vendita e distribuzione (ivi inclusi i relativi servizi di installazione, riparazione e manutenzione) dei prodotti - servizi del Gruppo Datalogic, ed in particolare:

- Apparecchiature elettroniche, e software e sistemi per la lettura, e riconoscimento, acquisizione, raccolta, elaborazione, monitoraggio, controllo, trasmissione e comunicazione di dati e voce di ogni e qualsivoglia tipo, ivi compresi dispositivi (fissi e/o portatili) di lettura di codici a barre (e/o di altre simbologie) e mobile computer per la raccolta, l'elaborazione e la trasmissione di dati e voce, sistemi di lettura a postazione fissa di codici a barre e/o di altre simbologie per qualsiasi tipologia di applicazione che consenta di generare e raccogliere i dati, elaborarli e trasmetterli;
- Sistemi di lettura, scrittura e trasmissione dati con tecnologia a radio frequenza (RFID) o con altra tecnologia;
- Sistemi a tecnologia laser per la marcatura, pulitura e/o saldatura di oggetti, e per applicazioni in campo medicale e della sicurezza;
- Sensori per la rilevazione, misurazione e sicurezza;
- Sistemi di visione;
- Sistemi di identificazione basati su immagini;
- Sistemi e software di controllo, gestione e configurazione di reti di apparecchiature;
- Software per la gestione dei punti di vendita.

Datalogic S.r.l. si avvale di diversi centri R&D (distribuiti in diversi paesi quali Italia, US e Cina) nonché di diversi poli produttivi (dislocati in Italia, Slovacchia, Vietnam e Ungheria), operando in oltre 30 paesi con presenza diretta, attraverso le proprie filiali e/o le proprie società (Europa, America, Asia e Oceania).

2.2 (segue): Datasensing S.r.l.

La società Datasensing S.r.l. svolge attività di ricerca, progettazione, fabbricazione, commercializzazione, vendita e distribuzione dei prodotti - servizi del Gruppo Datalogic, ed in particolare:

- Sistemi di visione e di identificazione basati su immagini
- Sensori per la rilevazione e la misurazione
- Sistemi ottici e laser per applicazioni in ambito della sicurezza

Datasensing S.r.l. si avvale di un centro R&D nonché di diversi poli produttivi (dislocati in Italia e Cina), operando in diversi paesi con presenza diretta, attraverso le proprie filiali e/o le proprie società.

2.3 (segue): Datalogic IP TECH S.r.l.

La Società IP TECH S.r.l. svolge attività relative allo sviluppo, coordinamento, organizzazione e svolgimento della ricerca avanzata nell'ambito del Gruppo Datalogic, attraverso:

- L'utilizzo e lo sfruttamento, in qualsivoglia forma, dei risultati ottenuti dalla ricerca;
- L'acquisizione e la messa a disposizione di tecnologie e know-how e la gestione di progetti tecnologici;
- La gestione, in qualsiasi forma, delle attività di tutela di brevetti, licenze, know how o altri diritti di proprietà intellettuale e industriale.

2.4 (segue): Gruppo Datalogic e responsabilità amministrativa ex D.Lgs. 231/2001

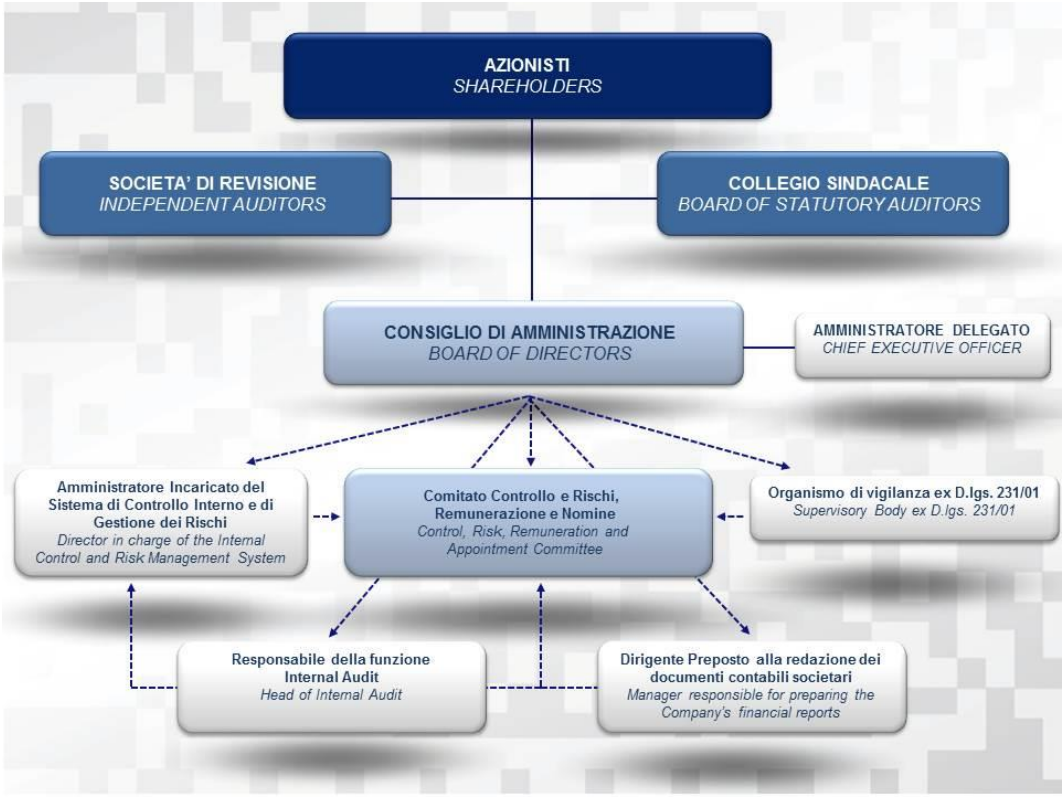
Quale Holding del Gruppo, Datalogic S.p.A., al fine di ulteriormente migliorare l'applicazione di quanto disposto dal Decreto, con il presente Modello ha ritenuto di adottare un "sistema 231" che costituisca, attraverso i suoi principi, il punto di riferimento per le altre società facenti parte del Gruppo. Il sistema è così sintetizzabile:

