Trusted Global Innovator

Information Type:	--- (Open Distribution/Public Document)
Company Name:	NTT DATA Italia
Information Owner:	Legal & Compliance

MODELLO ORGANIZZATIVO, DI GESTIONE E CONTROLLO DI NTT DATA ITALIA SPA

Ai sensi del D.Lgs. 231/2001

Parte Generale

Approvato dal Consiglio di Amministrazione del 29 giugno 2023

Le informazioni contenute in questo documento sono di proprietà NTT DATA Italia S.p.A., è vietata la riproduzione

MODELLO ORGANIZZATIVO, DI GESTIONE E CONTROLLO DI NTT DATA ITALIA SPA AI SENSI DEL D.LGS. 231/2001

Parte Generale

SOMMARIO

DEFINIZIONI 5
1 INTRODUZIONE 7
1.1 Adozione del modello ex D.Lgs. n. 231/2001 da parte di NTT DATA Italia S.p.A. 7
1.2 NTT DATA Italia S.p.A. 7
1.3 Il Modello di NTT DATA Italia 7
1.4 Principi generali del Modello 8
2 MAPPATURA DEI RISCHI 10
2.1 Premessa 10
2.2 Individuazione dei rischi e protocolli 10
2.2.1 La definizione di "*rischio accettabile*" 12
2.2.2 Analisi dei rischi potenziali 12
2.2.3 Valutazione/costruzione/adeguamento del sistema di controlli preventivi 13
2.3 Rilevazione e mappatura dei rischi 13
2.3.1 Reati contro la Pubblica Amministrazione (artt. 24 e 25, D.Lgs. 231/2001) 13
2.3.2 Reati Societari (art. 25-*ter*, D.Lgs. 231/2001) 14
2.3.3 Reati contro la salute e sicurezza sul lavoro (art. 25-*septies*, D.Lgs. 231/2001) 14
2.3.4 Reati Informatici (art. 24-*bis*, D.Lgs. 231/2001) 14
2.3.5 Delitti in materia di violazione del diritto d'autore (art. 25-*novies*, D.Lgs. 231/2001) 14
2.3.6 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies*, D.Lgs. 231/2001) 14
2.3.7 Impiego di cittadini terzi il cui soggiorno è irregolare (art. 25-*duodecies*, D.Lgs. 231/2001) 15
2.3.8 Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-*octies*, D.Lgs. 231/2001) 15
2.3.9 Autoriciclaggio (art. 25-*octies*, D.Lgs. 231/2001) 15
2.3.10 Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-*octies.1*, D.Lgs. 231/2001) 15
2.3.11 Delitti contro la personalità individuale (art. 25-*quinquies*, D.Lgs. 231/2001) 15
2.3.12 Reati tributari (art. 25-*quinquiesdecies*, D.Lgs. 231/2001) 16
2.3.13 Delitti in materia di contrabbando (art. 25-*sexiesdecies*, D.Lgs. 231/2001) 16
2.3.14 Ulteriori attività oggetto di controllo 16
3 VALORI E REGOLE DI COMPORTAMENTO 17
3.1 Codice di Condotta Commerciale Globale 17
3.2 Policy, procedure e istruzioni 17
3.3 Procedure sulla gestione delle risorse finanziarie 17
4 SISTEMA ORGANIZZATIVO, RUOLI E POTERI 17
4.1 Caratteristiche della Struttura Organizzativa 17
4.2 Definizione dei ruoli 18
4.3 Sistema delle deleghe e delle procure 18
5 CORPORATE GOVERNANCE E DIREZIONE D'IMPRESA 19
5.1 Modello di *Corporate Governance* 19
5.2 Comitati Aziendali 19
6 SISTEMA DI CONTROLLO INTERNO 19
6.1 Funzione Amministrazione, Finanza e Controllo 19
6.2 I processi e gli strumenti 20
7 ORGANISMO DI VIGILANZA 20

7.1 Nomina e composizione dell'Organismo 20
7.2 Competenze e Cause di (in)eleggibilità, decadenza e sospensione 21
7.3 Funzioni e poteri 22
7.4 Obblighi di informazione dell'Organismo di Vigilanza 24
7.5 Segnalazioni all'OdV da parte di dipendenti o esponenti aziendali o da parte di terzi 25
7.6 Verifiche periodiche e report dell'OdV 27
7.7 Sistema delle deleghe 27
7.8 Conservazione delle informazioni 28
8 DIFFUSIONE ED ATTUAZIONE DEL MODELLO 28
8.1 Piano di comunicazione 28
8.1.1 Comunicazione ai componenti degli organi sociali 28
8.1.2 Comunicazione ai Dirigenti e ai Responsabili di Funzione 28
8.1.3 Comunicazione a tutti gli altri dipendenti 28
8.1.4 Formazione del personale 28
8.2 Comunicazione a terzi 29
8.2.1 Formazione dei collaboratori esterni 29
9 SISTEMA DISCIPLINARE 29
9.1 Principi generali e criteri di irrogazione delle sanzioni 29
9.2 Sanzioni 30
9.2.1 Sanzioni verso lavoratori dipendenti (Quadri – Impiegati) 30
9.2.2 Misure verso i Dirigenti 32
9.2.3 Misure nei confronti dei "Soggetti apicali" e dei Sindaci 33
9.2.4 Collaboratori esterni 35
9.2.5 Misure a tutela delle segnalazioni (*Whistleblowing*) 36

DEFINIZIONI

Aree a rischio	Le aree di attività aziendale nel cui ambito risulta profilarsi, in termini più concreti, il rischio di commissione dei Reati contemplati dal D.Lgs. n. 231/2001
CCNL	Contratto collettivo nazionale di lavoro applicabile ai dipendenti di NTT Data Italia S.p.A.
CCNL Dirigenti	Contratto collettivo nazionale di lavoro per i dirigenti di aziende produttrici di beni e servizi, attualmente in vigore e applicato da NTT Data Italia S.p.A.
Codice di Condotta Commerciale Globale o Codice Etico o Codice di Condotta	Codice approvato da NTT DATA EMEA, integrato e adottato dal Consiglio di Amministrazione di NTT DATA Italia comprendente il complesso di diritti, doveri e responsabilità che NTT DATA Italia S.p.A. assume espressamente nei confronti dei propri interlocutori nello svolgimento della propria attività e disponibile sul sito internet e sul portale intranet della Società
Collaboratori	Coloro che agiscono in nome e/o per conto di NTT DATA Italia S.p.A. sulla base di apposito mandato o di altro vincolo contrattuale
Decreto	Il Decreto legislativo 8 giugno 2001 n. 231 e successive modifiche e integrazioni
Destinatari	Componenti degli organi sociali e degli organismi interni di *governance* aziendali, dipendenti, collaboratori a qualsiasi titolo, anche occasionali e tutti coloro che intrattengono rapporti commerciali e/o finanziari di qualsiasi natura con NTT Data Italia S.p.A., ovvero agiscono per conto della stessa sulla base di specifici mandati (ad esempio: consulenti, fornitori, partners)
Dipendenti	Tutti i lavoratori subordinati di NTT DATA Italia S.p.A. (compresi i dirigenti)
Familiari	Parenti e affini in linea retta entro il secondo grado (figli, genitori, nipoti – quali figli dei figli – e nonni, suoceri e genero, nuora, fratelli o sorelle del coniuge), parenti e affini in linea collaterale entro il terzo grado e inoltre i cugini (fratelli e sorelle, nipote e zio, oltre che cugini); coniuge e/o convivente
Funzioni o Funzione	Strutture organizzative di primo livello di NTT DATA Italia S.p.A.
Interlocutori	Ad esclusione dei collaboratori, tutte le controparti contrattuali di NTT DATA Italia S.p.A., persone fisiche o giuridiche, quali fornitori, clienti e, in generale, tutti i soggetti verso o da parte dei quali NTT DATA Italia S.p.A. eroghi o riceva una qualunque prestazione contrattuale
Linee Guida	Le Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo secondo il D.Lgs. 231/2001, approvate da Confindustria e s.m.i.
Modello 231	Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001
Modello o Modello organizzativo o MOG	Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001 adottato da NTT DATA Italia S.p.A.
NTT DATA Corp.	NTT DATA Corporation

NTT DATA EMEA	NTT DATA EMEA Ltd.
NTT DATA Group o Gruppo NTT DATA	NTT DATA Corp. e le sue società controllate
NTT DATA Italia o **Società**	NTT DATA Italia S.p.A.
Organi Sociali	Il Consiglio di Amministrazione e il Collegio Sindacale di NTT DATA Italia S.p.A.
OdV o Organismo	Organismo di Vigilanza ai sensi dell'art. 6, comma 1, lett. b) del D.Lgs. 231/2001
P.A.	Qualsiasi Pubblica Amministrazione, inclusi i relativi esponenti nella loro veste di pubblici ufficiali o incaricati di pubblico servizio anche di fatto
Reati o Reato o Reati 231	I reati rilevanti a norma del D.Lgs. 231/2001
Vertice aziendale	Il Presidente e l'Amministratore Delegato di NTT DATA Italia S.p.A.

1 INTRODUZIONE

1.1 Adozione del modello ex D.Lgs. n. 231/2001 da parte di NTT DATA Italia S.p.A.

Il Decreto legislativo 8 giugno 2001 n. 231 (*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29/09/2000, n. 300"*) ha introdotto nell'ordinamento giuridico italiano - come ormai noto - un particolare regime di responsabilità amministrativa a carico degli enti, che si configura qualora vengano commessi i reati elencati nel Decreto, nell'ambito delle attività svolte dagli enti.

Il Consiglio di Amministrazione di NTT DATA Italia S.p.A. ha approvato in data 28 gennaio 2006 la prima versione del Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001 nella consapevolezza che l'implementazione del Modello, pur costituendo una facoltà e non un obbligo, permette alla Società di disporre di un complesso di regole, strumenti e attività idonei a prevenire la commissione dei reati di cui al Decreto, a tenere indenne la Società dalla responsabilità ivi prevista in caso fosse comunque commesso uno dei suddetti reati, nonché a rafforzare la propria cultura di *governance* e sensibilizzare le risorse impiegate sui temi del controllo dei processi aziendali, per stimolare una prevenzione "attiva" dei Reati e - più in generale - di qualsiasi comportamento illecito all'interno della Società. A seguito delle integrazioni normative che - a partire dalla suddetta data - hanno interessato il Decreto, nonché dell'evoluzione giurisprudenziale riguardante il tema della responsabilità amministrativa degli enti, il Consiglio di Amministrazione di NTT DATA Italia ha - nel tempo - approvato numerosi aggiornamenti e modifiche al Modello, provvedendo altresì ad armonizzare e aggiornare il Codice Etico approvato da NTT DATA EMEA e adottato dalla Società.

Il presente documento riflette pertanto il Modello nella versione da ultimo approvata dal Consiglio di Amministrazione della Società il 29 giugno 2023, che segue quelle approvate alle date del 20 settembre 2011, del 29 luglio 2014, del 30 novembre 2016, del 10 dicembre 2018 e del 29 giugno 2020.

1.2 NTT DATA Italia S.p.A.

NTT DATA Italia fa parte - dal 2011 - del Gruppo NTT DATA Corp., con sede a Tokyo, player internazionale che fornisce servizi, prodotti e soluzioni IT innovativi e di qualità per Clienti di tutto il mondo, operanti in vari e diversi settori di attività (telecomunicazioni, servizi bancari e finanziari, assicurazioni, P.A., industria e distribuzione, utilities, editoria e media).

NTT DATA Italia è soggetta a Direzione e Coordinamento di NTT DATA EMEA Ltd. con sede a Londra.

