Trusted Global Innovator

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 10 dicembre 2018

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

Parte Generale

SOMMARIO

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 organizzativo, di 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 10 dicembre 2018, che segue quelle approvate alle date del 20 settembre 2011, del 29 luglio 2014 e del 30 novembre 2016.

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 organizzativi, di 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 231/01, 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 231/01.

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 ai successivi aggiornamenti).

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 il proprio governo interno 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:

individuazione ed Analisi dei Rischi e dei Protocolli

individuazione delle Componenti necessarie al Sistema

regolamentazione e nomina dell'Organismo di Vigilanza

definizione del Codice Etico dell'Azienda

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. 231/01, 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.

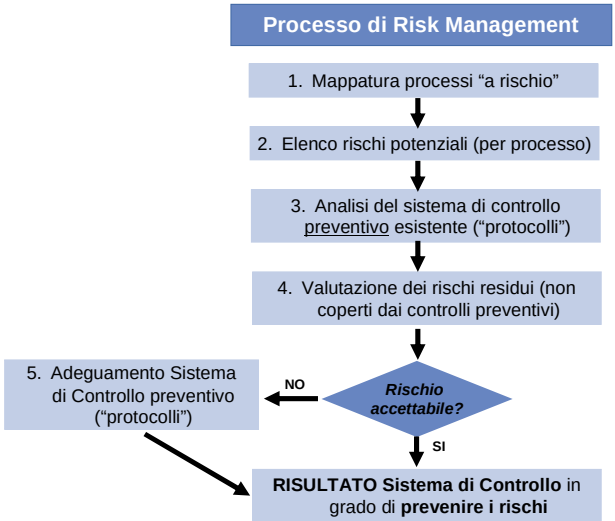
Come previsto dall'art. 6, co. 2, del D.Lgs. 231/2001, la realizzazione del sistema di gestione dei rischi (*risk management*) di NTT DATA Italia si articola in due fasi:

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 *una tantum*, 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 più 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

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

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

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

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 i 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. 231/01)

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. 231/01*)

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. 231/01)

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*)

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*)

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 contro la personalità individuale (art. 25-quinquies)

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.

2.3.11 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 **website di NTT DATA Italia** e sulla **intranet aziendale,** ed è diffuso in lingua italiana/inglese (sono eventualmente disponibili edizioni anche in altre lingue).

3.2 Policy e procedure

Sono state elaborate e diffuse policy e procedure 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 policy 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 da 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 Governane 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 Rewiew, 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:

- Un soggetto iscritto nel Registro dei Revisori legali istituito presso il Ministero dell'economia e delle finanze o avente 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.
- Il Responsabile della Funzione Legale.
- Un soggetto con esperienza nel settore nel quale la Società svolge la propria gestione caratteristica e/o con esperienza nelle attività maggiormente esposte al rischio di reato-presupposto ex lege n. 231/2001.

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 durata triennale. Alla scadenza del triennio, l'OdV continua a svolgere in 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.

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. 109 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 Decreto Legislativo n. 58/1998.

I candidati alla carica di membri dell'Organismo di Vigilanza devono autocertificare con dichiarazione sostitutiva di notorietà ex lege 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. 231/2001di "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, dalla 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.

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 disegnato dal 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.

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*".
- "*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) 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).

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.

La legge 30 novembre 2017, n. 179 (entrata in vigore il 29 dicembre 2017) in materia di "*whistleblowing*", ha introdotto il nuovo comma 2-bis dell'art. 6 del DLgs. 231/2001, ai sensi del quale i modelli di organizzazione adottati devono prevedere l'attivazione di uno o più canali che consentano di presentare, a tutela dell'integrità dell'ente stesso, segnalazioni circostanziate di condotte illecite, rilevanti rispetto ai reati ivi previsti e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione, di cui siano venuti a conoscenza in ragione delle funzioni svolte. Tali canali devono garantire la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione e almeno uno deve essere idoneo a garantire la riservatezza con modalità informatiche.

A tale proposito:

- Sono raccolte eventuali segnalazioni, relative alla commissione di reati previsti dal Decreto in relazione all'attività societaria o comunque a comportamenti non in linea con le regole di condotta adottate dalla società con segnalazioni specifiche all'Organismo di Vigilanza, anche via e-mail all'indirizzo **OdV@nttdata.com**. Esistono anche altri canali messi a disposizione dall'azienda per inviare le eventuali segnalazioni di *whistleblowing* (per esempio indirizzo email esterno all'azienda, amministrato da un Operatore specializzato terzo).
- Ogni dipendente è tenuto a sollevare dubbi circa la violazione di normative interne di NTT DATA Italia o di legge. Le questioni "dubbie" possono essere risolte, a livello locale, chiedendo al diretto superiore gerarchico e alla persona preposta alla verifica delle conformità con competenza suddivisa per business, Paese e lingua. Una volta sollevata la questione, la Società identifica le funzioni coinvolte e tenute a esaminare il rilievo, effettuare le necessarie indagini ed adottare i necessari provvedimenti.
- Le segnalazioni pervenute all'Organismo di Vigilanza saranno da questi valutate e gli eventuali provvedimenti conseguenti saranno proposti al Responsabile delle Risorse Umane/Human Resources e al diretto superiore dell'autore della violazione.
- Le segnalazioni, in linea con il Codice Etico, potranno essere sia in forma scritta sia verbale ed avere ad oggetto ogni violazione o sospetto di violazione del Modello. L'Organismo di Vigilanza agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione assicurando la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della società o delle

persone accusate erroneamente e/o in mala fede.

- L'Organismo di Vigilanza valuterà le segnalazioni ricevute e gli eventuali provvedimenti conseguenti a sua discrezione e responsabilità ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad un'indagine interna.
- L'OdV valuterà in piena ed insindacabile discrezionalità se da dare o meno seguito a segnalazioni anonime o non sufficientemente circostanziate.

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 data base informatico e/o cartaceo. I dati e le informazioni conservate nel data base 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 jure* 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 Decreto 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. 231/2001e 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 (cd. "*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, lettera 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 lege 231/01.

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. 231/2001e 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 (cd. 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 lege 231/01 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 lege 231/01 ed in modo da impedire 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 Dirigenti

1. AMBITO DI APPLICAZIONE

Ai sensi del combinato disposto degli artt. 5, lettera 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 lege 231;

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, lettera 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 l'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)

È causa di contestazione e successiva eventuale sanzione disciplinare nei confronti di dipendenti, amministratori e di terzi:

- la violazione della riservatezza sull'identità delle persone che abbiano segnalato secondo la Legge 30/11/2017 n° 179, reati di cui siano venuti a conoscenza per ragioni di lavoro.

- Effettuare false segnalazioni fatte avvalendosi illegittimamente delle facoltà definite dalla Legge 30/11/2017 n° 179 per ottenere vantaggi personali o di soggetti collegati o per danneggiare altre persone.

- Causare illegittimo pregiudizio alle persone che siano eventualmente oggetto delle segnalazioni pervenute ai sensi della Legge 179/2017.