1. tutte le società italiane facenti parte del Gruppo Datalogic, controllate direttamente o indirettamente, hanno adottato, in autonomia ed in funzione delle proprie caratteristiche e struttura, nonché profilo di rischio, un Modello Organizzativo;
2. tale Modello, una volta adottato, è soggetto ad opportune implementazioni al fine di una sua più efficace attuazione;
3. per ciascuna società viene nominato un OdV idoneo, per composizione, competenza e funzionalità, rispetto a quanto previsto dal Decreto;
4. Datalogic S.p.A. esprime, a sua tutela, i criteri minimi del Modello Organizzativo adottato dalle varie società controllate, nonché i criteri di operatività dei vari OdV;
5. l'OdV di Datalogic S.p.A., deve, tra i suoi specifici compiti, monitorare, attraverso opportuni flussi informativi, che tutti gli OdV del Gruppo garantiscano una corretta azione di controllo, così come previsto dal Decreto.

3. CORPORATE GOVERNANCE - *Datalogic S.p.A.*

Datalogic rivolge costantemente particolare attenzione all'adeguatezza ed al funzionamento del proprio sistema di governo societario, procedendo nell'evoluzione delle strutture decisionali e di controllo in conformità alle *best practices* nazionali e internazionali in materia di *corporate governance*. Il sistema tradizionale di *corporate governance* adottato da Datalogic S.p.A., come delineato nella *flowchart* seguente, è ispirato ai principi di correttezza e trasparenza nella gestione e nell'informazione, realizzati anche attraverso un continuo processo di verifica della loro effettiva implementazione ed efficacia. Coerentemente con le peculiarità e le caratteristiche della propria struttura societaria, Datalogic aderisce al Codice di Autodisciplina nelle forme e nei termini indicati nella propria relazione sul governo societario e sugli assetti proprietari redatta ai sensi dell'art. 123-*bis* del TUF, consultabile sul sito web

www.datalogic.com - sezione *Governance*, il cui contenuto deve considerarsi parte integrante ed essenziale del Modello.



4. IL MODELLO DI DATALOGIC – *premessa*.

Il Gruppo Datalogic ha ritenuto di procedere all'adozione e attuazione del Modello nella convinzione che l'adozione di tale Modello possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto di Datalogic, affinché seguano, nell'espletamento delle proprie attività, dei comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei Reati e Illeciti.

Il Modello Datalogic - rappresentando un *"atto di emanazione dell'organo dirigente"* (ai sensi dell'art. 6, comma 1, lett. a), del Decreto) - è stato approvato per la prima volta dal Consiglio di Amministrazione della Società in data 12 maggio 2005, ed è stato successivamente fatto proprio dai successivi organi amministrativi che si sono, mano a mano, succeduti nel tempo, i quali hanno, tra l'altro, provveduto, su impulso dell'Organismo di Vigilanza, ad apportare al Modello una serie di integrazioni connesse, da un lato, all'evolversi della struttura organizzativa dell'imprese e, dall'altro, alle novità normative che hanno interessato la materia nel corso degli anni con l'introduzione di ulteriori fattispecie di reati presupposto[6].

[6] L'adozione e l'aggiornamento periodico del Modello sono il risultato dello svolgimento da parte del Consiglio di Amministrazione delle seguenti attività:

a) identificazione dell'ambito di operatività aziendale da ricomprendere nel Modello e mappatura delle Attività a Rischio da sottoporre ad analisi e monitoraggio;

Il Modello Organizzativo della Società, elaborato anche sulla base delle "Linee Guida" di Confindustria, si concretizza in un articolato sistema piramidale di principi e procedure, che si può descrivere sinteticamente come segue:

a) Parte generale, in cui viene genericamente descritto il Modello in termini di obiettivi, funzionamento e organi posti a presidio dello stesso;

b) Parte speciale, in cui sono elaborati tutti i processi operativi volti a prevenire la commissione di reati in ambito aziendale, e in particolare:

   i. Reati in danno della Pubblica Amministrazione;

   ii. Reati societari;

   iii. *Market abuse*;

   iv. Sicurezza sul lavoro;

   v. Ricettazione e riciclaggio;

   vi. Delitti informatici e trattamento illecito dei dati;

   vii. Reati tributari.

Per la definizione della Parte speciale "Sicurezza sul lavoro" sono stati assunti come riferimento gli *standard* internazionali ISO 45001:2018 per la parte riguardante la sicurezza e l'igiene degli ambienti di lavoro.

4.1 (segue): funzione del Modello.

Il Modello trova fondamento nel sistema strutturato e organico di procedure, nonché di attività di controllo (da svolgersi anche in via preventiva), implementato da Datalogic e volto a prevenire la commissione dei Reati e degli Illeciti.

In particolare, mediante l'individuazione delle Attività a Rischio, nonché delle procedure di controllo alle quali queste ultime sono sottoposte, il Modello si propone di:

---

b) analisi dei protocolli in essere con riferimento alle Attività a Rischio e definizione delle eventuali implementazioni finalizzate a garantire l'adeguamento alle prescrizioni del Decreto; in tale ambito, particolare attenzione è posta alla:
(i) definizione di principi etici in relazione ai comportamenti che possono integrare i Reati e/o gli Illeciti;
(ii) definizione dei processi di Datalogic nel cui ambito, in linea di principio, potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione di Reati e/o Illeciti;
(iii) definizione delle modalità di formazione dei Dipendenti;
(iv) definizione dell'informativa da fornire ai Destinatari;
(v) definizione e applicazione di disposizioni disciplinari idonee a sanzionare il mancato rispetto delle misure indicate nel Modello e dotate di idonea deterrenza;
c) identificazione dell'Organismo di Vigilanza ed attribuzione al medesimo di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello;
d) definizione dei flussi informativi nei confronti dell'Organismo di Vigilanza.

a) determinare, in tutti coloro che operano in nome e per conto di Datalogic, soprattutto nelle medesime Attività a Rischio, la consapevolezza di poter incorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale ed amministrativo, non solo nei propri confronti ma anche nei confronti di Datalogic;

b) ribadire che tali forme di comportamento illecito sono fortemente condannate da Datalogic in quanto (anche nel caso in cui Datalogic fosse apparentemente in condizione di trarne vantaggio) sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etico-sociali cui intende attenersi nell'espletamento della propria missione aziendale;

c) consentire a Datalogic, grazie ad un'azione di monitoraggio sulle Attività a Rischio, di intervenire tempestivamente per prevenire o contrastare la commissione dei Reati e degli Illeciti.