1.3 Il Modello di NTT DATA Italia

Il Modello adottato dalla Società costituisce atto di emanazione *"dell'organo dirigente"* ai sensi dell'art. 6 co. 1, lett. a) del D.Lgs. 231/2001, organo che in NTT DATA Italia è identificabile con il Consiglio di Amministrazione, cui spetta pertanto la competenza in merito ad eventuali successive modifiche e integrazioni del MOG. L'Amministratore Delegato della Società ha la facoltà di apportare al testo del Modello modifiche e integrazioni di carattere solo formale.

I principi base descritti nella Parte Generale del Modello si applicano a NTT DATA Italia e sono condivisi dalle

Società controllate; essi devono essere rispettati in tutte le attività aziendali svolte sia in Italia sia all'estero. I Modelli di organizzazione, gestione e controllo delle Società controllate si ispirano infatti agli stessi valori e agli stessi principi generali di seguito descritti.

L'adozione del Modello non solo è necessaria per rendere la Società pienamente conforme al Decreto 231/2001, ma risulta fondamentale anche per sensibilizzare tutti coloro che lavorano per la Società a un comportamento trasparente, dettato dalla piena aderenza alla legge, come già evidenziato nella introduzione che precede. Lo scopo è quello di costruire e mantenere attivo un sistema strutturato e organico di procedure e di attività di controllo, volto alla prevenzione della commissione delle diverse tipologie di reati contemplate dal Decreto 231/2001.

Sono destinatari del presente documento tutti coloro che operano per il conseguimento dello scopo e degli obiettivi di NTT DATA Italia, in particolare, come specificato nelle "Definizioni" che precedono: i componenti degli organi sociali e degli organismi di governance della Società, i dipendenti, i consulenti esterni, i fornitori, i clienti e in generale tutti i terzi con cui NTT DATA Italia intrattiene rapporti inerenti le proprie attività sociali. Il Modello in tale ottica è stato elaborato in aderenza non solo ai dettami del Decreto, ma anche alle linee guida elaborate dalle associazioni di categoria, in particolare alle indicazioni di Confindustria con il documento "*Linee guida per la costituzione dei modelli di organizzazione, gestione e controllo*" emanato in data 7 marzo 2002 e da ultimo aggiornato nel 2021.

Questo documento è stato redatto con l'intento di supportare la comprensione del sistema organizzativo, di gestione e controllo della Società attraverso un framework di riferimento che evidenzi anche dove siano reperibili le informazioni più aggiornate sulle scelte e sugli strumenti in essere. Per questo motivo, spesso, contiene rinvii ad altri documenti aziendali.

NTT DATA Italia, in quanto controllata dalla società capogruppo NTT DATA Corp., è tenuta a recepire la normativa J-SOX (*Japan's Financial Instruments and Exchange Law*), che richiede a tutte le società quotate in borsa in Giappone e alle relative controllate di rafforzare la propria *governance* interna al fine di garantire una divulgazione delle informazioni finanziarie precisa e completa. Nell'ambito del Gruppo NTT DATA sono quindi svolte specifiche attività di *auditing* interno in coerenza con la suddetta normativa.

1.4 Principi generali del Modello

Il Modello adottato da NTT DATA Italia si fonda sui seguenti principi generali:

a) **Conoscenza dei rischi** attraverso la mappatura dei «processi sensibili» della Società e la valutazione del livello di rischio, anche alla luce delle considerazioni esposte nel Position Paper emesso dall'Associazione Italiana Internal Auditor;

b) **Definizione di valori e regole di comportamento**, raccolti nel Codice di Condotta e nelle procedure aziendali, manuali ed informatiche, con particolare attenzione a quelle relative alla gestione finanziaria;

c) **Chiara attribuzione dei ruoli e dei poteri**, mediante una struttura organizzativa, un sistema dei poteri e delle deleghe semplici e trasparenti, con indicazione, quando richiesto, delle soglie di approvazione delle spese;

d) **Condivisione delle regole di *governance* e gestione**, descritte negli statuti degli organi sociali miranti ad assicurare un adeguato livello di collegialità al processo decisionale;

e) **Attuazione di un efficace sistema di controllo interno**, basato sulle seguenti regole:

- Ogni operazione, transazione, azione deve essere: verificabile, coerente e congrua, e adeguatamente supportata a livello documentale affinché si possa procedere, in ogni momento, all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione e individuino chi ha autorizzato, registrato e verificato l'operazione stessa;
- Nessuno deve poter gestire in autonomia un intero processo, ovvero deve essere rispettato il principio della separazione delle funzioni e dei poteri;
- I poteri autorizzativi devono essere assegnati coerentemente con le responsabilità assegnate;
- Il sistema di controllo deve documentare l'effettuazione dei controlli, compresa la supervisione;

f) **Attività di sorveglianza** sull'efficacia del sistema di controllo e, più in generale, sull'intero Modello di organizzazione, gestione e controllo:

- L'attribuzione ad un Organismo di Vigilanza interno alla Società del compito di promuovere l'attuazione efficace e corretta del Modello anche attraverso il monitoraggio dei comportamenti aziendali e il diritto ad una informazione costante sulle attività rilevanti ai fini del D.Lgs. 231/2001;
- La messa a disposizione a favore dell'Organismo di risorse adeguate affinché sia supportato nei compiti affidatigli per raggiungere i risultati ragionevolmente ottenibili;
- L'attività di verifica del funzionamento del Modello con conseguente aggiornamento periodico (controllo *ex post*);
- L'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;

g) Comunicazione trasparente e diffusa dei valori, dei principi e delle regole, accompagnata, ove necessario, da attività di specifica formazione sugli strumenti che compongono il Modello e che la Società attua per prevenire tutti i comportamenti illeciti;

h) Applicazione di meccanismi disciplinari e sanzionatori, per comportamenti non allineati all'applicazione del Modello da parte di NTT DATA Italia.

Il presente Modello è coerente anche con i principi cardine indicati dalla controllante NTT DATA Corp., contenendo comunque specificità insite nelle strutture organizzative e nelle attività di business di NTT DATA Italia, con ulteriori specifiche misure legate alla peculiarità della propria realtà aziendale e con uno stretto coordinamento con le procedure ed i protocolli del Sistema di Gestione per la Qualità e con la pertinente Certificazione ISO 9001 di cui la Società è munita.

2 MAPPATURA DEI RISCHI

2.1 Premessa

Il Modello organizzativo della Società è implementato tenendo conto di una effettiva compatibilità dello stesso con l'attuale organizzazione aziendale, in modo da integrarsi efficientemente con l'operatività del business subendo all'occorrenza, in modo elastico, le dovute modifiche.

Per questo, l'Organismo di Vigilanza, di cui si tratterà diffusamente più avanti, è munito dei poteri necessari ai fini dell'attività di monitoraggio e verifica del Modello.

Come suggerito dalle Linee Guida di Confindustria, la creazione e l'implementazione di un Sistema di Gestione del Rischio, prevede i seguenti elementi e passaggi:

1. *individuazione ed Analisi dei Rischi e dei Protocolli;*
2. *individuazione delle Componenti necessarie al Sistema;*
3. *regolamentazione e nomina dell'Organismo di Vigilanza;*
4. *definizione del Codice Etico dell'Azienda;*
5. *definizione del Sistema Sanzionatorio specifico.*

2.2 Individuazione dei rischi e protocolli

Ai fini della predisposizione del Modello, in primo luogo, NTT DATA Italia ha individuato e aggiornato nel corso del tempo i comportamenti a rischio rispetto alle funzioni aziendali e ai reati contemplati dal D.Lgs. 231/2001, a questi collegati. A seguito di questa fase di analisi e di studio il Modello ha l'obiettivo di:

1) Far assumere a tutti coloro che operano in nome e per conto di NTT DATA Italia nelle aree di attività a rischio la consapevolezza di poter intercorrere, in caso di violazione delle disposizioni ivi riportate, in un illecito passibile di sanzioni, sul piano penale e amministrativo, non solo nei propri confronti, ma anche nei confronti della società;

2) Ribadire che tali forme di comportamento illecito sono decisamente condannate dalla Società in quanto (anche nel caso in cui la Società fosse in condizione di trarne vantaggio) sono comunque contrarie alle disposizioni di legge vigenti ed ai principi affermati dalle *policies* aziendali e dal Codice di Condotta e che la Società si impegna nel modo più determinato a prevenire tali comportamenti;

3) Consentire alla Società, grazie ad un'azione di monitoraggio sulle attività a rischio, di intervenire tempestivamente per prevenire e contrastare, per quanto possibile, la commissione dei reati stessi, e cioè:

   a. individuando le attività nel cui ambito possono essere commessi Reati, così effettuando ed aggiornando periodicamente una mappatura delle aree aziendali in cui si svolgono le attività maggiormente a rischio;

b. prevedendo specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai Reati da prevenire;

c. individuando modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei Reati;

d. prevedendo obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;

e. introducendo sistemi di informazione e sensibilizzazione a tutti i livelli aziendali delle regole di condotta e delle procedure istituite e un sistema disciplinare efficace ed idoneo a sanzionare il mancato rispetto delle misure qui indicate;

f. prevedendo, in relazione alla natura e alla dimensione dell'organizzazione, nonché del tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

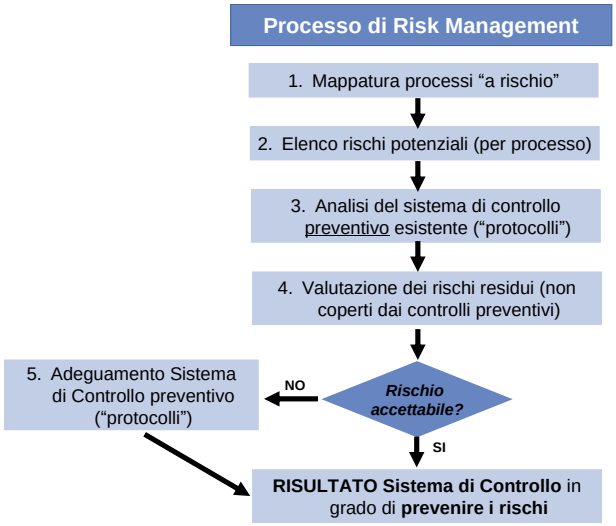
Come previsto dall'art. 6, co. 2, del D.Lgs. 231/2001, la realizzazione del sistema di gestione dei rischi (*risk management*) di NTT DATA Italia si articola in due fasi:

a) l'identificazione dei rischi attraverso l'analisi del contesto aziendale per evidenziare dove (in quale area/settore di attività) e secondo quali modalità si possono verificare ipotesi di reato;

b) la valutazione del sistema di controllo, ovvero la verifica che il sistema esistente all'interno della Società sia adeguato a mantenere i rischi evidenziati ad un livello accettabile e che sia programmato ed attuato il suo eventuale adeguamento/miglioramento, con l'obiettivo di ridurre la soglia minima del livello accettabile dei rischi identificati.

Sotto il profilo concettuale, ridurre un rischio comporta intervenire (congiuntamente o disgiuntamente) su due fattori determinanti:

- la probabilità di accadimento dell'evento;
- l'impatto dell'evento stesso.



L'individuazione delle aree/comportamenti aziendali a rischio è valutata sulla base del principio di potenziale accadimento sia in relazione al business, che rispetto alle funzioni coinvolte.

Questa valutazione, seppur di carattere preventivo, è la base di partenza per la definizione qualitativa del rischio come "*accettabile*" dalla Società, in quanto sono state messe in relazione l'incidenza e la probabilità di accadimento del rischio specifico.