ENGLISH VERSION

ORGANIZATION, MANAGEMENT, AND CONTROL MODEL OF NTT DATA Italia

Under Legislative Decree 231/2001

General Section

Approved by the Board of Directors on 10 December 2018

ORGANIZATION, MANAGEMENT AND CONTROL MODEL OF NTT DATA ITALIA SPA under Legislative Decree 231/2001

General Section

SUMMARY

DEFINITIONS

Risk areas	The areas of company activity in which, in more concrete terms, the risk of committing the Offences specified in Legislative Decree no. 231/2001 is present
NATIONAL COLLECTIVE NEGOTIATION AGREEMENT	National collective labour agreement applicable to employees of NTT Data Italia S.p.A.
CCNL Executives	National collective labour agreement for managers of companies producing goods and services, currently in force and applied by NTT Data Italia S.p.A.
Global Code of Business Conduct or Code of Ethics or Code of Conduct	Code approved by NTT DATA EMEA, modified and adopted by the Board of Directors of NTT DATA Italia including the set of rights, duties and responsibilities that NTT DATA Italia S.p.A. expressly assumes towards its counterparts in the performance of its activities and available on the Company's website and intranet portal.
Collaborators	Those who act in the name and/or on behalf of NTT DATA Italia S.p.A. on the basis of a specific mandate or other contractual obligation
Decree	Legislative Decree no. 231 of 8 June 2001 and subsequent amendments and additions
Recipients	Members of the corporate bodies and internal corporate *governance* bodies, employees, collaborators in any capacity, including occasional ones, and all those who have commercial and/or financial relationships of any nature with NTT Data Italia S.p.A., or who act on its behalf on the basis of specific mandates (for example: consultants, suppliers, partners)
Employees	All employees of NTT DATA Italia S.p.A. (including executives)
Relatives	Relatives and in-laws in a straight line up to the second degree (children, parents, grandchildren - such as children of the children - and grandparents, parents in-law and sons-in-law, daughters-in-law, brothers or sisters of the spouse), relatives and in-laws in a collateral line up to the third degree and also cousins (brothers and sisters, grandchild and uncle, as well as cousins); spouse and/or cohabiting partner
Departments	First level organisational structures of NTT DATA Italia S.p.A.
Counterparts	With the exclusion of collaborators, all contractual counterparts of NTT DATA Italia S.p.A., natural or legal persons, such as suppliers, customers and, in general, all persons to or from whom NTT DATA Italia S.p.A. provides or receives any contractual service.
Guidelines	The Guidelines for the construction of models of organisation, management and control according to Legislative Decree 231/2001, approved by Confindustria and subsequent amendments and additions.
Model 231	Organisation, Management and Control Model under Legislative Decree 231/2001
Model or Organisational model or MOG	Organisation, Management and Control Model under Legislative Decree no. 231/2001 adopted by NTT DATA Italia S.p.A.

NTT DATA Corp.	NTT DATA Corporation
NTT DATE EMEA	NTT DATA EMEA Ltd.
NTT DATA Group or NTT DATA Group	NTT DATA Corp. and its subsidiaries
NTT DATA Italia or Company	NTT DATA Italia S.p.A.
Corporate Bodies	The Board of Directors and the Board of Statutory Auditors of NTT DATA Italia S.p.A.
Supervisory Board or Board	Supervisory Board under art. 6, paragraph 1, letter b) of Legislative Decree 231/2001
Public administration	Any Public Administration, including its representatives in their capacity as public officials or persons in charge of a public service, also de facto
Offences or Offence or Offences 231	Relevant offences under Legislative Decree 231/2001
Management hierarchy	The Chairman and Chief Executive Officer of NTT DATA Italia S.p.A.

10 INTRODUCTION

10.1 Adoption of the model under Legislative Decree no. 231/2001 by NTT DATA Italia S.p.A.

Legislative Decree no. 231 of 8 June 2001 (*Rules governing the administrative liability of legal persons, companies and associations, including those without legal personality, in accordance with art. 11 of Law no. 300 of 29 September 2000*) introduced into the Italian legal system - as is now known - a particular system of administrative liability for companies, which applies when the offences listed in the Decree are committed, in the context of the activities carried out by companies.

On January 28, 2006, the Board of Directors of NTT DATA Italia S.p.A. approved the first version of the Organisational, Management and Control Model under Legislative Decree 231/2001 in the knowledge that the implementation of the Model, while representing a choice and not an obligation, allows the Company to have a set of rules, tools and activities suitable to prevent the commission of the offences referred to in the Decree, to hold the Company harmless from the liability stipulated in it in the event that one of the above-mentioned offences is committed, as well as to strengthen its culture of *governance* and raise employee awareness on issues of control of business processes, to stimulate an "active" prevention of the Offences and - more generally - of any illegal conduct within the Company.Following the regulatory changes that have affected the Decree since that date, as well as the development of case law regarding the issue of the companies' administrative liability, over time the Board of Directors of NTT DATA Italia has approved numerous updates and amendments to the Model, also harmonizing and updating the Code of Ethics approved by NTT DATA EMEA and adopted by the Company.

This document therefore reflects the Model in the version most recently approved by the Company's Board of Directors on 10 December 2018, which follows those approved on 20 September 2011, 29 July 2014 and 30 November 2016.

10.2 NTT DATA Italia S.p.A.

Since 2011 NTT DATA Italia is part of the NTT DATA Corp. Group, based in Tokyo, an international player that provides innovative and quality IT services, products and solutions for customers worldwide, operating in various and different sectors of activity (telecommunications, banking and financial services, insurance, P.A., industry and distribution, utilities, publishing and mass media).

NTT DATA Italia is subject to the direction and coordination of NTT DATA EMEA Ltd based in London.

10.3 The NTT DATA Italia Model

The Model adopted by the Company is an act issued by the *"executive body"* under art. 6, par. 1, letter a) of Legislative Decree 231/2001, a body that within NTT DATA Italia can be identified with the Board of Directors, which is therefore responsible for any subsequent amendments and additions to the MOG. The Chief Executive Officer of the Company has the right to make changes and additions to the text of the Model that are only of a formal nature.

The basic principles described in the General Part of the Model apply to NTT DATA Italia and are shared by the subsidiaries; they must be complied with in all company activities carried out both in Italy and abroad. The organisational, management and control models of the subsidiaries are in fact inspired by the same values and general principles described below.

The adoption of the Model is not only necessary to make the Company fully compliant with Decree 231/01, but is also essential to raise awareness among all those who work for the Company to a transparent behaviour, dictated by full compliance with the law, as already highlighted in the introduction above. The purpose is to build and maintain a structured and organic system of procedures and control activities, aimed at preventing the commission of the various types of offences covered by Decree 231/01.

This document is addressed to all those who work for the achievement of the purpose and objectives of NTT DATA Italia, in particular, as specified in the previous "Definitions": the members of the Company's corporate bodies and governance bodies, employees, external consultants, suppliers, customers and, in general, all third parties with whom NTT DATA Italia has relationships regarding its corporate activities. In this context, the Model was drawn up in compliance not only with the dictates of the Decree, but also with the guidelines developed by trade associations, in particular the indications of Confindustria with the document *"Guidelines for the establishment of organisation, management and control models"* issued on 7 March 2002 (and the subsequent updates).