Quali specifici strumenti diretti a programmare la formazione e l'attuazione delle decisioni aziendali ed effettuare i controlli sull'attività di impresa, anche in relazione ai Reati e agli Illeciti da prevenire, Datalogic ha individuato:

1. le regole di *corporate governance* adottate in recepimento del Codice di Autodisciplina;
2. il Codice Etico;
3. il sistema di controllo interno;
4. il sistema sanzionatorio di cui ai CCNL.

4.2 (segue): mappatura delle Attività a Rischio.

Attraverso un'analisi della struttura operativa di Datalogic sono state individuate le principali Attività a Rischio, nonché le relative aree aziendali[7] ed i protocolli preventivi in essere. I risultati di tale analisi sono sinteticamente riportati nella tabella seguente.

[7] L'aggregazione funzionale delle aree – attività a rischio reato è rappresentativa dell'attuale disegno organizzativo – footprint operativo di Gruppo (consultabile sul sito internet www.datalogic.com – sezione *Organizzazione*).

Parti speciali	Attività a rischio reato	Aree aziendali a rischio reato								Protocolli preventivi			Risk Assessment Highlights	
		AFC	LEG & IP	IT	RU	SG	OP	COM	ST	ORG	PROC	SIS	Principale attività a rischio reato	Principali protocolli preventivi (in relazione all'attività riportata)
A	Reati contro la Pubblica Amministrazione	✓	✓		✓	✓			✓	✓	✓	✓	> Provvedimenti amministrativi strumentali allo svolgimento delle attività Societarie (autorizzazioni - certificazioni)	> Governance: AFC – SG – LEG & IP > Processi: selezione fornitori – acquisti indiretti – gestione pagamenti > Sistemi: contabile – informativo
B	Reati societari	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Rappresentazione in Bilancio degli eventi societari	> Governance: AFC – LEG & IP > Processi: financial reporting > Sistemi: contabile – informativo > Certificazioni: contabile – finanziaria
													> Operazioni straordinarie	> Governance: AFC – LEG & IP > Processi: informazioni privilegiate – operazioni straordinarie > Sistemi: contabile – informativo > Certificazioni: contabile – finanziaria
C	Market Abuse	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Informazioni privilegiate – operazioni straordinarie	> Governance: Direzione Aziendale – AFC – LEG & IP > Processi: inside information – internal dealing > Sistemi: contabile – informativo > Certificazioni: contabile – finanziaria
													> Informativa pubblica	> Governance: AFC – LEG & IP – COM > Processo: gestione eventi societari – comunicazione esterna > Sistemi: contabile – informativo > Certificazioni: contabile – finanziaria
D	Sicurezza sul lavoro	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> FacilityManagement	> Governance: SG – RU – LEG & IP > Processi: gestione presidi di sicurezza > Sistemi: contabile – informativo > Certificazioni: ISO 45001 – ISO 14001 – SA8000
E	Ricettazione e riciclaggio	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Transazioni commerciali	> Governance: OP – VM – AFC – LEG & IP > Processi: acquisti – pagamenti – vendite – incassi > Sistemi: contabile – informativo > Certificazioni: contabile – finanziaria
													> Transazioni finanziarie	> Governance: AFC – LEG & IP > Processi: gestione finanziaria > Sistemi: contabile – informativo > Certificazioni: contabile – finanziaria
F	Delitti informatici e trattamento illecito di dati	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Sicurezza informatica – infrastruttura interna	> Governance: IT – LEG & IP > Processi: gestione presidi di sicurezza IT (software – hardware) > Sistemi : contabile – informativo > Certificazioni: ISO 27001
													> Sicurezza informatica – prodotti e soluzioni	> Governance: RS – IT – LEG & IP > Processi: gestione presidi di sicurezza IT (prodotti – soluzioni) > Sistemi: contabile – informativo > Certificazioni: ISO 27001
G	Reati tributari	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	> Dichiarazioni fiscali	> Governance: AFC > Processi: calcolo imposte – modello ICTP > Sistemi: contabile – informativo > Certificazioni: contabile – finanziaria
													> Crediti d'imposta	> Governance: AFC – RS – LEG & IP > Processi: calcolo crediti patent box – sviluppo prodotti e soluzioni > Sistemi: contabile – informativo > Certificazioni: contabile – finanziaria

Aree aziendali a rischio reato:
AFC Amministrazione, finanza e controllo
LEG & IP Affari legali e proprietà intellettuali
IT Sistemi informativi
RU Risorse umane
SG Servizi generali
OP Acquisti, pianificazione, produzione, logistica, qualità, ingegneria (Operations)
COM Comunicazione
ST Strategy

Protocolli preventivi:
ORG Struttura organizzativa / Segregazione delle funzioni / Sistema di deleghe
PROC Procedure / Processi aziendali / Codici di condotta / Framework operativi / Sistema di Gestione ISO
SIS Sistemi informativi e Applicativi / Infrastruttura Informatica

I seguenti protocolli preventivi garantiscono la prevenzione dei Reati e/o Illeciti ed il controllo delle aree aziendali a rischio:

ORG: configurazione generale della struttura organizzativa aziendale e conseguente assegnazione di poteri e responsabilità; segregazione delle funzioni volta ad evitare sovrapposizioni o accentramento dei poteri dispositivi – approvativi;

PROC: esistenza di procedure e processi aziendali tali da garantire la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia delle operazioni aziendali, l'affidabilità dell'informativa contabile e finanziaria, il rispetto di leggi e regolamenti, nonché adozione di codici a disciplina delle regole comportamentali nell'esercizio delle attività aziendali;

SIS: presenza di un sistema informatico a garanzia del processo di formazione dell'informativa contabile e finanziaria, nonché a presidio dell'attendibilità – correttezza delle informazioni e attività, veicolate attraverso l'utilizzo di applicativi e, più in generale, dell'infrastruttura informatica aziendale.