Il sistema non può però, per operare efficacemente, ridursi a un'attività effettuata di tanto in tanto, bensì deve tradursi in un processo continuo (o periodico), da reiterare con particolare attenzione nei momenti di cambiamento aziendale (ad esempio: apertura di nuove sedi, ampliamento di attività, acquisizioni, riorganizzazioni, ecc.).

2.2.1 La definizione di "*rischio accettabile*"

La soglia concettuale di accettabilità del rischio è rappresentata da un sistema di prevenzione tale da non poter essere aggirato se non intenzionalmente.

Per quel che riguarda i reati societari si è provveduto a verificare, ad esempio, il processo di formazione del bilancio, la gestione delle informazioni *price sensitive*, le procedure di funzionamento degli organi sociali.

Oltre all'aspetto oggettivo, ovvero l'area di possibile violazione, si è tenuta in debita considerazione anche la prospettiva soggettiva, ovvero chi sono i soggetti, attivi o passivi, di eventuali violazioni.

Nell'ambito di questo procedimento di revisione dei processi/funzioni a rischio, è opportuno identificare gli oggetti interessati dall'attività di monitoraggio, che in talune circostanze particolari ed eccezionali, potrebbero includere anche coloro che siano legati all'impresa da meri rapporti di parasubordinazione, quali ad esempio i consulenti esterni, o da altri rapporti di collaborazione, come i partner commerciali, nonché i dipendenti ed i collaboratori di questi ultimi.

Nel medesimo contesto è altresì opportuno porre in essere esercizi di *due diligence* tutte le volte in cui in sede di valutazione del rischio siano stati rilevati "indicatori di sospetto" (ad esempio conduzione di trattative in territori con alto tasso di corruzione, procedure particolarmente complesse, presenza di nuovo personale sconosciuto alla Società) afferenti ad una particolare operazione commerciale.

I processi dell'area finanziaria rivestono una posizione di evidente rilievo ai fini dell'applicazione del D.Lgs. 231/2001 La norma, probabilmente proprio per questo motivo, li evidenzia con una trattazione separata (art. 6, co. 2, lett. c) ancorché un'accurata analisi di valutazione degli ambiti aziendali "a rischio" dovrebbe comunque far emergere quello finanziario come uno di sicura rilevanza.

2.2.2 Analisi dei rischi potenziali

L'analisi dei potenziali rischi è stata messa in relazione con i possibili comportamenti soggettivi che possono portare alla commissione dei Reati per ogni area aziendale coinvolta.

La sintesi di tale analisi è rappresentata attraverso una scheda di rilevazione (*check list* riportata nella Parte Speciale del Modello) nella quale le funzioni aziendali della Società e le attività specifiche di soggetti ed organi aziendali, sono state raffrontate ai possibili reati presupposto rilevanti per NTT DATA Italia.

2.2.3 Valutazione/costruzione/adeguamento del sistema di controlli preventivi

Le attività precedentemente descritte si completano con una valutazione preventiva del sistema di controlli esistente, al fine di consentire all'Organismo di Vigilanza un'analisi degli scostamenti tra quest'ultimo e il Modello di prevenzione, e il suo adeguamento quando ciò si riveli necessario.

Il sistema di controlli preventivi mira a garantire che i rischi di commissione dei Reati, secondo le modalità individuate e documentate nella fase precedente, siano ridotti ad un "livello accettabile", secondo la definizione sopra esposta.

Si tratta, in sostanza, di progettare quelli che il D.Lgs. 231/2001 definisce "*specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire*", attività che NTT DATA Italia ha provveduto a realizzare con l'adozione di strumenti, sistemi di controllo, procedure e *policies* aziendali in linea con la predetta indicazione normativa.

2.3 Rilevazione e mappatura dei rischi

NTT DATA Italia ha compiuto e aggiorna periodicamente l'analisi dei processi e dell'operatività aziendale per individuare le aree a rischio (mappatura dei rischi), intendendo per queste ultime le aree di attività che risultano interessate dalle potenziali casistiche di reato *ex* D.Lgs. 231/2001.

In tal senso si è proceduto a una rilevazione e mappatura dei rischi riscontrati con specifico riferimento alle attività aziendali effettivamente svolte e alle funzioni di fatto esercitate dagli operatori.

Questa analisi ha evidenziato quali attività siano maggiormente esposte alla commissione dei reati indicati dal Decreto o comunque da presidiare. Tali Reati e le macro-aree di attività in tal modo individuati sono risultati quelli di seguito indicati.

2.3.1 Reati contro la Pubblica Amministrazione (artt. 24 e 25, D.Lgs. 231/2001)

Le attività ritenute sensibili in relazione ai Reati contro la Pubblica Amministrazione sono:

a) Negoziazione/stipulazione e/o esecuzione di contratti/convenzioni di concessioni con soggetti pubblici, ai quali si perviene mediante procedure negoziate (affidamento diretto o trattativa privata);
b) Negoziazione/stipulazione e/o esecuzione di contratti/convenzioni di concessioni con soggetti pubblici ai quali si perviene mediante procedure ad evidenza pubblica (aperte o ristrette);
c) Negoziazione/stipulazione o esecuzione di contratti con soggetti pubblici ai quali si perviene mediante trattative private;
d) Negoziazione/stipulazione e/o esecuzione di contratti con soggetti pubblici ai quali si perviene mediante procedure aperte o ristrette;
e) Gestione dei rapporti con organismi/Autorità di vigilanza relativi allo svolgimento di attività regolate dalla legge;
f) Gestione delle attività di acquisizione o gestione di contributi, sovvenzioni, finanziamenti, assicurazioni o garanzie concesse da soggetti pubblici;
g) Richiesta di provvedimenti amministrativi occasionali/ad hoc necessari allo svolgimento di attività strumentali a quelle tipiche aziendali;
h) Predisposizione di dichiarazioni dei redditi o dei sostituti di imposta o di altre dichiarazioni funzionali alla liquidazione di tributi in genere;
i) Adempimenti presso soggetti pubblici, quali comunicazioni, dichiarazioni, deposito atti e documenti, pratiche, ecc, differenti da quelli descritti ai precedenti punti e nelle verifiche/accertamenti/procedimenti sanzionatori che ne derivano;

j) Attività che prevedano l'installazione, manutenzione, aggiornamento o gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici;
k) Altre "*attività sensibili*": rapporti con le Istituzioni e le amministrazioni dello Stato.

2.3.2 Reati Societari (art. 25-*ter*, D.Lgs. 231/2001)

Le attività ritenute sensibili in relazione ai reati societari sono:

a) Redazione del bilancio e relazioni periodiche infrannuali;
b) Rapporti con soci, Società di Revisione, Collegio Sindacale, Audit e rapporti con Autorità di vigilanza;
c) Operazioni sul capitale e destinazione dell'utile;
d) Comunicazione, svolgimento e verbalizzazione Assemblee dei soci;
e) Gestione rapporti commerciali e trattative nei confronti della clientela privata e dei fornitori (con riferimento al reato di Corruzione tra privati e istigazione alla corruzione tra privati).

2.3.3 Reati contro la salute e sicurezza sul lavoro (art. 25-*septies*, D.Lgs. 231/2001)

Le attività ritenute sensibili in relazione ai reati in materia di salute e sicurezza sul lavoro, sono:

a) Istituzione e controllo del sistema di gestione della sicurezza e salute nei luoghi di lavoro;
b) Fasi esecutive di contratti di appalto, d'opera e di somministrazione;
c) Affidamento in qualità di committente di lavori e/o servizi all'interno delle proprie sedi.

2.3.4 Reati Informatici (art. 24-*bis*, D.Lgs. 231/2001)

Le attività e le condotte integranti le fattispecie di Reati informatici sono:

a) Accedere ad un sistema informatico protetto da misure di sicurezza;
b) Gestire codici, parole chiave, credenziali di accesso a sistemi informatici protetti da misure di sicurezza;
c) Riprodurre, diffondere, duplicare, commercializzare o mettere a disposizione di terzi programmi per elaboratore o altri beni di proprietà intellettuale in violazione di norme in materia di tutela del diritto d'autore.

2.3.5 Delitti in materia di violazione del diritto d'autore (art. 25-*novies*, D.Lgs. 231/2001)

Le attività che integrano fattispecie di Reati in materia di diritto d'autore sono:

a) Duplicare, importare, distribuire, vendere, concedere in locazione, diffondere/trasmettere al pubblico, detenere a scopo commerciale, o comunque per trarne profitto, senza averne diritto, programmi per elaboratori, banche dati protette ovvero qualsiasi opera protetta dal diritto d'autore o da diritti connessi, incluse opere a contenuto letterario, musicale, multimediale, cinematografico, artistico;
b) Diffondere tramite reti telematiche – senza averne diritto un'opera di ingegno o parte di essa;
c) Mettere in atto pratiche di *file sharing*;
d) Condividere qualsivoglia file attraverso piattaforme di tipo *peer-to-peer*.

2.3.6 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies*, D.Lgs. 231/2001)

Le attività riconducibili nel Reato in oggetto sono:

a) Fornire indicazioni idonee ad influenzare una persona chiamata a rendere dichiarazioni davanti all'Autorità Giudiziaria al fine di ottenere trattamenti di favore da parte di quest'ultima in relazione a processi o istruttorie in corso.

2.3.7 Impiego di cittadini terzi il cui soggiorno è irregolare (art. 25-*duodecies*, D.Lgs. 231/2001)

Le attività ritenute sensibili in relazione al Reato in oggetto sono:

a) Selezione ed assunzione del Personale;
b) Gestione del personale dipendente extracomunitario.

2.3.8 Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-*octies*, D.Lgs. 231/2001)

Pur se il rischio di commissione dei suddetti Reati appare del tutto teorico e residuale tenuto conto dei settori di attività in cui opera NTT DATA Italia si è ritenuto utile dedicare, nella Parte Speciale del Modello, un apposito paragrafo a tale tipologia di Reati in considerazione della loro rilevante pericolosità sociale, indicando misure, procedure e strumenti di controllo – in larga parte già presenti in NTT DATA Italia - idonei a prevenire il relativo rischio di commissione.

2.3.9 Autoriciclaggio (art. 25-*octies*, D.Lgs. 231/2001)

L'art. 3, comma 5, della L. n. 186 del 15/12/2014 ("*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 autoriciclaggio*") ha modificato l'articolo 25-*octies* del D.Lgs. 231/2001, introducendo nel novero dei reati presupposto, il reato di autoriciclaggio di cui all'art. 648-*ter*.1 del Codice Penale, punibile a partire dal 1° gennaio 2015. Di tale Reato, delle attività aziendali sensibili e dei relativi presidi, si tratterà in un apposito paragrafo della Parte Speciale del Modello, tenuto conto sia della complessità che presenta l'individuazione delle aree aziendali nelle quali potrebbe astrattamente essere commesso, sia della mancanza, allo stato attuale, di orientamenti giurisprudenziali consolidati in materia (l'introduzione dell'autoriciclaggio nel nostro ordinamento giuridico, nonché nel "catalogo" dei Reati 231, è avvenuta – come sopra evidenziato - in epoca recente).

2.3.10 Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-*octies.1*, D.Lgs. 231/2001)

L'attività ritenuta sensibile in relazione ai delitti in oggetto è l'elaborazione e diffusione di strumenti e programmi informatici.

2.3.11 Delitti contro la personalità individuale (art. 25-*quinquies*, D.Lgs. 231/2001)

Il 4 novembre 2016 è entrata in vigore la Legge 29 ottobre 2016, n. 199 che ha inserito nell'art. 25-*quinquies* D.Lgs. 231/2001 il nuovo reato di "intermediazione illecita e sfruttamento del lavoro" (art. 603-*bis* c.p.), c.d.