This document has been prepared with the aim of supporting the understanding of the Company's organisational, management and control system through a reference context that also highlights where the most up-to-date information on the choices and instruments in place can be found. For this reason, it often contains references to other company documents.

As a subsidiary of the parent company NTT DATA Corp., NTT DATA Italia is required to implement the J-SOX regulation (Japan's Financial Instruments and Exchange Law), which requires all companies listed on the Japanese stock exchange and its subsidiaries to strengthen their internal governance in order to ensure accurate and complete disclosure of financial information. Within the NTT DATA Group, specific internal auditing activities are therefore carried out in accordance with the above-mentioned regulations.

10.4 General principles of the Model

The Model adopted by NTT DATA Italia is based on the following general principles:

a) **Knowledge of the risks through** the mapping of the Company's "sensitive processes" and the evaluation of the level of risk, also in light of the reasons set out in the Position Paper issued by the Italian Association of Internal Auditors.

b) **Definition of values and rules of conduct,** collected in the Code of Conduct and in company procedures, manuals and information technology, with particular attention to those regarding the financial management.

c) **Clear assignment of roles and powers,** through an organisational structure, a system of simple and transparent powers and delegations, with the indication, when required, of the thresholds for approval of expenses.

d) **Sharing of governance and management rules,** as described in the statutes of the corporate bodies, aimed at ensuring an adequate level of collegiality in the decision-making process.

(e) **Implementation of an effective internal control system,** based on the following rules

- Each operation, transaction and action must be: verifiable, consistent and appropriate, and adequately supported at document level so that checks can be carried out at any time to certify the characteristics and reasons for the operation and identify who authorised, recorded and verified the operation.
- No one should be able to manage an entire process autonomously, i.e. the principle of the separation of functions and powers must be complied with.
- Authorisation powers must be assigned in a manner consistent with the assigned responsibilities.
- The control system must document the performance of the controls, including supervision.

f) **Surveillance activities on the effectiveness** of the control system and, more generally, on the entire Organisation, management and control model:

- The assignment of the task of promoting the effective and correct implementation of the Model to an internal Supervisory Board within the Company, also through the monitoring of company behaviour and the right to constant information on activities relevant for the purposes of Legislative Decree 231/2001.
- The provision of adequate resources to the Board so that it is supported in the tasks entrusted to it to achieve the results reasonably achievable.
- The activity of verifying the functioning of the Model with consequent periodic updating (ex post control).
- Awareness raising and dissemination of the established rules of conduct and procedures at all company levels.

i) **Transparent and widespread communication of values**, principles and rules, accompanied, where necessary, by specific training activities on the instruments that make up the Model and that the Company implements to prevent all unlawful conduct:

j) **Application of disciplinary mechanisms and sanctions** for conduct not in line with the application of the Model by NTT DATA Italia.

This Model is also consistent with the key principles indicated by the NTT DATA Corp parent company, but it also contains specific features inherent in the organisational structures and business activities of NTT DATA Italia, with further specific measures related to the specific nature of its business and with close coordination with the procedures and protocols of the Quality Management System and with the relevant ISO 9001 Certification which the Company holds.

11 RISK MAPPING

11.1 Introduction

The Company's organisational model is implemented taking into account its effective compatibility with the current company organisation, so as to integrate it efficiently with the business operations and, if necessary, undergo the necessary changes in a flexible manner.

For this reason, the Supervisory Board, which will be discussed in detail below, has the powers necessary for the purposes of monitoring and verifying the Model.

As suggested by the Confindustria Guidelines, the creation and implementation of a Risk Management System includes the following elements and steps:

identification and analysis of risks and protocols

identification of the components necessary for the system

regulation and appointment of the Supervisory Board

definition of the Company's Code of Ethics

definition of the specific sanctions system.

11.2 Risk identification and protocols

For the purposes of preparing the Model, first of all, over time NTT DATA Italia has identified and updated the conduct at risk with respect to the company functions and the offences stipulated by Legislative Decree. 231/01, connected to them. Following this analysis and study phase, the Model aims:

1) To make all those who work in the name and on behalf of NTT DATA Italia in the areas of activity at risk aware that, in the event of violation of the provisions contained in it, they may commit an offence punishable by criminal and administrative sanctions, not only against themselves, but also against the company.

2) Reiterate that these forms of unlawful conduct are strongly condemned by the Company because (even if the Company were in a position to take advantage of them) they are in any case contrary to the provisions of the law in force and to the principles affirmed by the Company policies and by the Code of Conduct and that the Company undertakes in the most determined way to prevent such conduct.

4) By means of monitoring the activities at risk, to allow the Company to intervene promptly to prevent and counteract, as far as possible, the commission of the offences themselves, namely:

g. identifying the activities in which offences may be committed, thus periodically mapping and updating the company areas in which the activities most at risk are carried out;
h. providing specific protocols aimed at planning the formation and implementation of the Company's decisions in relation to the Offences to be prevented;
i. identifying methods for managing financial resources that are suitable for preventing the commission of the

Offences;

j. Stipulating the obligations to provide information to the body responsible for supervising the operation of and compliance with the models;

k. introducing information and awareness systems at all company levels regarding the established rules of conduct and procedures and an effective disciplinary system capable of sanctioning non-compliance with the measures indicated herein;

l. in relation to the nature and size of the organisation, as well as the type of activity carried out, stipulating appropriate measures to ensure that the activity is carried out in compliance with the law and to promptly detect and eliminate situations of risk.

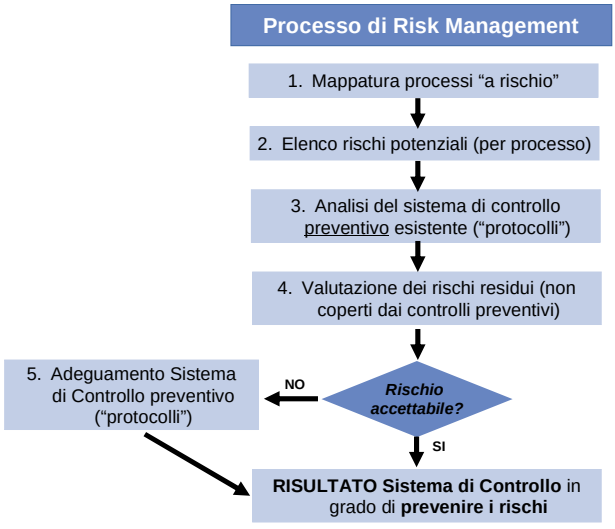
As stipulated in Article 6(1)(b) and (c) of Regulation (EC) No 880/2004, the Commission shall, in accordance with the procedure stipulated in Article 6(2), adopt the measures necessary to comply with the provisions of Regulation (EC) No 880/2004. 2, of Legislative Decree 231/2001, the implementation of the *risk management* system of NTT DATA Italia is divided into two phases:

c) the identification of risks through the analysis of the company context to highlight where (in which area/sector of activity) and according to which methods hypothetical offences may occur;

d) evaluation of the control system, i.e. verification that the existing system within the Company is adequate to maintain the highlighted risks at an acceptable level and that any modification/improvement is planned and implemented, with the objective of reducing the minimum threshold of the acceptable level of the identified risks.