A ciascuna delle Attività a Rischio è dedicata una specifica Parte Speciale, cui si rimanda.

Il rischio afferente agli altri *reati presupposto* previsti dal Decreto[8], risulta di fatto remoto e difficilmente ipotizzabile nell'interesse o a vantaggio di Datalogic.

4.3 (segue): principi di controllo e sistemi di controllo preventivo.

Il Modello è basato sul sistema di controllo interno di Datalogic, fondato sull'attribuzione di responsabilità, le linee di dipendenza gerarchica e la descrizione dei compiti, con specifica previsione di principi di controllo quali, ad esempio, la contrapposizione di funzioni.

In particolare, le procedure manuali ed informatiche implementate da Datalogic (il sistema gestionale informatico e, in generale, i processi gestiti dalla funzione Sistemi Informativi) sono tali da regolamentare lo svolgimento delle attività, prevedendo gli opportuni punti di controllo ed adeguati livelli di sicurezza.

Inoltre, nell'ingegnerizzazione dei processi, laddove possibile, è stata introdotta la separazione di compiti fra coloro che svolgono attività cruciali di un processo a rischio e sono stati considerati i principi di trasparenza e verificabilità (in particolare, si è agito affinché ogni operazione, transazione, azione risultasse verificabile, documentata, coerente e congrua).

Per quanto concerne la gestione finanziaria, dove il controllo procedurale si avvale di strumenti consolidati, sono stati adottati diversi protocolli preventivi, fra cui l'abbinamento firme (per importi eccedenti le strette necessità dell'operatività quotidiana), frequenti riconciliazioni, supervisione e snodi autorizzatori, separazione di compiti con la già citata contrapposizione di funzioni.

Il Modello prevede inoltre un sistema di controllo di gestione in grado di fornire tempestiva segnalazione, a seconda dei casi, dell'insorgere o dell'esistenza di situazioni anomale.

Nell'ambito del sistema organizzativo, specifica attenzione è stata poi prestata ai sistemi premianti dei Dipendenti, affinché gli stessi risultino stimolanti ma raggiungibili, evitando *target* palesemente immotivati ed inarrivabili, che potrebbero costituire incentivo al compimento di Reati e/o Illeciti.

Inoltre, con specifico riferimento ai poteri autorizzativi e di firma, questi sono stati assegnati in coerenza con le responsabilità organizzative e gestionali definite, prevedendo, quando richiesto, una puntuale indicazione delle soglie di approvazione delle spese.

I limiti dei poteri autorizzativi e di firma sono recepiti, quali protocolli di blocco, nel sistema gestionale informatico.

In ogni caso, in funzione dell'attuale Modello a nessuno sono attribuiti poteri illimitati e sono adottati idonei accorgimenti affinché i poteri e le responsabilità siano chiaramente

[8] Per la lista completa delle fattispecie di reato, si rimanda al testo integrale del Decreto 231/2001, e successive modifiche e integrazioni.

definiti e conosciuti all'interno dell'organizzazione.

In quest'ottica nessuno può gestire in autonomia un intero processo e per ogni operazione è richiesto un adeguato supporto documentale (o informatico per i processi gestiti tramite il sistema gestionale informatico) su cui si possa procedere in ogni momento all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa[9].

Il Modello, quindi, coinvolge ogni aspetto dell'attività di Datalogic, attraverso la netta distinzione dei compiti operativi da quelli di controllo, con l'obiettivo di gestire correttamente le Attività a Rischio e le possibili situazioni di conflitto di interesse.

In particolare, i controlli coinvolgono, con ruoli e a livelli diversi, il Consiglio di Amministrazione (in particolar modo il Comitato Controllo e Rischi costituito in seno allo stesso), il Collegio Sindacale, il soggetto preposto al controllo interno (*Internal Auditor*)[10], l'Organismo di Vigilanza e i Dipendenti.

Per quanto concerne gli aspetti di "controllo" il Modello, oltre a prevedere l'istituzione di un autonomo ed indipendente Organismo di Vigilanza, garantisce l'integrazione e il coordinamento delle attività di quest'ultimo con il già esistente sistema per il controllo interno, facendo patrimonio delle esperienze maturate.

Il Modello non modifica le funzioni, i compiti, e gli obiettivi preesistenti del sistema dei controlli, ma mira a fornire maggiori garanzie circa la conformità delle prassi e delle attività aziendali alle norme del Codice Etico e della normativa aziendale che ne declina i principi nella disciplina delle Attività a Rischio.

Infine, sempre in tema di controlli, il Modello prevede l'obbligo di documentare (eventualmente attraverso la redazione di verbali) l'effettuazione delle verifiche ispettive e dei controlli effettuati.

5. MODELLO E CODICE ETICO

Le regole di comportamento contenute nel presente Modello si integrano con quelle del Codice Etico, pur presentando il Modello, per le finalità che esso intende perseguire in attuazione delle disposizioni riportate nel Decreto, una portata diversa rispetto al Codice Etico.

[9] Il Modello mira quindi a garantire il principio di separazione delle funzioni, per cui l'autorizzazione all'effettuazione di un'operazione, deve essere sotto la responsabilità di persona diversa da chi contabilizza, esegue operativamente o controlla l'operazione.

[10] Si precisa che in data 26 giugno 2007 il Consiglio di Amministrazione di Datalogic ha deliberato l'approvazione del regolamento dell'*Audit Committee* al fine di disciplinare in modo uniforme e coordinato i compiti e le funzioni di controllo contabile del cosiddetto C*omitato Contabile Speciale*, denominato appunto "*Audit Committee"*. In particolar modo, l'*Audit Committee* assicura il monitoraggio e il controllo dell'organizzazione e l'efficienza delle procedure di controllo interno ed il processo di predisposizione del bilancio garantendo altresì l'incontro, il confronto ed il coordinamento delle attività espletate dagli organi di controllo già esistenti (quali il Comitato Controllo e Rischi, il Collegio Sindacale e la Società di Revisione). Attualmente l'*Audit Committee* risulta istituito nella società Datalogic S.r.l..