"*caporalato*" che punisce le condotte di reclutamento e assunzione di manodopera allo scopo di destinarla al lavoro in condizioni di sfruttamento.
Le attività ritenute sensibili in relazione al reato di caporalato sono quelle relative alla gestione di personale utilizzato in subappalto.

2.3.12 Reati tributari (art. 25-*quinquiesdecies*, D.Lgs. 231/2001)

Le attività ritenute sensibili in relazione ai reati tributari sono:

a) Attività di fatturazione attiva e di recupero crediti;
b) Attività di fatturazione passiva e pagamento fornitori;
c) Selezione e gestione dei fornitori;
d) Gestione della liquidità e dei conti correnti societari;
e) Gestione degli adempimenti fiscali e previdenziali;
f) Conservazione della documentazione contabile;
g) Pagamento delle imposte;
h) Gestione dei rapporti con i Pubblici Ufficiali in caso di verifiche/visite ispettive.

2.3.13 Delitti in materia di contrabbando (art. 25-*sexiesdecies*, D.Lgs. 231/2001)

Le attività ritenute sensibili in relazione ai delitti in oggetto sono:

a) Adempimento dei diritti di confine;
b) Selezione e gestione dei fornitori.

2.3.14 Ulteriori attività oggetto di controllo

Oltre ai presidi e ai controlli riguardanti direttamente le aree e le attività nel cui ambito possano astrattamente essere commessi i Reati sopra indicati, il Modello 231 prevede ulteriori, specifici controlli per i seguenti processi di gestione delle "provviste" o strumentali:

a) Transazioni finanziarie;
b) Approvvigionamento beni e servizi;
c) Utilizzo delle risorse materiali di impatto ambientale;
d) Consulenze e prestazioni professionali;
e) Concessioni di utilità (erogazione liberalità, borse di studio, sponsorizzazione eventi);
f) Gestione amministrativa, finanziaria e contabile necessaria alla conduzione della società;
g) Gestione delle risorse umane (selezione e assunzione di personale, sistema di incentivazione).

Tra le aree di attività a rischio il Modello ha infatti considerato oltre a quelle aventi un rilievo diretto come attività che potrebbero teoricamente integrare condotte di reato, anche quelle aventi un rilievo indiretto e strumentale nella commissione dei Reati. In particolare, si intendono strumentali quelle attività nelle quali possono realizzarsi le condizioni di fatto che rendono possibile la commissione di Reati nell'ambito delle aree e delle attività specificamente considerate a rischio di reato nel Modello.

3 VALORI E REGOLE DI COMPORTAMENTO

3.1 Codice di Condotta Commerciale Globale

NTT DATA Italia ha raccolto e descritto i valori comuni a tutti coloro che operano all'interno del Gruppo NTT DATA nel Codice di Condotta Commerciale Globale, approvato e aggiornato nel tempo dal Consiglio di Amministrazione.

Questo Codice esprime gli impegni e le responsabilità etiche nella conduzione degli affari e delle attività aziendali assunti da NTT DATA Italia verso tutti i portatori di interesse ("*stakeholder*"), nella convinzione che l'etica sia perseguibile congiuntamente al successo d'impresa.

Il documento è disponibile sul **sito internet di NTT DATA Italia** e sulla **intranet aziendale,** ed è diffuso in lingua italiana e inglese (sono eventualmente disponibili edizioni anche in altre lingue).

3.2 *Policy*, procedure e istruzioni

Sono state elaborate e diffuse *policies*, procedure e istruzioni che descrivono i processi sensibili e i comportamenti standard per garantire ai dipendenti e ai collaboratori di NTT DATA Italia un indirizzo sui comportamenti che la Società ritiene allineati ai valori espressi dal Codice di Condotta e dal presente Modello.

Tutte le *policies* e le procedure aziendali sono inviate/comunicate ai singoli dipendenti ogni qualvolta vi siano aggiornamenti di contenuto o di forma, e di norma pubblicate nella intranet aziendale.

3.3 Procedure sulla gestione delle risorse finanziarie

Le transazioni finanziarie della Società sono documentate e riferite in processi che codificano in modo chiaro e trasparente le attività, indicando gli autori responsabili secondo l'organizzazione aziendale.

Le registrazioni contabili di natura monetaria sono svolte secondo i vigenti principi contabili e NTT DATA Italia assicura l'utilizzo di metodologie e prassi omogenee fra le diverse unità responsabili della redazione dell'informativa amministrativo-contabile propria e delle società controllate.

4 SISTEMA ORGANIZZATIVO, RUOLI E POTERI

4.1 Caratteristiche della Struttura Organizzativa

NTT DATA Italia è dotata di strumenti organizzativi fondati sui principi generali di:

- Conoscibilità all'interno della Società e del Gruppo;
- Indicazione dei ruoli (inclusi i poteri assegnati);
- Indicazione delle linee di riporto.

4.2 Definizione dei ruoli

La definizione dei ruoli è tale da assicurare che un processo non sia mai seguito in autonomia da una sola persona, sia nel caso di processi operativi di sviluppo e gestione dei progetti, sia nel caso dei processi interni di supporto.

I processi operativi di sviluppo e gestione del progetto, che, in altri termini, rappresentano i processi di vendita e produzione, sono presidiati dalle linee attraverso team di lavoro composti da diverse qualifiche, dove ognuno contribuisce alla formulazione di proposte e soluzioni al cliente, secondo uno stile collaborativo e in base alle proprie competenze e qualifica. Durante le fasi di sviluppo e gestione di progetto, le operazioni che hanno un impatto, anche solo potenziale, sulle risorse finanziare d'impresa (sia in entrata che in uscita) sono monitorate e documentate. Il controllo è responsabilità delle Business Review mensili e della Direzione, attraverso la reportistica prodotta dalla Funzione Amministrazione, Finanza e Controllo - *AFC* (anche solo "**Finance**") che, tra l'altro, è incaricata di segnalare comportamenti non allineati agli standard.

La Funzione AFC da un lato supporta le linee operative in merito alla generazione e all'utilizzo delle risorse finanziarie legate alla gestione caratteristica, dall'altra supporta il *top management* nella gestione delle risorse finanziarie relative alla gestione patrimoniale, straordinaria e tributaria. La Direzione e gli Organi sociali hanno la responsabilità di verificare l'andamento economico e finanziario della gestione sulla base della reportistica preparata dalla Funzione AFC.

Gli avanzamenti di qualifica all'interno delle linee operative e i cambiamenti di ruolo, più in generale, delle funzioni di staff sono comunicati ai dipendenti della Società (e del Gruppo, qualora siano all'interno di Funzioni di Corporate).

4.3 Sistema delle deleghe e delle procure

Il sistema delle deleghe e delle procure assicura il funzionamento aziendale calando i poteri necessari al Consiglio di Amministrazione, all'Amministratore Delegato e ai vari delegati.

Per "*delega*" si intende l'atto interno di attribuzione di compiti e funzioni attraverso comunicazioni organizzative e procedure aziendali; per "*procura*" il negozio giuridico unilaterale con cui la società attribuisce poteri di rappresentanza esterna verso terzi. Ai titolari di una funzione che ha necessità di poteri di rappresentanza è conferita una procura adeguata e coerente con i compiti assegnati.

Le caratteristiche principali del sistema delle deleghe sono:

- La delega riflette il posizionamento organizzativo di chi la riceve, coniugando potere di gestione e relativa responsabilità;
- Ogni delega esplicita in modo chiaro e univoco i poteri e il delegato.

Gli elementi distintivi del sistema delle procure sono:

- La procura è conferita esclusivamente a soggetti dotati di delega attraverso appositi atti che descrivono i poteri di rappresentanza e, laddove necessario, i poteri di spesa nonché il rispetto dei Modelli Organizzativi e Codice Etico della Società;

- Gli acquisti per importi elevati (soglie indicate negli atti di delega) devono essere autorizzati dall'AD;
- Gli ordini di acquisto devono essere emessi dal Responsabile degli Acquisti (verificati anche dal Controllo di Gestione) e ne viene garantita la tracciabilità tramite utilizzo di apposite tecnologie informatiche (esempio Portale Fornitori).

5 CORPORATE GOVERNANCE E DIREZIONE D'IMPRESA

5.1 Modello di *Corporate Governance*

In concomitanza con la richiesta di quotazione ai mercati regolamentati (prima metà del 2006), la Società aveva avviato un processo di adeguamento del proprio Modello di *Corporate Governance* ai requisiti del Codice di Autodisciplina delle Società Quotate con l'obiettivo di garantire ai propri azionisti un sistema di governance e di direzione efficace e trasparente.

Il Modello di *Corporate Governance* è stato successivamente adeguato e semplificato a seguito della decisione di rinviare la quotazione in Borsa.

Attualmente, anche a seguito delle recenti variazioni in ordine all'assetto societario e di controllo, il Modello di *Corporate Governance* si compendia nel Consiglio di Amministrazione, nonché nel Collegio Sindacale.

5.2 Comitati Aziendali

Sono operativi Comitati Aziendali e di Gruppo. Ad esempio, è attivo il comitato di Direzione che affronta temi strategici per lo sviluppo del Gruppo in sede di *Business Review*, in cui sono definite priorità commerciali ed elaborato il budget annuale, nonché condiviso l'andamento economico alla luce degli obiettivi.

6 SISTEMA DI CONTROLLO INTERNO

6.1 Funzione Amministrazione, Finanza e Controllo

All'interno dell'organizzazione aziendale di NTT DATA Italia sono state identificate le unità preposte al funzionamento dei sistema di controllo interno al fine di raggrupparle sotto il titolo di "Funzione Amministrazione, Finanza e Controllo", come già si è accennato al precedente par. 4.2. Coloro che gestiscono e controllano le risorse finanziarie della Società agiscono secondo i medesimi principi e le stesse regole di comportamento, adottando un unico Modello di controllo basato su processi, strumenti e tecniche operative simili salvo specificità di business o di Paese.
Il capo della Funzione è il *Chief Financial Officer* (CFO) che definisce la struttura organizzativa delle unità di cui è responsabile, articola i processi di pianificazione e controllo, secondo modalità e tempi allineati alle norme e alle esigenze di indirizzo e supervisione espresse dal Vertice e dagli Organi Sociali.

6.2 I processi e gli strumenti

Il sistema di controllo interno è definito come l'insieme dei processi attuati dal *management* finalizzato a fornire una ragionevole sicurezza sul conseguimento degli obiettivi di gestione e di *compliance*, quali l'efficacia ed efficienza delle attività operative, l'attendibilità delle informazioni aziendali, contabili e gestionali, sia a fini interni sia per soggetti terzi, e la assoluta conformità alle leggi, ai regolamenti, alle norme e alle *policies* aziendali e di gruppo.

7 ORGANISMO DI VIGILANZA

7.1 Nomina e composizione dell'Organismo

L'Organismo è un organo collegiale composto da tre membri effettivi, dei quali uno con funzioni di Presidente scelto a maggioranza dall'Organismo medesimo, ove non sia già indicato dal Consiglio in sede di nomina. L'organo collegiale si compone come segue:

- due professionisti esterni con competenze in materia legale, gestionale, di analisi dei sistemi di controllo o comunque di alta esperienza nelle problematiche di specifica attinenza alle attività di competenza dell''Organismo di Vigilanza[1];
- il Responsabile della Funzione Legale.