From a conceptual point of view, reducing a risk involves intervening (jointly or severally) on two determining factors:

- the probability of the event happening;
- the impact of the event itself.



The identification of company areas/types of behaviour at risk is assessed on the basis of the principle of potential occurrence both in relation to the business activity and with respect to the involved departments.

This assessment, although of a preventive nature, is the starting point for the qualitative definition of risk as "*acceptable*" by the Company, since the incidence and probability of occurrence of the specific risk have been linked.

However, in order to operate effectively, the system cannot be reduced to a *one-off* activity, but must be translated into a continuous (or periodic) process, to be repeated with particular attention in times of corporate change (for example: opening of new offices, expansion of activities, acquisitions, reorganizations, etc.).

11.2.1 The definition of *"acceptable risk"*

The conceptual threshold of risk acceptability is represented by a system of prevention that cannot be circumvented unless done so intentionally.

With regard to corporate offences, for example, the process of preparing the annual accounts, the management of *price sensitive* information and the procedures for the functioning of corporate bodies have been verified.

In addition to the objective aspect or the area of possible violation, due consideration was also given to the subjective perspective, i.e. who are the people, active or passive, involved in any violations.

In the context of this process of reviewing processes/functions at risk, it is advisable to identify the persons affected by the monitoring activity, which in certain particular and exceptional circumstances, could also include those who are linked to the company by mere relationships of para-subordination, such as for example external consultants, or other collaborative relationships, such as business partners, as well as employees and collaborators of the latter.

In the same context, it is also advisable to carry out *due diligence* whenever "indicators of suspicion" (e.g. conducting negotiations in areas with a high rate of corruption, particularly complex procedures, presence of new personnel unknown to the Company) have been identified during the risk assessment process relating to a particular commercial transaction.

The processes in the financial area are clearly important for the purposes of the application of Legislative Decree 231/2001, and it is probably for this reason that it deals with them separately (art. 6, par. 2, letter c), even though a careful analysis of the evaluation of the business areas "at risk" should, however, identify the financial one as having clear importance.

11.2.2 Analysis of potential risks

The analysis of potential risks has been linked to possible subjective behaviour that may lead to the commission of Offences for each involved company area.

The summary of this analysis is represented by a survey form (*check list* included in the special section of the Model) in which the Company's corporate functions and the specific activities of persons and corporate bodies were compared to the possible offences relevant to NTT DATA Italia.

11.2.3 Evaluation/construction/adjustment of the preventive control system

The activities described above are completed with a prior evaluation of the existing control system, in order to allow the Supervisory Board to analyse the deviations between the latter and the prevention Model, and to adapt it when necessary.

The system of preventive checks aims to ensure that the risks of commission of the Offences, as identified and

documented in the previous phase, are reduced to an "acceptable level", as defined above.

It is, in essence, a matter of implementing what Legislative Decree 231/2001 defines as *"specific protocols aimed at planning the formation and implementation of the company decisions in relation to the offences to be prevented"*, an activity that NTT DATA Italia has implemented through the adoption of instruments, control systems, procedures and company policies in line with the above-mentioned regulatory instructions.

11.3 Risk detection and mapping

NTT DATA Italia has carried out and periodically updates the analysis of company processes and operations in order to identify the areas at risk (risk mapping), meaning by the latter the areas of activity that are affected by potential offence cases under Legislative Decree no. 231/2001.

In this sense, the identified risks were identified and mapped with specific reference to the company activities actually carried out and the functions actually performed by the operators.

This analysis has shown which activities are most exposed to the commission of the offences indicated in the Decree or in any case to be monitored. These Offences and the macro-areas of activity thus identified were the following.

11.3.1 Penalties against the Public Administration

The activities considered sensitive in relation to Offences against the Public Administration are:

l) Negotiation/signing and/or performance of contracts/conventions of concessions with public entities, which are reached through negotiated procedures (direct award or private negotiation).

m) Negotiation/signing and/or performance of contracts/conventions of concessions with public entities which are reached through public procedures (open or restricted).

n) Negotiation/signing or performance of contracts with public entities that are reached through private negotiations.

o) Negotiation/signing and/or performance of contracts with public entities that are reached through open or restricted procedures.

p) Management of relations with bodies/supervisory authorities relating to the performance of activities regulated by law.

q) Management of acquisition activities or management of contributions, subsidies, financing, insurance or guarantees granted by public bodies.

r) Request for occasional/ad hoc administrative measures necessary to carry out activities instrumental to typical company activities

s) Preparation of tax returns or substitutes for tax or other declarations for the settlement of taxes in general.

t) Compliance with public bodies, such as communications, declarations, filing of deeds and documents, files, etc., different from those described in the previous points and in the sanction checks/assessments/procedures resulting from them.

u) Activities that involve the installation, maintenance, updating or management of software by public entities or provided by third parties on behalf of public entities.

v) Other *"sensitive activities"*: relations with the institutions and administrations of the State.

11.3.2 Corporate Offences

The sensitive activities in terms of corporate offenses are the following:

f) Preparation of the annual accounts and periodic interim reports.

g) Relations with shareholders, audit firm, board of statutory auditors, audits and relations with supervisory authorities.

h) Capital transactions and allocation of profit.

i) Communication, carrying out and minutes recording of Shareholders' Meetings.

j) Management of business relations and negotiations with private customers and suppliers (with reference to the offence of bribery between private individuals and incitement to corruption between private individuals).

11.3.3 Offenses against health and safety in the workplace

The activities considered sensitive in relation to health and safety offences at work, are:

d) Establishment and control of the management system of health and safety in the workplace.
e) Performance phases of procurement, works and supply contracts.
f) As a client entrusting works and/or services within its own facilities.

11.3.4 Computerized offenses

The activities and behaviour that represent the types of computer offences are:

d) Access to a computer system protected by security measures.
e) Managing codes, keywords, credentials to access computer systems protected by security measures.
f) Reproducing, disseminating, duplicating, selling or making available to third parties proprietary computer programs or other intellectual property in violation of copyright protection rules.

11.3.5 Offences relating to the violation of copyright (art. 25-*novies*, Legislative decree 231/01)

The activities that constitute offences in the field of copyright are:

e) Duplicating, importing, distributing, selling, leasing, disseminating/transmitting to the public, holding for commercial purposes, or otherwise for profit, without having the right, proprietary computer programs, protected databases or any work protected by copyright or related rights, including works with literary, musical, multimedia, cinematographic or artistic content.

f) Disseminating an intellectual work or part of it by telematic means without having the right to do so.

g) Implementing file sharing practices.

h) Sharing any file through peer-to-peer platforms.

11.3.6 Inducement to not make statements or to make false statements to the judicial authorities (*art. 25-decies, Legislative decree231/01*)

The activities that can be traced back to the Offence in question are:

b) Providing instructions to influence a person required to make statements before the Judicial Authority in order to obtain favourable treatment from the latter in relation to ongoing proceedings or investigations.