Infatti, mentre il Codice Etico rappresenta uno strumento adottato in via autonoma e suscettibile di applicazione sul piano generale da parte di Datalogic allo scopo di esprimere dei principi di "deontologia aziendale" che il Gruppo Datalogic riconosce come propri e sui quali richiama l'osservanza da parte di tutti i Dipendenti, il Modello risponde invece a specifiche prescrizioni contenute nel Decreto e nel TUF, finalizzate a prevenire la commissione dei Reati e degli Illeciti.

6. L'ORGANISMO DI VIGILANZA – *premessa.*

L'art. 6, lett. b) del Decreto richiede, quale condizione per ottenere l'esimente dalla responsabilità amministrativa, che il compito di vigilare sul funzionamento e l'osservanza delle indicazioni del Modello nonché di curarne l'aggiornamento, sia affidato ad un organismo interno alla società dotato di autonomi poteri di iniziativa e di controllo.

Il Consiglio di Amministrazione, considerate le dimensioni della Società, il suo assetto organizzativo e le caratteristiche del *business*, istituisce l'Organismo di Vigilanza nominando i suoi componenti, dopo averne determinato il numero, nel rispetto dei requisiti indicati nel presente paragrafo, ovvero attribuendo le relative funzioni al Collegio Sindacale nominato dall'Assemblea della Società.

L'Organismo di Vigilanza si caratterizza per i seguenti requisiti:

- Autonomia e indipendenza

I requisiti di autonomia e indipendenza sono fondamentali affinché l'Organismo di Vigilanza non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo. Tali requisiti sono garantiti dalla insindacabilità delle scelte dell'Organismo di Vigilanza da parte degli organi dell'ente e con la previsione di un'attività di reporting al Consiglio di Amministrazione.

- Professionalità

L'Organismo di Vigilanza possiede al suo interno competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere; tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio.

- Continuità di azione

L' Organismo di Vigilanza (i) lavora costantemente sulla vigilanza del Modello con i necessari poteri di indagine; (ii) si configura come una struttura interna, in modo da garantire la continuità dell'attività di vigilanza; (iii) cura l'attuazione del Modello assicurarne il costante aggiornamento; (iv) non svolge mansioni operative che possano condizionare la visione d'insieme delle attività aziendali che ad esso si richiede.

I compiti assegnati all' Organismo di Vigilanza richiedono, pertanto, che lo stesso, nello svolgimento delle proprie funzioni (i) sia dotato di autonomi poteri di iniziativa e di controllo; (ii) sia posto all'*esterno* dei processi produttivi, come unità di staff a diretto ed

esclusivo "riporto" del Consiglio di Amministrazione e, dunque, svincolato da ogni rapporto gerarchico con i singoli responsabili delle strutture operative aziendali.

Nello svolgimento dei compiti di vigilanza e controllo, l'Organismo di Vigilanza di Datalogic (i) è supportato da tutte le funzioni aziendali e si può avvalere di altre professionalità esterne che, di volta in volta, si rendessero a tal fine necessarie; (ii) è autorizzato al libero accesso presso tutte le funzioni della Società – senza necessità di alcun consenso preventivo – onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D.Lgs. 231/2001.

Si precisa che per quanto concerne la salute e la sicurezza, l'Organismo di Vigilanza può avvalersi di tutte le risorse attivate per la gestione dei relativi aspetti, tra i quali il Responsabile del Servizio di Prevenzione e Protezione (RSPP), gli Addetti al Servizio di Prevenzione e Protezione (ASPP), il Rappresentante dei Lavoratori per la Sicurezza (RLS), il Medico Competente (MC) e gli addetti primo soccorso nonché alle emergenze in caso d'incendio.

6.1 (segue): la composizione dell'Organismo di Vigilanza di Datalogic.

Il Consiglio di Amministrazione, ove le funzioni dell'Organismo di Vigilanza non siano attribuite al Collegio Sindacale, ha facoltà di scegliere liberamente i componenti dell'Organismo stesso tra i soggetti che abbiano i seguenti requisiti:

- Requisiti professionali

  I componenti dell'Organismo di Vigilanza devono essere scelti tra soggetti particolarmente qualificati e con esperienza nell'esercizio di attività di amministrazione o di controllo ovvero fra soggetti che abbiano ricoperto ruoli direttivi presso imprese, enti pubblici, pubbliche amministrazioni, o abbiano svolto o svolgano attività professionali o di insegnamento universitario in materie giuridiche, economiche e finanziarie.

  In considerazione delle caratteristiche dimensionali e delle relative regole di *corporate governance*, è auspicata la presenza nell'Organismo di Vigilanza:

  a. del responsabile della funzione di *Internal Auditing* di Datalogic le cui conoscenze della struttura organizzativa e societaria possono facilitare la reale e concreta attività dell'Organismo di Vigilanza così come previsto dal Decreto;

  b. di due professionisti, giuristi o economisti, che abbiano maturato specifiche competenze nel settore del diritto penale dell'economia, così come in materia finanziaria – societaria, in modo tale da supportare costantemente l'operato dell'Organismo di Vigilanza con una *"sensibilità giuridica"* di tipo marcatamente *"specialistico"*[11].

- Requisiti personali e di onorabilità

[11] Per conoscere i riferimenti anagrafici dei membri dell'Organismo di Vigilanza in carica, si rimanda al contenuto della relazione sul governo societario e sugli assetti proprietari redatta ai sensi dell'art. 123-bis del TUF, consultabile sul sito web www.datalogic.com - sezione *Governance*.

È altresì necessario garantire che i componenti dell'Organismo di Vigilanza abbiano, oltre che qualità professionali, anche qualità personali tali da renderli idonei a svolgere il compito a loro affidato, dichiarandolo all'atto di accettazione della nomina. I componenti dell'Organismo di Vigilanza, pertanto, dovranno essere esenti da cause di incompatibilità e conflitti di interessi tali che possano minarne l'indipendenza e la libertà d'azione e di giudizio.

Non posso essere eletti componenti dell'Organismo di vigilanza coloro i quali non siano in possesso dei requisiti di onorabilità previsti per i membri del Consiglio di Amministrazione ai sensi dell'art. 147-*quinquies* del TUF, nonché gli interdetti, gli inabilitati e i falliti.