Il Consiglio di Amministrazione, riferendone all'Assemblea degli Azionisti, ha la competenza di nominare e revocare – per giusta causa, anche legata ad interventi di ristrutturazione organizzativa della Società – i membri dell'Organismo. I membri dell'Organismo sono scelti tra soggetti qualificati ed esperti negli ambiti sopra indicati, dotati di adeguata professionalità e in possesso dei requisiti di indipendenza, autonomia e onorabilità, anche sotto il profilo dell'insussistenza di condanne penali, come meglio infra indicato. I membri dell'Organismo possono essere nominati sia tra soggetti esterni sia tra soggetti interni alla Società. I membri dell'Organismo non sono soggetti, in tale qualità e nell'ambito dello svolgimento della propria funzione, al potere gerarchico e disciplinare di alcun organo o funzione societaria.

L'incarico dell'OdV ha generalmente durata triennale, fatta salva la facoltà del Consiglio di Amministrazione di stabilire una durata inferiore dell'incarico. Alla scadenza del triennio – o del minor periodo di durata dell'incarico stabilito dal Consiglio di Amministrazione –, l'OdV continua a svolgere in regime di *prorogatio* le proprie funzioni fino alla nomina dei nuovi componenti da parte del Consiglio di Amministrazione. I membri dell'OdV sono rieleggibili.

I componenti interni dell'Organismo decadono in caso di cessazione volontaria del rapporto di lavoro o di collaborazione con NTT DATA e di licenziamento per giusta causa e in aggiunta, per il Responsabile della funzione legale, in caso di cessazione dal ruolo di Responsabile della stessa funzione. In caso di dimissioni, rinuncia, sopravvenuta incapacità, morte, revoca o decadenza di un componente dell'Organismo, il Consiglio di Amministrazione provvederà, senza indugio, alla sua sostituzione. È fatto obbligo al Presidente, ovvero al componente più anziano, di comunicare tempestivamente al Consiglio di Amministrazione il verificarsi di una delle ipotesi dalle quali derivi la necessità di reintegrare un componente dell'Organismo.

In caso di dimissioni, rinuncia, sopravvenuta incapacità, morte, revoca o decadenza del Presidente, subentra a questi il componente più anziano di età, il quale rimane in tale carica fino alla data in cui il Consiglio di Amministrazione abbia deliberato la nomina del nuovo Presidente dell'Organismo.

[1] Disposizione aggiornata con delibera del CdA del 29 giugno 2023.

Per tutti gli altri aspetti l'OdV opera secondo quanto previsto dal proprio Regolamento, di cui appresso. L'Organismo di Vigilanza disciplina le proprie attività di vigilanza e controllo per il tramite di un Regolamento da trasmettere al Consiglio di Amministrazione della Società per la relativa presa d'atto nella prima riunione utile, come pure le eventuali modifiche che l'Organismo riterrà necessario apportare allo stesso nel corso del suo incarico.

7.2 Competenze e Cause di (in)eleggibilità, decadenza e sospensione

Competenze

Le competenze dei componenti dell'Organo di Vigilanza, sommariamente suddivise tra competenze legali e organizzative, possono essere così riassunte:

Competenze di natura legale: ovvero approfondita conoscenza delle metodologie utilizzate nell'interpretazione delle norme di legge con specifica preparazione nell'analisi delle fattispecie di reato e nell'individuazione delle possibili condotte sanzionabili.
Tale preparazione presuppone una dimestichezza con la ricerca e l'analisi della giurisprudenza in materia. La risorsa in commento deve essere, in sintesi, capace di esaminare e interpretare il dettato normativo individuando le fattispecie di reato, nonché l'applicabilità di tali fattispecie nell'ambito della operatività aziendale. Deve inoltre essere in possesso di conoscenza dell'operatività aziendale, maturata in posizione di responsabilità e di inquadramento gerarchico all'interno dell'impresa e di capacità di tradurre in norme di comportamento i processi delineati nel Modello organizzativo dedicato alla prevenzione dei rischi.

Competenza di natura organizzativa, ovvero specifica preparazione sul tema dell'analisi delle procedure e dei processi organizzativi aziendali, nonché dei principi generali sulla legislazione in materia di "compliance" e dei controlli alla stessa correlati. Almeno uno dei membri dell'Organismo di Vigilanza dovrà avere esperienza nella predisposizione di procedure e manuali di controllo. Il profilo è quindi quello di un esperto di controlli interni che abbia maturato tale esperienza nell'ambito di attività già da tempo "vincolate" e "vigilate".

Competenza nel settore nel quale la Società svolge la propria gestione caratteristica e/o con esperienza nelle attività maggiormente esposte al rischio di reato-presupposto.

È garantita, in ragione del posizionamento riconosciuto alle funzioni citate nel contesto dell'organigramma aziendale e delle linee di riporto ad esse attribuite, la necessaria autonomia dell'Organismo di Vigilanza.

Al fine di coadiuvare la definizione e lo svolgimento delle attività di competenza e di consentire la massima adesione ai requisiti e compiti di legge, l'Organismo di Vigilanza:

- si avvale della funzione Internal Audit, ove istituita, o funzione equivalente, dotata di risorse adeguate;
- può coinvolgere le opportune risorse aziendali per estrarre, elaborare dati e produrre reportistica.

Cause di (in)eleggibilità, decadenza e sospensione dei membri dell'Organismo di Vigilanza

I componenti dell'Organismo di Vigilanza devono essere in possesso dei requisiti di onorabilità di cui all'art. 26 del D.Lgs. 1 settembre 1993, n. 385: in particolare, non possono essere nominati componenti dell'Organismo di Vigilanza coloro che si trovino nelle condizioni previste dall'art. 2382 c.c.

Non possono, inoltre, essere nominati alla carica di componenti dell'Organismo di Vigilanza coloro i quali sono stati condannati con sentenza ancorché non definitiva, ed anche se emessa *ex* artt. 444 e ss. c.p.p. e anche

se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:

1) alla reclusione per un tempo non inferiore ad un anno per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267;
2) a pena detentiva per un tempo non inferiore ad un anno per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
3) alla reclusione per un tempo non inferiore ad un anno per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, per un delitto in materia tributaria;
4) per un qualunque delitto non colposo alla pena della reclusione per un tempo non inferiore a due anni;
5) per uno dei reati previsti dal titolo XI del libro V del codice civile così come riformulato del decreto legislativo n. 61/2002;
6) per un reato che importi e abbia importato la condanna ad una pena da cui derivi l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;
7) per uno o più reati tra quelli tassativamente previsti dal Decreto anche se con condanne a pene inferiori a quelle indicate ai punti precedenti;
8) coloro che hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate le sanzioni previste dall'art. 9 del Decreto;
9) coloro nei cui confronti sia stata applicata una delle misure di prevenzione previste dall'art. 10, comma 3, della legge 31 maggio 1965, n. 575, come sostituito dall'articolo 3 della legge 19 marzo 1990, n. 55 e successive modificazioni;
10) coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187-*quater* del D.Lgs. n. 58/1998.

I candidati alla carica di membri dell'Organismo di Vigilanza devono autocertificare con dichiarazione sostitutiva di notorietà *ex* D.P.R. n. 445/2000 di non trovarsi in alcuna delle condizioni indicate dal numero 1 al numero 10, impegnandosi espressamente a comunicare eventuali variazioni rispetto al contenuto di tali dichiarazioni.

I membri dell'Organismo di Vigilanza decadono dalla carica nel momento in cui vengano a trovarsi, successivamente alla loro nomina, in una delle situazioni sopra indicate.

Infine non possono essere nominati, o decadono, coloro che si trovino in una delle seguenti condizioni:

- Conflitti d'interesse, anche potenziali, con la Società tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti che si andrebbero a svolgere;
- Titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere loro di esercitare una notevole influenza sulla Società;
- Rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina a membro dell'OdV.

7.3 Funzioni e poteri

L'Organismo di Vigilanza definisce e svolge le attività di competenza secondo la regola della collegialità ed è dotato ai sensi dell'art. 6, comma 1, lett. b), del D.Lgs. 231/2001 di "autonomi poteri di iniziativa e controllo".

Le attività che l'Organismo è chiamato ad assolvere sono:

- Vigilanza sull'**effettività** del Modello, che si sostanzia nella verifica della coerenza tra i comportamenti concreti ed il Modello istituito;

- Disamina in merito all'**adeguatezza** del Modello, ossia della sua reale (e non meramente formale) capacità di prevenire, in linea di massima, i comportamenti non voluti;

- Analisi circa il **mantenimento** nel tempo dei requisiti di solidità e funzionalità del modello;

- Cura del necessario **aggiornamento** in senso dinamico del Modello, nell'ipotesi in cui le analisi operate rendano necessario effettuare correzioni ed adeguamenti. Tale cura, di norma, si realizza in due momenti distinti e integrati:
    - **Presentazione di proposte di adeguamento** del Modello verso gli organi/funzioni aziendali in grado di dare loro concreta attuazione nel tessuto aziendale. A seconda della tipologia e della portata degli interventi, le proposte saranno dirette verso le funzioni di Personale/HR ed Organizzazione, Amministrazione, ecc., o, in taluni casi di particolare rilevanza, verso il Consiglio di Amministrazione;
    - ***Follow-up***, ossia verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte.

L'Organo di Vigilanza, avvalendosi dei poteri allo stesso attribuiti, è chiamato pertanto in concreto a svolgere primariamente le seguenti attività:

- Stabilire le attività di controllo ad ogni livello operativo, dotandosi degli strumenti, informativi e non, atti a segnalare tempestivamente anomalie e disfunzioni del Modello verificando ed approntando, laddove necessario, i manuali di controllo;

- Attivare le procedure di controllo tenendo presente l'esigenza di snellezza delle procedure e il fatto che la responsabilità primaria sul controllo delle attività è comunque demandata ai Responsabili delle Funzioni e/o ai vertici aziendali, agli organi sociali a ciò deputati e alla società di revisione;

- Attivarsi per mantenere aggiornato il Modello conformemente alla evoluzione della normativa vigente in materia, nonché in conseguenza delle modifiche all'organizzazione interna e all'attività aziendale;

- Collaborare alla predisposizione ed integrazione della "normativa" interna (Codici deontologici e di comportamento, Procedure/Istruzioni operative, Manuali di controllo, ecc.) dedicata alla prevenzione dei rischi;

- Identificare, misurare e monitorare adeguatamente tutti i rischi assunti o assumibili nonché derivanti dalla interpretazione ed applicazione delle norme di riferimento, rispetto ai reali processi e procedure aziendali e con riferimento ai diversi segmenti operativi dell'azienda, procedendo ad un costante aggiornamento dell'attività di rilevazione e mappatura dei rischi;

- Promuovere iniziative atte a diffondere la conoscenza tra gli organi ed i dipendenti della società del Modello fornendo le istruzioni ed i chiarimenti eventualmente necessari, nonché istituendo specifici seminari di formazione;

- Provvedere a coordinarsi con le altre funzioni aziendali per un miglior controllo delle attività e per tutto quanto attenga alla concreta attuazione del Modello;

- Disporre verifiche straordinarie e/o indagini mirate laddove si evidenzino disfunzioni del Modello o si sia verificata la commissione dei reati oggetto delle attività di prevenzione;

- Assicurare l'elaborazione del programma di vigilanza approvato, in coerenza con i principi contenuti nel Modello 231, nell'ambito dei vari settori di attività; assicurare il coordinamento dell'attuazione del programma di vigilanza e l'attuazione degli interventi di controllo programmati e non programmati.