11.3.7 Employment of third party citizens whose stay is illegal (art. 25-duodecies, Legislative decree 231/01)

The activities considered sensitive in relation to the Offence in question are:

c) Selection and recruitment of personnel
d) Management of non-EU employees.

11.3.8 Receiving, laundering and using money, goods or benefits of illicit origin (art. 25-*octies*)

Although the risk of commission of the above Offences appears to be entirely theoretical and residual, taking into account the sectors of activity in which NTT DATA Italia operates, it was considered useful to dedicate, in the Special Section of the Model, a specific paragraph to this type of Offences in view of their significant social danger, indicating measures, procedures and control instruments - for the most part already present within the NTT DATA Italia structures - suitable for preventing the relative risk of commission.

11.3.9 Money laundering (Article 25-*octies*)

Article 3, paragraph 5, of Law no. 186 of 15/12/2014 ("*Provisions on the emergence and return of capital held abroad as well as for the strengthening of the fight against tax evasion.Provisions on self-laundering*") has amended Article 25 -*octies* of Legislative Decree231/2001, introducing in the category of possible offences, the offence of self laundering under Article 648-ter.1 of the Criminal Code, punishable from 1 January 2015.This offence, the sensitive company activities and the related controls, will be dealt with in a specific paragraph in the Special Section of the

Model, taking into account both the complexity involved in identifying the company areas in which it could theoretically be committed, and the lack, at present, of consolidated jurisprudential guidelines on the subject (the introduction of self-laundering in our legal system, as well as in the "catalogue" of 231 Offences, took place recently - as mentioned above).

11.3.10 Crimes against individuals (Article 25-quinquies)

On November 4, 2016, Law no. 199 of October 29, 2016 entered into force, inserting into Article 25 quinquies of Legislative Decree 231/2001 the new offence of "illicit brokering and exploitation of labour" (Article 603-bis of the Italian Criminal Code), the so-called "*illegal job brokerage*" which punishes the recruitment and hiring of manpower for the purpose of exploiting them for work.
The activities considered sensitive in relation to the crime of "illegal job brokerage" are those relating to the management of personnel used in subcontracting.

11.3.11 Other activities subject to control

In addition to the controls and monitoring directly concerning the areas and activities within which the above mentioned Offences may theoretically be committed, Model 231 provides further, specific controls for the following processes of "supplies" or instruments management:

h) Financial transactions
i) Procurement of goods and services
j) Use of material resources with environmental impact
k) Consulting and professional services
l) Utility concessions (donations, scholarships, sponsorship of events)
m) Administrative, financial and accounting management necessary for the company's management
n) Human resources management (selection and recruitment of personnel, incentive system).

Among the areas of activity at risk, the Model has in fact considered not only those having a direct relevance as activities that could theoretically invite criminal conduct, but also those having an indirect and instrumental relevance in the commission of the Offences. In particular, instrumental activities are those in which the factual conditions that make it possible to commit Offences within the areas and activities specifically considered at risk of crime in the Model are present.

12 VALUES AND RULES OF CONDUCT

12.1 Global Code of Business Conduct

NTT DATA Italia has collected and described the values common to all those who operate within the NTT DATA Group in the Global Code of Business Conduct, approved and updated periodically by the Board of Directors.

This Code expresses the ethical commitments and responsibilities in the conduct of business and corporate activities undertaken by NTT DATA Italia towards all stakeholders, in the belief that ethics can be pursued in conjunction with

corporate success.

The document is available on the **NTT DATA Italia website** and on **the company's intranet**, and is available in Italian/English (editions are also available in other languages).

12.2 Policies and procedures

Policies and procedures describing sensitive processes and standard behaviours have been developed and disseminated in order to provide NTT DATA Italia employees and collaborators with guidance on the behaviours that the Company considers to be in line with the values expressed in the Code of Conduct and in this Model.

All company policies and procedures are sent/communicated to the individual employees whenever there are updates of content or form, and usually published on the company intranet.

12.3 Procedures on the management of financial resources

The Company's financial transactions are documented and reported in processes that clearly and transparently codify the activities, indicating the responsible authors according to the corporate organisation.

Monetary accounting entries are made in accordance with current accounting standards and NTT DATA Italia ensures the use of homogeneous methods and practices among the various units responsible for preparing its own administrative-accounting reports and that of its subsidiaries.

13 ORGANISATIONAL SYSTEM, ROLES AND POWERS

13.1 Characteristics of the organisational Structure

NTT DATA Italia is equipped with organisational tools based on the general principles of:

- Awareness within the Company and the Group
- Indication of roles (including assigned powers)
- Indication of reporting lines.

13.2 Definition of roles

The definition of roles is such as to ensure that a process is never followed independently by a single person, both in the case of operational processes of project development and management, and in the case of internal support processes.

The operational processes of project development and management, which, in other words, represent the sales and production processes, are overseen by the lines through work teams composed of different qualifications, where each contributes to the formulation of proposals and solutions to the customer, according to a collaborative style and based on their skills and qualifications. During the project development and management phases, operations that have an impact, even if only potential, on the company's financial resources (both incoming and outgoing) are monitored and documented. Control is the responsibility of persons in charge of the monthly Business Reviews and

of the Management, through the reports produced by the Administration, Finance and Control Departments - AFC (even if only "**Finance**") which, among other things, is responsible for reporting conduct not in line with the standards.

The AFC Department, on the one hand, supports the operational guidelines regarding the generation and use of financial resources related to the characteristic management, on the other hand it supports the top management in the management of financial resources related to assets, extraordinary and tax management. The management and the corporate bodies are responsible for monitoring the economic and financial performance of operations on the basis of the reports prepared by the FTA.

Advances in qualifications within the operational lines and changes in the role of personnel in general are communicated to employees of the Company (and of the Group, if they take place within Corporate Departments).

13.3 System of proxies and powers of attorney

The system of proxies and powers of attorney ensures the functioning of the company by reducing the powers required by the Board of Directors, the Chief Executive Officer and the various proxies.

"*Proxy*" means the internal act of assigning tasks and functions through organisational communications and company procedures; "power of *attorney*" means the unilateral legal transaction whereby the company assigns powers of external representation to third parties. Holders of a position requiring powers of representation shall be granted a power of attorney that is appropriate and consistent with the assigned tasks.

The main features of the proxy system are as follows:

- The proxy reflects the organisational position of the person receiving it, combining management power and relevant responsibility
- Each power of attorney clearly and unambiguously expresses the powers and the empowered person.

The distinctive elements of the power of attorney system are:

- The power of attorney is granted exclusively to persons with delegated powers by means of specific acts that describe the powers of representation and, where necessary, the spending powers as well as compliance with the Company's Organisational Models and Code of Ethics.
- High value purchases (thresholds indicated in the powers of attorney) must be authorised by the AD.
- Purchase orders must be issued by the Purchasing Manager (also verified by Management Control) and their traceability is guaranteed through the use of specific information technologies (e.g. Supplier Portal).