All'atto della nomina i componenti dell'Organismo di Vigilanza devono rilasciare apposita dichiarazione attestante la sussistenza dei requisiti richiesti, impegnandosi a comunicare alla Società il venire meno degli stessi nel corso del mandato. I membri dell'Organismo di Vigilanza vengono nominati dal Consiglio di Amministrazione e rimangono in carica, di regola, fino alla scadenza del mandato conferito allo stesso Consiglio di Amministrazione da parte dell'Assemblea degli Azionisti, ovvero il periodo stabilito dal Consiglio all'atto della nomina.

Il Consiglio di Amministrazione conferisce all'Organismo di Vigilanza la dotazione finanziaria necessaria ad espletare al meglio la propria funzione.

Le funzioni e i poteri dell'Organismo di Vigilanza (identici per tutte le Parti Speciali), nonché le modalità di gestione dei necessari flussi informativi sono sinteticamente indicati nei paragrafi.

6.2 (segue): funzioni e poteri dell'Organismo di Vigilanza di Datalogic.

L' Organismo di Vigilanza ha il compito di vigilare:

a) sull'osservanza del Modello da parte dei Destinatari;

b) sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione di Reati e/o Illeciti;

c) sull'opportunità di aggiornamento del Modello, qualora se ne verifichino i presupposti, formulando proposte al Consiglio di Amministrazione in conseguenza di (i) significative violazioni delle prescrizioni del Modello, (ii) significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa, (iii) modifiche legislative al decreto legislativo 231/2001 o che comunque prevedano nuove ipotesi di responsabilità diretta dell'ente;

Inoltre, l'Organismo di Vigilanza, a seguito dell'accertamento di violazioni del Modello Organizzativo, è chiamato a segnalare tempestivamente le stesse alla funzione risorse umane e, nel caso di gravità oggettiva del fatto costituente infrazione disciplinare (anche in considerazione del ruolo ricoperto dal soggetto che effettuato l'infrazione), al Consiglio di Amministrazione e al Collegio Sindacale per gli opportuni provvedimenti disciplinari che dovranno essere irrogati.

L'adempimento dei predetti compiti è garantito dallo svolgimento delle seguenti attività:

(i) verifiche e controlli preventivi sulle principali Attività a Rischio, utilizzando specifiche *check list*, ovvero sull'effettività dei processi aziendali e l'archiviazione della relativa documentazione;

(ii) interviste al personale apicale di Datalogic, titolare delle principali funzioni ed Attività a Rischio;

(iii) formazione dei Dipendenti ed informazione dei Destinatari;

(iv) aggiornamento e manutenzione del Modello, in relazione al mutare delle condizioni aziendali e/o normative;

(v) analisi delle segnalazioni ricevute a fronte di ogni violazione o sospetto di violazione del Codice Etico e/o di ogni altro protocollo preventivo previsto dal Modello.

L'Organismo di Vigilanza si avvale dei flussi informativi garantiti dai responsabili delle singole aree aziendali, nonché della funzione di *Internal Auditing*, quale preposto al controllo interno di Datalogic. Le attività svolte e gli strumenti utilizzati consentono di rilevare eventuali eccezioni ed anomalie, nonché di porre in essere le necessarie azioni correttive.

L'Organismo di Vigilanza si riunisce formalmente almeno una volta ogni trimestre, fatte salve situazioni di emergenza. Di ogni riunione deve essere redatto un verbale sul libro delle riunioni dell'Organismo di Vigilanza precedentemente vidimato. Il verbale di ogni riunione è sottoscritto da tutti i membri dell'Organismo di Vigilanza partecipanti alla riunione stessa.

6.3 (segue): rendicontazione dell'Organismo di Vigilanza di Datalogic.

La rendicontazione dell'attività svolta dall'Organismo di Vigilanza viene effettuata con le seguenti modalità:

a) su base semestrale, al Comitato Controllo e Rischi di Datalogic ed al Collegio Sindacale;

b) su base annua, nei confronti del Consiglio di Amministrazione, attraverso una relazione contenente i risultati conseguiti nell'anno, ed il piano di attività per quello successivo.

Il Consiglio di Amministrazione ed il Collegio Sindacale hanno la facoltà di convocare in qualsiasi momento l'Organismo di Vigilanza, il quale, a sua volta, ha facoltà di richiedere, attraverso le funzioni ed i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

7. FLUSSI INFORMATIVI NEI CONFRONTI DEI DIPENDENTI

Datalogic, consapevole dell'importanza degli aspetti formativi ed informativi quale protocollo preventivo di primario rilievo, opera al fine di garantire la conoscenza da

parte dei Dipendenti sia del contenuto del Decreto e degli obblighi derivanti dal medesimo, sia del Modello.

Le attività di formazione, sensibilizzazione ed informazione nei confronti dei Dipendenti, nonché degli Organi Sociali, sono gestite dai responsabili delle funzioni aziendali coinvolte nell'applicazione del Modello in collaborazione con l'Organismo di Vigilanza, a partire dall'assunzione o dell'inizio del rapporto di lavoro.

Tra le stesse si segnalano in particolare:

a) la consegna, ai nuovi assunti, di un set informativo contenente (oltre al materiale indicato da ulteriori policy o procedure aziendali, quali privacy e sicurezza delle informazioni, igiene e sicurezza sul lavoro) il CCNL, un riassunto del contenuto del Decreto e del Modello, con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza;

b) la sottoscrizione da parte dei Dipendenti di un apposito modulo per presa conoscenza ed accettazione;

c) una specifica attività di formazione attraverso corsi d'aula o utilizzando strumenti e servizi di e – learning (in tal caso con soluzioni che garantiscano il riscontro dell'avvenuta formazione).

A garanzia della formazione ed informazione dei Dipendenti, è, tra le altre attività, predisposta una specifica area della rete informatica aziendale dedicata al Decreto.