Al fine di rendere realizzabile l'attività dell'Organismo di Vigilanza, è necessario che:

- Le attività poste in essere dall'Organismo non possano essere sindacate da alcun altro organismo o struttura aziendale, fermo restando però che l'organo dirigente è in ogni caso chiamato a svolgere un'attività di vigilanza sull'adeguatezza del suo intervento, in quanto all'organo dirigente ritorna la responsabilità ultima del funzionamento e dell'efficacia del Modello organizzativo;

- L'Organismo di Vigilanza abbia libero accesso presso tutte le funzioni della società senza necessità di alcun consenso preventivo al fine di ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D.Lgs. 231/2001;

- L'Organismo possa avvalersi sotto la propria diretta sorveglianza e responsabilità dell'ausilio di tutte le strutture della società ovvero di consulenti esterni.

Nel contesto delle procedure di formazione del budget aziendale, l'Organismo di Vigilanza avrà a propria disposizione una dotazione di risorse finanziarie, proposta dall'Organismo stesso, della quale l'Organismo potrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte ecc.).

Nello svolgimento dei compiti assegnati, l'Organismo di Vigilanza ha accesso senza limitazioni alle informazioni aziendali per le attività di indagine, analisi e controllo. È fatto obbligo di informazione, in capo a qualunque funzione aziendale, dipendente e/o componente degli organi sociali, a fronte di richieste da parte dell'Organismo di Vigilanza o al verificarsi di eventi o circostanze rilevanti ai fini nello svolgimento delle attività di competenza dell'Organismo di Vigilanza.

7.4 Obblighi di informazione dell'Organismo di Vigilanza

L'obbligo di informazione nei confronti dell'Organismo di Vigilanza è un ulteriore strumento per agevolare l'attività di vigilanza sull'efficacia del Modello e di accertamento a posteriori delle cause che hanno reso possibile il verificarsi del reato.

Tale obbligo è rivolto alle funzioni aziendali a rischio reato e riguarda: ***a)*** le risultanze periodiche dell'attività di controllo dalle stesse posta in essere per dare attuazione ai modelli (report riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.); ***b)*** le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non rilevante se singolarmente considerato potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento).

Le suddette informazioni sono indirizzate all'OdV con cadenza semestrale (**flussi informativi ordinari**), e riguardano, ad esempio:

- Le decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- Statistiche relative agli incidenti sul luogo di lavoro con specificazione della causa/motivo, l'avvenuto, l'eventuale riconoscimento di infortunio e la relativa gravità;
- Elenco delle eventuali cause legali pendenti che coinvolgono la Società (non già segnalate all'OdV tempestivamente);
- Le commissioni di inchiesta o relazioni interne dalle quali possano teoricamente emergere responsabilità per le ipotesi di reato di cui al D.Lgs. 231/2001;
- I prospetti riepilogativi degli appalti affidati a seguito di gare a livello nazionale ed europeo, ovvero a trattativa privata;
- Le notizie relative a commesse attribuite da enti pubblici o soggetti che svolgano funzioni di pubblica utilità;
- Le eventuali forniture richieste eccezionalmente ai fornitori in stato 'Black List';
- Il blocco delle attività di fatturazione relativa a fatture superiori all'importo di 500K€ prive di un adeguato supporto documentale/contrattuale;
- Le eventuali visite ispettive esterne condotte da Funzionari Pubblici, con breve descrizione dell'attività svolta.

Oltre ai flussi informativi ordinari, di cui sopra devono essere obbligatoriamente e tempestivamente trasmesse all'OdV informazioni riguardanti situazioni e/o eventi particolari o determinati, come in appresso specificati (**flussi informativi straordinari**) concernenti:

- I 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 di cui al D.Lgs. 231/2001;
- Le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;
- Qualsiasi fatto, atto, evento od omissione rilevato od osservato nell'esercizio delle responsabilità e dei compiti assegnati, con profili di criticità rispetto all'osservanza delle norme del decreto;
- Le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello organizzativo, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i Dipendenti), ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

L'Organismo di Vigilanza potrà proporre all'Amministratore Delegato eventuali modifiche delle liste sopra indicate. L'eventuale omessa o ritardata comunicazione all'OdV dei flussi informativi sopra elencati sarà considerata violazione del Modello organizzativo e potrà essere sanzionata secondo quanto previsto dal Sistema Disciplinare di cui al successivo paragrafo 9.2.

Le informazioni fornite consentono all'OdV di migliorare le proprie attività di pianificazione dei controlli e non ad imporgli attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati. In altre parole, all'Organismo non incombe un obbligo di agire ogni qualvolta vi sia un'informativa/segnalazione, essendo rimesso alla sua discrezionalità e responsabilità di stabilire in quali casi attivarsi.

7.5 Segnalazioni all'OdV da parte di dipendenti o esponenti aziendali o da parte di terzi

In ambito aziendale dovrà essere portata a conoscenza dell'Organismo di Vigilanza, oltre alla documentazione

prescritta dalle procedure contemplate nel presente Modello, ogni altra informazione, di qualsiasi tipo, proveniente da terzi e attinente all'attuazione del Modello nelle aree di attività a rischio.

In particolare, l'obbligo di informazione è esteso anche ai dipendenti che vengano in possesso di notizie relative alla commissione dei reati in specie all'interno dell'ente o che apprendano nell'esercizio delle loro funzioni della perpetrazione di pratiche non in linea con le norme di comportamento che l'ente è tenuto ad emanare (come visto in precedenza) nell'ambito del Modello *ex* D.Lgs. 231/2001 (i c.d. codici etici).

L'obbligo di informare il datore di lavoro di eventuali comportamenti contrari al Modello organizzativo rientra nel più ampio dovere di diligenza e obbligo di fedeltà del prestatore di lavoro di cui agli artt. 2104 e 2105 c.c.

Tali norme stabiliscono, rispettivamente:

- "*Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale*" (art. 2104 c.c.);
- "*Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende*" (art. 2104 c.c.) e "*Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio*". (art. 2105 c.c.).

Nel disciplinare un sistema di *reporting* efficace è garantita la riservatezza a chi segnala le violazioni nel rispetto della Legge 30 novembre 2017 n. 179. Allo stesso tempo, sono previste misure deterrenti contro ogni informativa impropria, sia in termini di contenuti che di forma.

NTT DATA Italia S.p.A, al fine di garantire una gestione responsabile ed in linea con le prescrizioni legislative, ha implementato un sistema di **Whistleblowing**, adeguato alle modifiche normative introdotte dal D.Lgs. 10 marzo 2023, n. 24, che ha recepito la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

In generale, la normativa in tema di segnalazione delle violazioni è ampiamente disciplinata dal D.Lgs. 24/2023 – al quale si rinvia –, che prevede, per quanto si ritiene opportuno evidenziare in questa sede:

- la possibilità di segnalare le violazioni – cioè comportamenti, atti od omissioni che ledono l'interesse dell'ente – che si ritiene siano state commesse, tra cui rientrano: (*i*) gli illeciti amministrativi, contabili, civili e penali e (*ii*) le condotte illecite rilevanti ai sensi del Decreto 231, o violazioni dei modelli di organizzazione e gestione;

- l'individuazione di una persona, di un ufficio interno autonomo dedicato o di un soggetto esterno e autonomo per la gestione del canale di segnalazione;

- l'individuazione di specifici canali, anche informatici, di segnalazione interna delle violazioni, in forma scritta e/o orale;

- la riservatezza e la confidenzialità delle informazioni ricevute e la protezione dei dati personali del segnalante e del segnalato;

- precise tempistiche per l'avvio, lo svolgimento e la conclusione dell'attività istruttoria effettuata dal soggetto che gestisce la segnalazione;

- il divieto di ritorsioni nei confronti del segnalante, cioè di qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, che provoca o può provocare alla persona segnalante, in via diretta o indiretta, un danno ingiusto;

- la nullità degli atti di ritorsione eventualmente posti in essere nei confronti del segnalante;

la previsione di sanzioni disciplinari: (*i*) per coloro che violino la riservatezza del segnalante; (*ii*) per coloro che inviino, con dolo o colpa grave, segnalazioni infondate (*iii*) nel caso di commissione di una ritorsione nei confronti del segnalante e (*iv*) nel caso in cui la segnalazione sia stata ostacolata o vi sia stato il tentativo di ostacolarla.
La Società ha implementato la **procedura per le segnalazioni del *whistleblower***, alla quale si rinvia.

Tale procedura costituisce parte integrante del Modello 231

7.6 Verifiche periodiche e report dell'OdV

Al fine di garantire l'aggiornamento e l'efficienza del presente Modello, l'Organismo di Vigilanza procederà ad effettuare due tipi di verifiche:

- Verifiche sugli atti: verifica annuale dei principali atti societari e dei contratti di maggior rilevanza conclusi dalla società in aree di attività di rischio al fine di verificare la rispondenza delle attività ad essi attinenti alle norme procedurali e comportamentali stabilite dal Modello;

- Verifica del Modello: verifica periodica del funzionamento del Modello e dell'effettivo rispetto delle procedure di comportamento stabilite internamente dalla società per la prevenzione dei reati nelle aree di attività esposte alla commissione dei reati.

A valle di queste verifiche sarà redatto dall'OdV apposito *report* che evidenzi le criticità rilevate e suggerisca le azioni da intraprendere, da sottoporre all'attenzione del Consiglio di Amministrazione, con periodicità annuale.

7.7 Sistema delle deleghe

La Società adotta un sistema di deleghe e procure – come descritto al paragrafo 4.3 che precede - affinché la strategia definita nel piano industriale e approvata dal CdA, possano essere attuate dalla struttura organizzativa. Il sistema delle deleghe e delle procure riflette la gerarchia dei ruoli.

L'Organismo di Vigilanza potrà indicare le eventuali modifiche da apportare a detta *policy*/strategia al fine di adeguarla ai dettami del Decreto.

Le indicazioni fornite dall'Organismo di Vigilanza saranno valutate dal CdA che adotterà in autonomia le opportune determinazioni.

7.8 Conservazione delle informazioni

Ogni informazione, segnalazione, report previsti nel Modello sono conservati dall'Organismo di Vigilanza in un apposito *database* informatico e/o cartaceo. I dati e le informazioni conservate nel *database* sono poste a disposizione di soggetti esterni all'Organismo di Vigilanza previa autorizzazione dell'Organismo di Vigilanza stesso. Quest'ultimo definisce per iscritto criteri e condizioni di accesso al data base.

8 DIFFUSIONE ED ATTUAZIONE DEL MODELLO

8.1 Piano di comunicazione

8.1.1 Comunicazione ai componenti degli organi sociali

Il Modello è portato a conoscenza a cura della Segreteria societaria di ciascun componente degli organi sociali che - per sopravvenuta nomina o per assenza - non abbia già concorso all'approvazione del Modello.

8.1.2 Comunicazione ai Dirigenti e ai Responsabili di Funzione

I principi e i contenuti del Modello sono comunicati formalmente, su disposizione dell'Organismo di Vigilanza, dalla Direzione a tutti i dirigenti (a ruolo e in servizio) e ai Responsabili di Funzione, mediante consegna del presente documento e/o diffusione in intranet aziendale.

8.1.3 Comunicazione a tutti gli altri dipendenti

Il presente documento è inviato/reso disponibile in forma elettronica a tutti i dipendenti ed è fruibile per consultazione sul sito all'indirizzo www.nttdata.com/it (disponibile anche per i terzi), nonché sulla intranet aziendale.

Al fine di sollecitare la diffusione della conoscenza del Modello presso tutti i Dipendenti, nell'ambito delle Funzioni di staff, i Responsabili di Unità e le funzioni direttive hanno il compito di segnalare e sottolineare l'importanza dei valori, delle regole e degli strumenti che compongono il Modello stesso.