14 CORPORATE GOVERNANCE AND CORPORATE MANAGEMENT

14.1 Corporate Governance Model

In conjunction with the request for listing on regulated markets (first half of 2006), the Company began a process of adapting its Corporate Governance Model to the requirements of the Code of Conduct for Listed Companies with the aim of guaranteeing its shareholders an effective and transparent system of governance and management.

The Corporate Governance Model was subsequently adapted and simplified following the decision to postpone the listing on the Stock Exchange.

Currently, also following the recent changes in the corporate and control structure, the Corporate Governance Model is summarised in the Board of Directors, as well as in the Board of Statutory Auditors.

14.2 Corporate Committees

The Company and Group Committees are operational. For example, the Management Committee is active and deals with strategic issues for the development of the Group in the Business Rewiew, in which commercial priorities are defined and the annual budget is drawn up, and the economic performance is presented in the light of the company's objectives.

15 INTERNAL CONTROL SYSTEM

15.1 The Administration, Finance and Control Department

Within the NTT DATA Italia company organisation, the departments responsible for the functioning of the internal control system have been identified in order to group them under the title of "Administration, Finance and Control Department, as already mentioned in the previous paragraph. 4.2.. Those who manage and control the Company's financial resources act according to the same principles and the same rules of conduct, adopting a single control Model based on similar processes, tools and operating techniques except for specific business activities or country characteristics.
The head of the Department is the Chief Financial Officer/CFO, who defines the organisational structure of the units for which he is responsible, and organises the planning and control processes, in accordance with procedures and timescales aligned with the rules and requirements for guidance and supervision expressed by the Top Management and the Corporate Bodies.

15.2 Processes and tools

The internal control system is defined as the set of processes implemented by the *management* to provide reasonable assurance of the achievement of management and *compliance* objectives, such as the effectiveness and efficiency of operating activities, the reliability of company, accounting and management information, both for internal purposes and for third parties, and absolute compliance with the company and group laws, regulations, rules and policies.

16 SUPERVISORY BOARD

16.1 Appointment and structure of the Board

The Board is a collective body made up of three standing members, one of whom acts as Chairman, chosen by the majority of the Board, where not already indicated by the Board at the time of appointment. The collective body has the following structure:

- A person registered in the Register of Legal Auditors established at the Ministry of Economy and Finance or having competence in legal, management, analysis of control systems or in any case with significant experience in issues of specific relevance to the activities of the Supervisory Board.
- The Head of the Legal Department.
- A person with experience in the sector in which the Company carries out its characteristic management and/or with experience in the activities most exposed to the risk of a presumed crime under Law no. 231/2001.

The Board of Directors, reporting to the Shareholders' Meeting, has the power to appoint and revoke the members of the Board - on valid grounds, also related to organisational restructuring of the Company.The members of the Board are chosen from qualified individuals and experts in the above-mentioned fields, with an adequate degree of professionalism and meeting the requirements of independence, autonomy and honourable character, also from the point of view of the absence of criminal convictions, as better indicated below. The members of the Board may be appointed either from external parties or from within the Company. The members of the Board are not subject, in this capacity and within the scope of the performance of their duties, to the hierarchical and disciplinary power of any corporate body or department.

The Supervisory Board's term of office is three years. At the end of the three-year period, the Supervisory Board continues to perform its functions as an extension until the appointment of new members by the Board of Directors. The members of the Supervisory Board are eligible for re-election.

The internal members of the Board are removed from office in the event of voluntary termination of employment or collaboration with NTT DATA and dismissal for just cause and, in addition, for the Head of the legal department, in the event of termination of the department Head’s role. In the event of the resignation, withdrawal, incapacity, death, revocation or forfeiture of a member of the Board, the Board of Directors will immediately replace him/her. The Chairman, or the most senior member, is required to promptly notify the Board of Directors of the occurrence of one of the cases which make it necessary to appoint a new member of the Board.

In the event of resignation, withdrawal, incapacity, death, revocation or removal of the Chairman, the latter is replaced by the oldest member, who remains in this position until the date on which the Board of Directors has resolved to appoint a new Chairman of the Board.

For all other aspects, the Supervisory Board operates in accordance with the provisions of its Regulations, as follows. The Supervisory Board regulates its supervisory and control activities by means of a set of Regulations to be submitted to the Board of Directors of the Company for relevant acknowledgement at the first useful meeting, as well as any amendments that the Board deems necessary to make to it during its mandate.

16.2 Jurisdiction and grounds for (in)eligibility, revocation and suspension

Competences

The responsibilities of the members of the Supervisory Board, roughly divided between legal and organisational responsibilities, can be summarised as follows:

Legal competences: i.e. in-depth knowledge of the methodologies used to interpret the laws with specific preparation in the analysis of the types of crimes and in the identification of possible sanctionable conduct.
Such preparation presupposes familiarity with the research and analysis of the relevant case-law. The employee in question must, in brief, be capable of examining and interpreting the provisions of the law by identifying the types of offences, as well as the applicability of these types of offences in the context of the company's operations. They must also understand the company's operations, knowledge gained in a position of responsibility and hierarchical context within the company and have the ability to translate into rules of conduct the processes outlined in the organisational Model dedicated to risk prevention.

Organisational expertise, i.e. specific preparation regarding the analysis of company procedures and organisational processes, as well as general principles on "compliance" legislation and related controls. At least one of the members of the Supervisory Board must have experience in preparing control procedures and manuals. The profile is therefore that of an internal control expert who has gained this experience in the context of activities that have long been "regulated" and "supervised".

Competence in the sector in which the Company carries out its characteristic management and/or with experience in the activities most exposed to the risk of alleged offences.

The necessary autonomy of the Supervisory Board is guaranteed, due to its recognised position in relation to the departments mentioned in the context of the company organisational chart and the reporting lines assigned to them.

In order to assist in defining and carrying out the activities for which it is responsible and to ensure maximum compliance with the legal requirements and obligations, the Supervisory Board:

- avails itself of the Internal Audit department, where established, or an equivalent department, with adequate resources.
- may involve appropriate company resources to extract, process data and produce reports.

Grounds or (in)eligibility, removal and suspension of members of the Supervisory Board

The members of the Supervisory Board must meet the integrity requirements set out in Article 109 of the Legislative Decree of September 1, 1993, no. 385: in particular, those who find themselves in the situations stipulated by Article 2382 of the Italian Civil Code cannot be appointed as members of the Supervisory Board.