8. FLUSSI INFORMATIVI NEI CONFRONTI DI SOGGETTI TERZI

Agli ulteriori Destinatari, in particolare Partner, Fornitori e Consulenti, sono fornite da parte delle funzioni aziendali aventi contatti istituzionali con gli stessi, in coordinamento con l'Organismo di Vigilanza, apposite informative sulle politiche e le procedure adottate da Datalogic sulla base del Modello, sul Codice Etico, nonché sulle conseguenze che comportamenti contrari alle previsioni del Modello o comunque contrari al Codice Etico o alla normativa vigente possono avere con riguardo ai rapporti contrattuali.

Laddove possibile sono inserite nei testi contrattuali specifiche clausole dirette a disciplinare tali conseguenze, quali clausole risolutive o diritti di recesso in caso di comportamenti contrari alle norme del Codice Etico e/o a Protocolli del Modello.

9. SISTEMA DISCIPLINARE – *premessa*.

Condizioni necessarie per garantire l'effettività del Modello e un'azione efficiente dell'Organismo di Vigilanza è la definizione di un sistema di sanzioni commisurate alla violazione dei protocolli preventivi e/o di ulteriori regole del Modello o del Codice Etico. Tale sistema disciplinare costituisce, infatti, ai sensi dell'art. 6, comma 1, lettera e) del Decreto, un requisito essenziale ai fini dell'esimente rispetto alla responsabilità di Datalogic.

Il sistema disciplinare Datalogic prevede sanzioni per ogni Destinatario, in considerazione della diversa tipologia di rapporti, e si conforma ai principi di proporzione e contradditorio, per effetto dei quali la sanzione irrogata viene sempre

commisurata all'entità dell'atto contestato, garantendo al soggetto coinvolto la possibilità di addurre giustificazioni a difesa del proprio comportamento.

L'applicazione del sistema disciplinare e delle relative sanzioni prescinde dall'eventuale instaurazione di un procedimento penale e dall'esito del conseguente giudizio per la commissione di una delle condotte illecite previste dal decreto legislativo 231/2001. Il sistema disciplinare Datalogic, infatti, completando e rendendo effettivo il Modello, ha come obiettivo principale non tanto la repressione dei reati una volta che gli stessi siano stati commessi, ma, piuttosto, quello di contrastare comportamenti prodromici ai reati medesimi e, conseguentemente, di evitare che i reati cd. presupposto possano essere realizzati, se non eludendo fraudolentemente il Modello medesimo.

Il sistema disciplinare Datalogic, pertanto, ha una funzione essenzialmente preventiva, operando, per l'appunto, come un presidio interno all'impresa che si aggiunge e previene l'applicazione di sanzioni "esterne" da parte dello Stato.

Il sistema disciplinare Datalogic viene costantemente monitorato dall'Organismo di Vigilanza e dalle Risorse Umane.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni restano di competenza delle Risorse Umane, fermo restando il necessario coinvolgimento dell'Organismo di Vigilanza nella procedura di accertamento delle violazioni e di irrogazione delle sanzioni per violazioni del Modello. Pertanto, l'archiviazione di un provvedimento disciplinare ovvero l'irrogazione di una sanzione disciplinare per violazione del Modello necessita della preventiva informazione e del preventivo parere dell'Organismo di Vigilanza.

È fatta salva la facoltà per la Società di rivalersi per ogni danno e/o responsabilità che alla stessa possano derivare da comportamenti di dipendenti in violazione del Modello.

Al fine di esplicitare preventivamente i criteri di correlazione tra le mancanze dei lavoratori ed i provvedimenti disciplinari adottati, il Consiglio di Amministrazione classifica le azioni degli Amministratori, Sindaci, Dipendenti e altri soggetti terzi in:

1. comportamenti tali da ravvisare una mancata esecuzione degli ordini impartiti da Datalogic sia in forma scritta che verbale nell'esecuzione di Attività a Rischio, quali a titolo di esempio:

   - violazione delle procedure, regolamenti, istruzioni interne scritte o verbali;

   - violazione, aggiramento o disattivazione colposa di uno o più protocolli preventivi;

2. comportamenti tali da ravvisare una grave infrazione alla disciplina e/o alla diligenza nel lavoro tali da far venire meno radicalmente la fiducia della Società nei confronti dell'Amministratore e/o Dipendente quali:

   - adozione, nell'espletamento delle Attività a Rischio, di comportamenti di cui al precedente punto 1. diretti in modo non equivoco al compimento di Reati o a rappresentarne l'apparenza a danno di Datalogic s.p.a.;

3. adozione, nell'espletamento delle Attività a Rischio, di comportamenti di cui al precedente punto 1. diretti in modo non equivoco al compimento di Reati e/o Illeciti o a rappresentarne l'apparenza a danno di Datalogic; comportamenti tali da provocare grave nocumento morale o materiale a Datalogic tali da non consentire la prosecuzione del rapporto neppure in via temporanea, quale l'adozione di comportamenti che integrino uno o più Reati e/o Illeciti, ovvero comportamenti di cui al precedente punto 1. commessi con dolo.

4. comportamenti tali da impedire o inficiare l'utilizzo dei canali di comunicazione dedicati alla segnalazione di eventuali violazioni del Modello (c.d. Whistleblowing), quali:

   - mancata istituzione dei canali di segnalazione;
   - mancata istituzione di procedure per l'effettuazione e per la gestione delle segnalazioni;
   - adozione di procedure per l'effettuazione e per la gestione delle segnalazioni non conformi alle prescrizioni di legge;
   - attuazione di atti, ovvero comportamenti, ritorsivi, ovvero ostativi, al rilascio della segnalazione.

L'adeguatezza del sistema disciplinare alle prescrizioni del Decreto viene costantemente monitorata dall'Organismo di Vigilanza.

9.1 (segue): sanzioni per i Dipendenti.

Le violazioni del Modello compiute dai Dipendenti costituiscono illecito disciplinare e sono sanzionate nel pieno rispetto dell'articolo 7 della legge n. 300/1970 (c.d. "Statuto dei lavoratori") e dal CCNL di riferimento, sia per quanto riguarda le sanzioni applicabili (che in linea di principio risultano "tipizzate" in relazione al collegamento con specificati indebiti disciplinari) sia per quanto riguarda la forma di esercizio di tale potere.

Il sistema disciplinare correntemente applicato in Datalogic è in linea con le disposizioni di cui ai CCNL, e rispetta i prescritti requisiti di efficacia e deterrenza.