8.1.4 Formazione del personale

La formazione del personale ai fini dell'attuazione del Modello è gestita dal Responsabile delle Risorse Umane/Human Resources in stretta collaborazione con la funzione *Legal & Compliance* e con l'Organismo di Vigilanza. I principi e i contenuti del Modello 231 sono divulgati anche mediante corsi di formazione cui i soggetti sopra individuati sono tenuti a partecipare. La struttura dei corsi di formazione è definita dal Responsabile delle Risorse Umane/*Human Resources*, con la funzione *Legal & Compliance* e con la consulenza dell'Organismo di Vigilanza.

Sono utilizzati anche i seguenti strumenti formativi:

- Periodica nota informativa interna;
- Una informativa nelle lettere/documenti in fase di assunzione per i neoassunti (esempio tipo strumento "*Welcome Kit/Your Guidebook*" o similare);
- Accesso a Intranet;
- Lettera circolare anche a mezzo posta/posta elettronica.

8.2 Comunicazione a terzi

Potranno essere fornite apposite Informative a soggetti esterni a NTT DATA Italia (per esempio: Rappresentanti, Consulenti e Partner Commerciali) sulle politiche e le procedure adottate dalla società sulla base del presente Modello organizzativo, nonché i testi delle clausole contrattuali abitualmente utilizzate al riguardo.

L'impegno al rispetto dei principi di riferimento del Modello 231 da parte dei terzi aventi rapporti contrattuali con NTT DATA Italia è infatti previsto da apposita clausola del relativo contratto che forma oggetto di accettazione del terzo contraente, con risoluzione *ipso iure* in caso di inadempimento.

8.2.1 Formazione dei collaboratori esterni

I collaboratori esterni, che NTT DATA Italia potrebbe coinvolgere nello sviluppo e gestione di progetti per esigenze di *know-how* o indisponibilità di risorse interne, dovranno conoscere quanto previsto dal D.Lgs. 231/2001 e, ove tenuti, dichiarare di aver adottato il Modello 231 o, quanto meno, procedure idonee ad evitare in alcun modo il coinvolgimento di NTT DATA Italia in caso di commissione dei reati previsti dalla predetta normativa.

9 SISTEMA DISCIPLINARE

9.1 Principi generali e criteri di irrogazione delle sanzioni

I meccanismi disciplinari qui indicati costituiscono parte integrante del Modello organizzativo della Società.

In generale, l'applicazione delle sanzioni disciplinari prescinde dall'eventuale avvio e dall'esito conclusivo del procedimento penale per la commissione di uno dei reati previsti dal D.Lgs. 231/2001.

Nei singoli casi l'irrogazione delle sanzioni specifiche saranno definite e applicate in proporzione alla gravità delle mancanze valutata, nel rispetto dei princìpi generali che regolano il diritto del lavoro.

Nei singoli casi, il tipo e l'entità delle sanzioni specifiche verranno applicate in proporzione alla gravità delle mancanze e, comunque, in base ai seguenti criteri generali tra loro cumulabili:

a) elemento soggettivo della condotta (dolo o colpa, quest'ultima per imprudenza, negligenza o imperizia anche in considerazione della prevedibilità o meno dell'evento);

b) rilevanza degli obblighi violati;

c) gravità del pericolo creato;

d) recidività nel biennio;

e) entità del danno eventualmente creato alla Società dall'eventuale applicazione delle sanzioni previste dal D.Lgs. 231/2001 e successive modifiche e integrazioni;

f) livello di responsabilità gerarchica e/o tecnica;

g) presenza di circostanze aggravanti o attenuanti con particolare riguardo alle precedenti prestazioni

lavorative, ai precedenti disciplinari nell'ultimo biennio;

h) eventuale condivisione di responsabilità con altri lavoratori che abbiano concorso nel determinare la mancanza;

i) qualora con un solo atto siano state commesse più infrazioni, punite con sanzioni diverse, si applica la sanzione più grave;

j) la recidiva nel biennio comporta automaticamente l'applicazione della sanzione più grave nell'ambito della tipologia prevista;

k) principi di tempestività ed immediatezza impongono l'irrogazione della sanzione disciplinare, prescindendo dall'esito dell'eventuale giudizio penale.

SOGGETTI DESTINATARI

Il presente sistema disciplinare si articola per categoria di inquadramento dei destinatari, ex art. 2095 c.c. nonché dell'eventuale natura autonoma o parasubordinata del rapporto che intercorre tra i destinatari stessi e la Società ed è rivolto:

a) alle persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società (c.d. "*Soggetti apicali*");
b) alle persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui sopra (c.d. "*Soggetti sottoposti*"), nonché alle persone di cui al paragrafo 9.2.4 (c.d. "*Collaboratori esterni*").

In ogni caso, l'irrogazione della sanzione prevede il coinvolgimento dell'OdV che valuta la sussistenza e la gravità della violazione.

9.2 Sanzioni

9.2.1 Sanzioni verso lavoratori dipendenti (Quadri – Impiegati)

1. AMBITO DI APPLICAZIONE

Ai sensi del combinato disposto degli artt. 5 lett. b) e 7 del D.Lgs. 231/2001, ferma la preventiva contestazione e la procedura prescritta dall'art. 7 della Legge 20 maggio 1970 n. 300 (c.d. Statuto dei Lavoratori), le sanzioni previste nella presente Sezione si applicano nei confronti di quadri, impiegati alle dipendenze della Società che pongano in essere illeciti disciplinari derivanti da:

a) mancato rispetto delle procedure e prescrizioni contenute nel Modello organizzativo per grave inosservanza delle disposizioni dirette a garantire lo svolgimento dell'attività in conformità della legge e a scoprire ed eliminare tempestivamente situazioni di rischio, ai sensi del D.Lgs. 231/2001;

b) violazione grave o reiterata delle procedure interne contenute nel Modello organizzativo ponendo in essere un comportamento consistente nel tollerare significative irregolarità ovvero nell'omettere di svolgere i controlli e/o le verifiche previste nelle singole procedure, anche nel caso in cui non sia derivato un pregiudizio agli interessi della Società;

c) violazione e/o elusione del sistema di controllo interno, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione della procedura ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti, incluso l'Organismo di Controllo;

d) inosservanza grave o reiterata delle regole contenute nel Codice Etico;

e) inosservanza reiterata dell'obbligo di informativa all'Organismo di Controllo e/o al diretto superiore gerarchico sul mancato rispetto delle procedure e prescrizioni del Modello organizzativo;

f) comportamenti diretti alla commissione di un reato previsto dal D.Lgs. 231/2001 e successive modifiche ed integrazioni.

2. SANZIONI

Il mancato rispetto delle procedure e prescrizioni contenute nella presente Sezione del Sistema Disciplinare, paragrafo 1 lettere da a) ad f) da parte dei quadri, impiegati, a seconda della gravità della infrazione, è sanzionato con i seguenti provvedimenti disciplinari indicati in via graduata e nel pieno rispetto dei Contratti Collettivi Lavoro applicabili:

a) rimprovero verbale;

b) rimprovero scritto;

c) multa non superiore all'importo di tre ore di retribuzione;

d) sospensione dal servizio;

e) licenziamento con preavviso;

f) licenziamento senza preavviso.

Ove i dipendenti sopra indicati siano muniti di procura con potere di rappresentare all'esterno la Società, l'irrogazione della sanzione più grave della multa comporterà anche la revoca automatica della procura stessa.

2.A) Rimprovero verbale

Verrà irrogata la sanzione del rimprovero verbale nei casi di violazione colposa e lieve delle procedure e/o prescrizioni contenute nel Modello organizzativo nonché delle regole contenute nel Codice Etico che non abbiano conseguenze per la Società.

2.B) Rimprovero scritto

Verrà irrogata la sanzione del rimprovero scritto nelle ipotesi di:

a) recidiva nel biennio nei casi di violazione colposa di procedure e/o prescrizioni contenute nel Modello organizzativo, nonché delle regole contenute nel Codice Etico;

b) errori procedurali di lieve entità dovuti a negligenza del lavoratore aventi rilevanza esterna.

2.C) MULTA

Oltre che nei casi di recidiva nella commissione di infrazioni di cui alla lett. b) del punto 2 b) che precede, la sanzione della multa potrà essere applicata nei casi in cui, per il livello di responsabilità gerarchico o tecnico, o in presenza di circostanze aggravanti, il comportamento colposo e/o negligente possa minare, sia pure a

livello potenziale, l'efficacia del Modello organizzativo; quali a titolo esemplificativo ma non esaustivo:

a) l'inosservanza dell'obbligo di informativa all'Organismo di Controllo e/o al diretto superiore gerarchico o funzionale sul mancato rispetto delle procedure e prescrizioni del Modello organizzativo;

b) l'inosservanza degli adempimenti previsti dalle procedure e prescrizioni indicate nel Modello organizzativo, nonché delle regole contenute nel Codice Etico, nell'ipotesi in cui essi hanno riguardato o riguardano un procedimento di cui una delle parti necessarie è la Pubblica Amministrazione.

2.D) SOSPENSIONE DAL SERVIZIO

Verrà irrogata la sanzione della sospensione dal servizio, oltre che nei casi di recidiva nella commissione di infrazioni da cui possa derivare l'applicazione della multa, nei casi di gravi violazioni di procedure e prescrizioni contenute nel Modello organizzativo nonché delle regole contenute nel Codice Etico tali da esporre la Società a rischi e responsabilità *ex* D.Lgs. 231/2001.

2.E) LICENZIAMENTO CON PREAVVISO

Verrà irrogata la sanzione del licenziamento con preavviso nei casi di reiterata grave violazione delle procedure e prescrizioni contenute nel Modello organizzativo e delle regole del Codice Etico aventi rilevanza esterna nello svolgimento di attività nelle aree/attività a rischio di reato *ex* D.Lgs. 231/2001 e successive modifiche ed integrazioni.

2.F) LICENZIAMENTO SENZA PREAVVISO

Verrà irrogata la sanzione del licenziamento senza preavviso per mancanze così gravi da non consentire la prosecuzione neppure in via provvisoria del rapporto di lavoro (c.d. giusta causa) quali a titolo esemplificativo, ma non esaustivo:

a) adozione di un comportamento diretto alla commissione di un reato ricompreso fra quelli previsti nel D.Lgs. 231/2001 e successive modifiche ed integrazioni;

b) violazione e/o elusione fraudolenta di procedure e prescrizioni contenute nel Modello organizzativo e delle regole del Codice Etico aventi rilevanza esterna al fine di commettere o agevolare reati *ex* D.Lgs. 231/2001 e tali da far venir meno il rapporto fiduciario con il datore di lavoro;

c) violazione e/o elusione del sistema di controllo interno, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione della procedura ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti, incluso l'Organismo di controllo al fine di commettere, concorrere o agevolare reati *ex* D.Lgs. 231/2001. Qualora il lavoratore sia incorso in una delle mancanze di cui al presente articolo la Società potrà disporre la sospensione cautelare con effetto immediato.

La Direzione Personale/*HR* comunica l'irrogazione della sanzione all'Organismo di Vigilanza. Il sistema disciplinare viene costantemente monitorato dall'OdV e dalla Funzione Risorse Umane/*HR*.

Sono rispettati tutti gli adempimenti di legge e di contratto relativi all'irrogazione della sanzione disciplinare.