In addition, those who have been convicted by a sentence, even if not final, and even if issued under articles 444 and subsequent of the Code of Criminal Procedure and even in case of a conditionally suspended sentence, except for the effects of rehabilitation, cannot be appointed as a member of the Supervisory Board:

11) to imprisonment for a period of not less than one year for one of the crimes stipulated by the Royal Decree 267 of 16 March 1942;
12) to imprisonment for a period of not less than one year for one of the offences stipulated by the regulations governing banking, financial, securities and insurance activities and by the regulations governing markets and securities and payment instruments;
13) to imprisonment for a period of not less than one year for an offence against the public administration, against public faith, against public property, against the public economy, for a tax offence;
14) for any crime not punishable by imprisonment for a period of time not less than two years;

15) for one of the offences stipulated in Title XI of Book V of the Civil Code as reformulated by Legislative Decree no 61/2002;

16) for an offence which amounts to and has led to the conviction from which derives the prohibition, even temporary, to hold public offices, or the temporary prohibition to hold an executive position in legal persons and companies;

17) for one or several of the offences strictly stipulated by the Decree, even if with sentences lower than those indicated in the previous points;

18) those who have held the position of member of the Supervisory Board within companies to which the sanctions stipulated in art. 9 of the Decree have been applied;

19) persons to whom one of the prevention measures stipulated by Article 10, paragraph 3, of Law No. 575 of 31 May 1965, as replaced by Article 3 of Law No. 55 of 19 March 1990 and subsequent amendments, has been applied;

20) those against whom the accessory administrative sanctions stipulated by art. 187 quater of Legislative Decree no. 58/1998 have been applied.

Candidates for the office of member of the Supervisory Board must self-certify by means of a declaration in lieu of notoriety under Law no. 445/2000 that they do not find themselves in any of the situations listed under numbers 1 to 10, expressly undertaking to communicate any changes in the content of these declarations.

The members of the Supervisory Board cease to hold office when they find themselves, after their appointment, in one of the situations indicated above.

Finally, those who are in one of the following situations may not be appointed, or shall be removed:

Conflicts of interest, including potential conflicts of interest, with the Company such as to prejudice the independence required by the role and tasks to be performed. Direct or indirect ownership of shares of such an importance as to enable them to exercise significant influence over the Company. Public employment in central or local government during the three years preceding the appointment as a member of the Supervisory Board.

16.3 Functions and powers

The Supervisory Board defines and carries out the activities for which it is responsible according to the rule of collegiality and is endowed, under art. 6, paragraph 1, letter b) of Legislative Decree 231/2001 with "autonomous powers of initiative and control".

The activities that the Board is called on to perform are:

- Supervision of the **effectiveness** of the Model, which consists in verifying the consistency between the actual behaviours and the established Model.
- Examining the **adequacy** of the Model, i.e. its real (and not merely formal) capacity to prevent unwanted conduct in principle.
- Analysing the **maintenance** over time of the model's requirements of efficacy and functionality.
- Carrying out the **necessary dynamic updating** of the Model, in the event that the analyses carried out make it necessary to make corrections and adjustments. As a rule, this updating takes place in two distinct

and integrated phases:

- **Presentation of proposals to adapt the Model** to the corporate bodies/departments able to give them concrete implementation in the corporate fabric. Depending on the type and scope of the interventions, the proposals will be directed to the Personnel/HR and organisation, Administration departments, etc., or, in some cases of particular importance, to the Board of Directors.
- **Follow-up**, i.e. verification of the implementation and effective functionality of the proposed solutions.

The Supervisory Board, making use of the powers attributed to it, is therefore specifically called on to primarily carry out the following activities:

- Establishing the control activities at each operating level, equipping itself with the informative or non-informative tools to promptly report anomalies and malfunctions of the Model by verifying and preparing control manuals, where necessary.

- Activating the control procedures by bearing in mind the need to streamline the procedures and the fact that the primary responsibility for activity control is in any case entrusted to the Department Heads and/or to the top management of the company, to the corporate bodies appointed for this purpose and to the independent auditors.

- Updating the Model in accordance with the evolution of the regulations in force on the subject, as well as as a consequence of the changes in the company's internal organisation and activity.

- Collaborating in the preparation and integration of internal "regulations" (Codes of ethics and conduct, Procedures/operating instructions, Control manuals, etc.) dedicated to risk prevention.

- Adequately identifying, measuring and monitoring all the assumed risks or risks likely to be assumed as well as deriving from the interpretation and application of the reference standards, with respect to the actual company processes and procedures and with reference to the various operating segments of the company, constantly updating the risk detection and mapping activity.

- Promoting initiatives aimed at spreading knowledge of the Model among the bodies and employees of the company by providing any necessary instructions and clarifications, as well as by setting up specific training seminars.

- Coordinating with the other company departments to improve activity control and all matters regarding the concrete implementation of the Model.

- Carrying out extraordinary checks and/or targeted investigations when malfunctions of the Model are detected or when the offences covered by the prevention activities have been committed.

- Ensuring that the approved supervisory programme is drawn up, in line with the principles contained in Model 231, within the various sectors of activity; ensuring the coordination of the implementation of the supervisory programme and the implementation of planned and unplanned control measures.

In order to make the activity of the Supervisory Board feasible, it is necessary that:

- The activities carried out by the board may not be reviewed by any other body or corporate structure,

without prejudice, however, to the fact that the governing body is in any case called on to supervise the adequacy of its intervention, since the governing body is ultimately responsible for the functioning and effectiveness of the organisational model.

- The Supervisory Board has free access to all the company departments without the need for any prior consent in order to obtain any information or data deemed necessary for the performance of the tasks stipulated by Legislative Decree 231/2001.

- Under its own direct supervision and responsibility, the board may use the assistance of all the company structures or external consultants.

In the context of the procedures for drawing up the company budget, the Supervisory Board will have at its disposal an allocation of financial resources, proposed by the board itself, which the Board will be able to use for any requirement necessary for the correct performance of its tasks (e.g. specialist consultancy, travel, etc.).

In carrying out the tasks assigned to it, the Supervisory Board has unrestricted access to company information for investigation, analysis and control activities. All corporate departments, employees and/or members of the corporate bodies are required to provide information in the event of requests from the Supervisory Board or the occurrence of events or circumstances relevant to the performance of the activities of the Supervisory Board.

16.4 Obligations to notify the Supervisory Board

The obligation to notify the Supervisory Board is a further instrument to facilitate the monitoring the Model's effectiveness and the subsequent assessment of the causes that made possible the occurrence of the offence.

This obligation is addressed to the company departments at risk of offences and concerns: a) the periodic results of the control activity they carried out to implement the models (summary reports of the carried out activity, monitoring activities, final indices, etc.); b) the anomalies or atypical cases found in the available information (a fact that is not relevant if considered individually, could have different relevance if repeated or if the area of occurrence is extended).

The above-mentioned information is sent to the Supervisory Board every six months (**ordinary information flows**), and concerns, for example:

- Decisions relating to the application, allocation and use of public funds.
- Statistics on workplace accidents with specification of the cause/reason, the occurrence, possible recognition of the accident and its severity.
- List of any pending lawsuits involving the Company (not already reported to the Supervisory Board in a timely manner).
- Commissions of inquiry or internal reports from which liability may theoretically emerge for the offences under Legislative Decree 231/2001.
- Summaries of contracts awarded following tenders at national and European level, i.e. by means of private negotiation.
- Information regarding contracts awarded by public bodies or persons performing functions of public utility.