Il mancato rispetto e/o la violazione dei principi generali del Modello, delle regole di comportamento imposte dal Codice Etico e delle procedure, regolamenti o istruzioni aziendali, ad opera di Dipendenti, costituiscono quindi inadempimento alle obbligazioni derivanti dal rapporto di lavoro e illecito disciplinare (quali insubordinazione, esecuzione negligente delle prestazioni, pregiudizio alla disciplina o morale aziendale, ai sensi dell'articolo 24 del CCNL, lettere *c)*, *d)* ed *l)*; infrazioni alla disciplina e/o alla diligenza del rapporto di lavoro più gravi di quelle di cui all'articolo 24, ai sensi dell'articolo 25, lettere A) e B)).

Con riferimento alle sanzioni applicabili, si precisa che esse saranno adottate ed applicate nel pieno rispetto delle procedure previste dalle normative collettive nazionali applicabili al rapporto di lavoro.

Fermo restando il principio di collegamento tra i provvedimenti disciplinari applicabili e

le fattispecie in relazioni alle quali le stesse possono essere assunti, nell'applicazione della sanzione disciplinare deve necessariamente essere rispettato il principio della proporzionalità tra infrazione e sanzione. Restano ferme e si intendono qui richiamate tutte le disposizioni di cui al predetto art. 7 della legge 300/1970 in relazione sia all'esposizione dei codici disciplinari "mediante affissione in luogo accessibile a tutti", che all'obbligo di preventiva contestazione dell'addebito al dipendente, anche al fine di consentire allo stesso di approntare una idonea difesa e di fornire eventuali giustificazioni.

9.2 (segue): sanzioni per i dirigenti.

In caso di violazione, da parte dei dirigenti, dei principi generali del Modello, delle regole di comportamento imposte dal Codice Etico e degli altri protocolli preventivi, Datalogic provvederà ad assumere nei confronti dei responsabili i provvedimenti ritenuti idonei in funzione del rilievo e della gravità delle violazioni commesse, anche in considerazione del particolare vincolo fiduciario sottostante al rapporto di lavoro tra Datalogic e il lavoratore con qualifica di dirigente.

Nei casi di cui al punto 2. di cui alla premessa, Datalogic potrà procedere alla risoluzione anticipata del contratto di lavoro ovvero all'applicazione di altra sanzione ritenuta idonea in relazione alla gravità del fatto. Nel caso in cui il comportamento del dirigente rientri nei casi previsti dal punto 3. di cui alla premessa, Datalogic procederà alla risoluzione anticipata del contratto di lavoro senza preavviso ai sensi dell'articolo 2119 del codice civile e articolo 23, comma 1, punto 1. del CCNL. Ciò in quanto il fatto stesso deve considerarsi essere stato posto in essere contro la volontà di Datalogic nell'interesse o a vantaggio del dirigente e/o di terzi.

9.3 (segue): sanzioni per gli amministratori e per i sindaci.

In caso di realizzazione di Reati e/o Illeciti o di violazione del Codice Etico, del Modello e/o relativi protocolli preventivi da parte degli amministratori o dei sindaci di Datalogic, l'Organismo di Vigilanza informerà l'intero Consiglio d'Amministrazione ed il Collegio Sindacale, i quali provvederanno ad assumere le opportune iniziative.

In casi di gravi violazioni da parte degli amministratori non giustificate e/o non ratificate dal Consiglio di Amministrazione, il fatto potrà considerarsi giusta causa per la revoca dalla carica. Si considera grave violazione non giustificata la realizzazione di condotte di cui ai Reati e/o Illeciti.

9.4 (segue): misure nei confronti di soggetti terzi.

Salvo situazioni eccezionali da portare all'attenzione dell'Organismo di Vigilanza, condizione necessaria per concludere validamente contratti di ogni tipologia con Datalogic, e in particolare contratti di fornitura, outsourcing, mandato, agenzia, procacciamento di affari, associazione in partecipazione e consulenza, è l'assunzione dell'obbligo da parte del contraente di rispettare il Codice Etico e/o i protocolli preventivi applicabili.

Tali contratti dovranno prevedere clausole risolutive, o diritti di recesso in favore di Datalogic senza alcuna penale in capo a quest'ultima, in caso di realizzazione di Reati e/o

Illeciti, ovvero in caso di violazione di regole del Codice Etico, del Modello e/o dei relativi protocolli preventivi.

Datalogic si riserva comunque l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni a Datalogic, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal Decreto.

10. SEGNALAZIONI

Ciascun destinatario del Modello ha facoltà di segnalarne eventuali violazioni alla Società, anche in forma anonima, tramite i canali di comunicazione di seguito riepilogati:

- Piattaforma segnalazioni disponibile sul sito della Società (https://datalogic.integrity.complylog.com/) che garantisce la possibilità di rilasciare segnalazioni scritte ovvero tramite registrazione di messaggi vocali.

Ovvero tramite un incontro in presenza con l'Organismo di Vigilanza della Società. Ogni segnalazione è presa in carico e valutata dalla Società secondo le corrispondenti previsioni di legge[12], nei relativi modi e tempi, prevedendo:

- avviso di ricevimento della segnalazione, entro 7 giorni dalla stessa;
- formale riscontro, entro 3 mesi dall'avviso di ricevimento;
- conseguente archiviazione documentale.

I contenuti delle segnalazioni, al fine di garantirne un'adeguata valutazione, si caratterizzano come:

- fattuali, circostanziati e fondati su elementi di fatto precisi e concordanti, nonché privi di alcuna opinione di carattere personale;
- privi di uno scopo opportunistico, denigratorio, improprio o strumentale;
- finalizzati a tutelare l'integrità della Società.

Si rammenta infine che la Società garantisce adeguata tutela al segnalante da eventuali ritorsioni e conseguenze pregiudizievoli, non rivelandone l'identità, fatti salvi gli obblighi di legge.

***** OMISSIS *****

[12] D. Lgs. 231/2001 ss.mm.ii., Regolamento UE 2016/679 in materia di Privacy e D. Lgs. 24/2023 a recepimento Direttiva (UE) 2019/1937 in materia di segnalazioni.