9.2.2 Misure verso i Dirigenti

1. AMBITO DI APPLICAZIONE

Ai sensi del combinato disposto degli artt. 5 lett. b) e 7 del D.Lgs. 231/2001 e, limitatamente a tali norme, nel

rispetto della procedura prevista dall'art. 7 della Legge 20 maggio 1970 n. 300, le sanzioni indicate nella presente Sezione si applicano nei confronti dei dirigenti che pongano in essere illeciti disciplinari derivanti da:

a) violazione delle procedure interne contenute nel Modello organizzativo ponendo in essere un comportamento consistente nel tollerare irregolarità di servizi ovvero nel non osservare doveri od obblighi di servizio anche nel caso in cui non sia derivato un pregiudizio al servizio o agli interessi della Società;

b) grave mancato rispetto delle procedure e prescrizioni contenute nel Modello organizzativo tali da comportare situazioni di rischio, ai sensi del D.Lgs. 231/2001;

c) violazione e/o elusione del sistema di controllo interno, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione della procedura ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti, incluso l'Organismo di controllo, al fine di commettere, concorrere o agevolare reati *ex* D.Lgs. 231/2001;

d) inosservanza grave delle regole contenute nel Codice Etico;

e) reiterata inosservanza dell'obbligo di informativa all'Organismo di controllo e/o al diretto superiore gerarchico sul mancato rispetto delle procedure e prescrizioni del Modello organizzativo;

f) grave o reiterata omessa vigilanza in qualità di "responsabile gerarchico" sul rispetto delle procedure e prescrizioni del Modello organizzativo da parte dei propri sottoposti al fine di verificare le loro azioni nell'ambito delle aree a rischio reato e, comunque, nello svolgimento di attività strumentali a processi operativi a rischio reato;

2. SANZIONI

In caso di mancato rispetto delle procedure e prescrizioni contenute nella presente Sezione del Sistema Disciplinare paragrafo 1 lettere da a) ad h), a seconda della gravità della infrazione, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti applicabile. In particolare:

- in caso di violazione non grave di una o più regole procedurali o comportamentali previste nel Modello, il dirigente incorre nel richiamo scritto all'osservanza del Modello, la quale costituisce condizione necessaria per il mantenimento del rapporto fiduciario con la Società;
- in caso di grave o reiterata violazione di una o più prescrizioni del Modello tale da configurare un notevole inadempimento, il dirigente incorre nel provvedimento del licenziamento con preavviso;
- laddove la violazione di una o più prescrizioni del Modello sia di gravità tale da ledere irreparabilmente il rapporto di fiducia, non consentendo la prosecuzione anche provvisoria del rapporto di lavoro, il lavoratore incorre nel provvedimento del licenziamento senza preavviso.

Ove il dirigente sia munito di procura con potere di rappresentare all'esterno la Società, l'irrogazione della sanzione disciplinare comporterà anche la revoca automatica della procura stessa.

9.2.3 Misure nei confronti dei "Soggetti apicali" e dei Sindaci

1. AMBITO DI APPLICAZIONE

Ai fini del D.Lgs. 231/2001, nell'attuale organizzazione della Società sono "*Soggetti apicali*":

- il Consigliere Delegato;
- gli Amministratori muniti della legale rappresentanza;
- gli altri Amministratori;
- i Direttori Generali, ove nominati.

Ai sensi del combinato disposto degli artt. 5 lett. a) e 6 del D.Lgs. 231/2001, le sanzioni previste nella presente Sezione si applicano nei confronti dei "*Soggetti apicali*" nei seguenti casi:

a) grave o reiterato mancato rispetto degli specifici protocolli (procedure e prescrizioni) previsti nel Modello organizzativo ai sensi del D.Lgs. 231/2001, diretti a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire, e delle regole contenute nel Codice Etico, inclusa la violazione delle disposizioni relative ai poteri di firma e, in generale, al sistema delle deleghe nonché la violazione delle misure relative alla gestione delle risorse finanziarie;

b) violazione e/o elusione del sistema di controllo interno previsto nel Codice Etico e nel Modello organizzativo, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione prevista dai protocolli (procedure e prescrizioni) ovvero impedendo il controllo o l'accesso alle informazioni ed alla documentazione ai soggetti preposti, incluso l'Organismo di controllo;

c) violazione grave o reiterata degli obblighi di informativa previsti nel Modello organizzativo nei confronti dell'Organismo di controllo e/o dell'eventuale soggetto sovraordinato; inadempimento, nell'esercizio dei poteri gerarchici e nei limiti derivanti dal sistema delle deleghe, degli obblighi di controllo e vigilanza sul comportamento dei diretti sottoposti, intendendosi tali solo coloro che, alle dirette ed immediate dipendenze del soggetto apicale, operano nell'ambito delle aree a rischio di reato.

2. MISURE DI TUTELA

A seconda della gravità dell'infrazione commessa dall'Amministratore, il Consiglio di Amministrazione, sentito il parere del Collegio Sindacale, assumerà i più opportuni provvedimenti, ivi inclusi l'avocazione a sé di operazioni rientranti nelle deleghe, la modifica o la revoca delle deleghe stesse e la convocazione dell'Assemblea per l'eventuale adozione, nei casi più gravi, dei provvedimenti di cui agli artt. 2383 e 2393 cod. civ.

Ove la violazione denunciata risulti commessa da due o più membri del Consiglio di Amministrazione, il Collegio Sindacale, ove ritenga fondata la denuncia ricevuta dall'Organismo di Controllo e il Consiglio di Amministrazione non vi abbia provveduto, convoca l'Assemblea ai sensi dell'art. 2406 cod. civ. che, una volta accertata la sussistenza della violazione, adotta i provvedimenti più opportuni tra cui, nei casi più gravi, quelli di cui agli artt. 2383 e 2393 cod. civ.

3. COESISTENZA DI PIÙ RAPPORTI IN CAPO AL MEDESIMO SOGGETTO

Nell'ipotesi in cui il soggetto apicale rivesta, altresì, la qualifica di dirigente, in caso di violazioni poste in essere in qualità di apicale, a questo verranno applicate le sanzioni della presente Sezione, fatta salva, comunque, l'applicabilità delle diverse azioni disciplinari esercitabili in base al rapporto di lavoro subordinato intercorrente con la Società e nel rispetto delle procedure di legge, in quanto applicabili.

4. MISURE NEI CONFRONTI DEI SINDACI

Nel caso di violazione da parte di uno o più Sindaci, l'OdV informa il Consiglio di Amministrazione e il Collegio Sindacale, affinché procedano senza indugio e conformemente ai poteri previsti dalla legge e/o dallo Statuto, a convocare l'Assemblea degli azionisti perché proceda alle deliberazioni del caso, che potranno anche consistere nella revoca dell'incarico per giusta causa.

9.2.4 Collaboratori esterni

1. AMBITO DI APPLICAZIONE

Nei confronti di coloro che, in qualità di collaboratori, consulenti e fornitori di NTT DATA Italia, soggetti dunque destinatari degli obblighi di cui al D.Lgs. 231/2001, abbiano posto in essere le gravi violazioni delle regole del Codice Etico e delle procedure e prescrizioni contenute nel Modello organizzativo, di seguito indicate, potrà essere disposta la risoluzione di diritto del rapporto contrattuale ai sensi dell'art. 1456 c.c.

Resta salva, in ogni caso, l'eventuale richiesta da parte della Società del risarcimento dei danni subiti.

2. INADEMPIMENTI

a) elusione fraudolenta di procedure e prescrizioni aziendali e delle regole del Codice Etico attinenti all'oggetto dell'incarico aventi rilevanza esterna ovvero violazione delle stesse realizzata attraverso un comportamento diretto alla commissione di un reato ricompreso fra quelli previsti nel D.Lgs. 231/2001 e successive modifiche ed integrazioni;

b) mancata, incompleta o non veritiera documentazione dell'attività svolta, oggetto dell'incarico, tale da impedire la trasparenza e verificabilità della stessa.

3. CLAUSOLE CONTRATTUALI

Si riporta qui di seguito il testo della clausola da riportare - con gli opportuni adattamenti - negli Ordini a fornitori terzi, nei contratti e nei Patti Interni di costituendi Raggruppamenti Temporanei di Impresa (RTI / ATI):

"*Con specifico riferimento al D.Lgs. n. 231/2001 e s.m.i. (**"Decreto 231"**) e alle finalità di prevenzione e di repressione degli illeciti penali dolosi ivi previsti e riportati (**"Reati-Presupposto"**), il Fornitore, il Collaboratore e/o il terzo affidatario, con rapporti d'affari con NTT DATA Italia ai sensi del presente Contratto (il **"Contraente"**), dichiara di avere preso atto e di impegnarsi a rispettare i princìpi cardine riflessi nel Codice di Condotta Commerciale Globale NTT DATA consultabile su website NTT DATA Italia http://emea.nttdata.com/it/chi-siamo/index.html (**"Codice Etico"**), tra cui la lotta alla corruzione e alla contraffazione di beni di proprietà intellettuale e industriale e si obbliga altresì al rispetto degli standard minimi di condotta specificati nell'Allegato "A" al Codice Etico (congiuntamente i **"Principi Cardine"**).*
Il Contraente dichiara altresì di avere preso visione del Modello Organizzativo (Parte Generale) di NTT DATA Italia, consultabile sul website e/o sul Portale Fornitori.
*In ragione di quanto sopra, il Contraente è consapevole che (a) l'omessa o parziale inosservanza dei Principi Cardine del Codice Etico e/o (b) il rinvio a giudizio per uno dei Reati-Presupposto di cui al Decreto 231 (ove siano sanzionabili per dolo) costituiranno fattispecie di grave inadempimento contrattuale e legittimeranno NTT DATA Italia a **risolvere ipso jure** il presente Contratto ai sensi e per gli effetti dell'art. 1456 cod. civ., nei termini temporali riportati nella presente clausola, fermo restando il risarcimento dei danni eventualmente*

causati alla Società stessa".

9.2.5 Misure a tutela delle segnalazioni (*Whistleblowing*)

•

Il Decreto *Whistleblowing* prevede che sia istituito un sistema sanzionatorio nei confronti dei soggetti che si rendano responsabili degli illeciti di seguito indicati.

1 Segnalazioni dolosamente o colposamente infondate

Salvo quanto previsto dal Decreto *Whistleblowing*, se all'esito dell'analisi della segnalazione dovesse emergere che la stessa è infondata e viene accertato che la persona segnalante ha effettuato la segnalazione con dolo o colpa grave, saranno applicate le sanzioni previste dal Modello.

Le sanzioni disciplinari dovranno essere irrogate nei confronti del segnalante, tenuto conto, in via esemplificativa:

- della gravità dell'elemento soggettivo, e cioè della sussistenza di un atteggiamento doloso o gravemente colposo di chi abbia fatto la segnalazione rivelatasi infondata;
- della gravità dei fatti falsamente segnalati;
- dell'utilizzo di mezzi fraudolenti (ad es. la falsificazione di prove).

Resta ferma, in ogni caso, ogni valutazione circa l'opportunità di presentare atti di denuncia o querela nel caso di atti o fatti aventi rilevanza penale.

2 Violazione della riservatezza del segnalante

Ogni violazione della riservatezza del segnalante sarà valutata ai fini dell'applicazione delle sanzioni previste dal Modello.

In tal caso, si terrà conto in via meramente esemplificativa e non esaustiva:

- del fatto che la rivelazione sia avvenuta intenzionalmente o per errore;
- delle modalità della rivelazione e della sua diffusione;
- del fatto che la rivelazione abbia esposto a rischi il *whistleblower*.

3 Altri illeciti

Nel caso in cui sia stato rilevato uno dei seguenti illeciti, saranno applicate le sanzioni previste dal Modello:

- è stata commessa una ritorsione nei confronti della persona segnalante;
- la segnalazione è stata ostacolata o si è tentato di ostacolarla.