In addition to the ordinary information flows referred to above, information regarding particular or specific situations and/or events, as specified below (extraordinary information flows), must also be provided to the **Supervisory Board in a timely and compulsory** manner:

- Measures and/or information from the judicial police or any other authority, from which you can infer that

investigations are being carried out, even against unknown persons, for the offences under Legislative Decree 231/2001.
- Requests for legal assistance made by managers and/or employees in the event of initiation of legal proceedings for the offences stipulated in the Decree.
- Any fact, act, event or omission detected or observed in the exercise of the assigned responsibilities and tasks which present a risk with respect to compliance with the decree's provisions.
- Information on the actual implementation of the Organisational Model at all company levels, with evidence of the disciplinary proceedings carried out and of any sanctions imposed (including measures against Employees), or of the measures for the closure of such proceedings with the relevant reasons.

The Supervisory Board may propose any changes to the above-mentioned lists to the Chief Executive Officer. Any omission or delay in notifying the Supervisory Board of the information flows listed above will be considered a violation of the Organisational Model and may be sanctioned in accordance with the provisions of the Disciplinary System referred to in paragraph 9.2 below.

The information provided allows the Supervisory Board to improve its planning of controls and do not impose on it activities of timely and systematic verification of all the presented phenomena. In other words, the Board does not have an obligation to act whenever it receives information/reports, being left to its discretion and responsibility to establish in which cases to act.

16.5 Reports to the Supervisory Board by employees or company representatives or by third parties

Within the company, in addition to the documentation required by the procedures set out in this Model, any other information of any kind, originating from third parties and relating to the implementation of the Model in areas of activity at risk must be brought to the attention of the Supervisory Board.

In particular, the obligation to provide information is also extended to employees who come into possession of information relating to the commission of offences in particular within the company or who learn in the exercise of their functions of the perpetration of practices that are not in line with the rules of conduct that the company is required to issue (as seen above) within the scope of the Model specified in Legislative Decree 231/2001 (the so-called codes of ethics).

The obligation to inform one's employer of any conduct contrary to the Organisational Model is part of the broader duty of care and loyalty of the employee as per articles 2104 and 2105.

These rules specify, respectively:
- "*The employee must use the diligence required by the nature of the service due, by the interest of the company and by the best interests of national production*".
- "*It must also comply with the provisions for the performance and discipline of the work imparted by the company and its collaborators on whom it is hierarchically dependent*". (art. 2104) and "*The employee must not carry out business activities, on his own behalf or on behalf of third parties, in competition with the company, nor disclose information relating to the company's organisation and production methods, or make use of them in such a way as to be prejudicial to it*".(Article 2105).

The specification of an effective reporting system guarantees confidentiality to those who report violations in accordance with Law no. 179 of 30 November 2017. At the same time, deterrent measures are provided against any improper information, both in terms of content and form.

Law no. 179 of November 30, 2017 (which came into force on December 29, 2017) on *whistleblowing* introduced the new paragraph 2-bis of Article 6 of Legislative Decree 231/2001, under which the adopted organisational models must provide for the activation of one or several channels that make it possible to submit, for the protection of the company's integrity, detailed reports of unlawful conduct, relevant with respect to the offences provided for in it and based on precise and consistent factual elements, or of violations of the organisational and management model, of which they have become aware by reason of the functions they perform. These channels must guarantee the confidentiality of the reporter's identity in the report management activities and at least one must be able to guarantee confidentiality in computerised form.

In this regard:

- Any reports relating to the commission of offences stipulated in the Decree in relation to the company's activities or in any case regarding behaviour that is not in line with the rules of conduct adopted by the company are collected, with specific reports to the Supervisory Body, also by email to the address**OdV@nttdata.com**.There are also other channels which the company makes available to send any *whistleblowing* reports (for example, email address outside the company, administered by a specialized third-party Operator).
- Every employee is required to raise concerns about the violation of NTT DATA Italia's internal regulations or the law. "Doubtful" issues can be resolved at local level by asking the immediate supervisor and the person responsible for verifying compliance, with expertise broken down by business activity, Country and language. Once the issue has been raised, the Company identifies the involved departments and is required to examine the issue, carry out the necessary investigations and take the necessary action.
- Reports received by the Supervisory Board will be evaluated by the latter and any consequent measures will be proposed to the Human Resources Manager/Human Resources and to the direct superior of the perpetrator of the violation.
- Reports, in line with the Code of Ethics, may be either written or verbal and concern any violation or suspected violation of the Model. The Supervisory Board will act in such a way as to keep the reporters safe from any form of retaliation, ensuring the confidentiality of the reporter's identity, without prejudice to the legal obligations and the protection of the rights of the company or of persons accused erroneously and/or in bad faith.
- The Supervisory Board will evaluate the received reports and any consequent measures at its discretion and responsibility, possibly hearing the author of the report and/or the person responsible for the alleged violation and giving written reasons for any refusal to carry out an internal investigation.
- The Supervisory Board will assess with full and unquestionable discretion whether or not to follow up anonymous or insufficiently detailed reports.

16.6 Periodic checks and reports of the Supervisory Board

In order to guarantee the updating and efficiency of this Model, the Supervisory Board will carry out two types of checks:

- Document verification: annual verification of the main corporate documents and of the most important contracts concluded by the company in areas of risk activity in order to verify the compliance of the activities pertaining to them with the procedural and behavioural rules established by the Model.

- Verification of the Model: periodic verification of the Model's functioning and of the effective compliance

with the conduct procedures established internally by the company for the prevention of crimes in the areas of activity exposed to the commission of crimes.

Following these verifications, the Supervisory Board draws up a special report, highlighting the identified risks and suggesting the actions to be taken, to be submitted to the attention of the Board of Directors, on an annual basis.

16.7 Proxy system

The Company adopts a system of power of attorneys and proxies - as described in paragraph 4.3 above - so that the strategy defined in the business plan and approved by the Board of Directors can be implemented by the organisational structure. The system of powers of attorneys and proxies reflects the hierarchy of roles.

The Supervisory Board may indicate any changes to be made to this policy/strategy in order to adapt it to the requirements of the Decree.

The indications provided by the Supervisory Board will be evaluated by the Board of Directors, which will autonomously adopt the appropriate decisions.

16.8 Information archiving

All information, notification and reports stipulated in the Model are kept by the Supervisory Board in a special computer and/or paper database. The data and information stored in the database are made available to persons outside the Supervisory Board with the prior authorisation of the Supervisory Board itself. The latter shall define the criteria and conditions for access to the database in writing.

17 MODEL DISSEMINATION AND IMPLEMENTATION

17.1 Communication plan

17.1.1 Communication to the members of the corporate bodies

The Model shall be brought to the attention of the Corporate Secretarial office of each corporate body who - due to their appointment or absence - has not already taken part in the approval of the Model.

17.1.2 Communication to Executives and Department Managers

On the instructions of the Supervisory Board, the principles and contents of the Model are formally communicated by the Management to all managers (in office and per position) and to the Department Managers, through delivery of this document and/or distribution on the company intranet.

17.1.3 Communication to all other employees

This document is sent/made available in electronic form to all employees and is available for consultation on the website www.nttdata.com/itat the address (also available to third parties), as well as on the company intranet.

In order to encourage the Model's dissemination to all employees, within the personnel departments, the Department Managers and the management functions have the task of communicating and underlining the importance of the values, rules and instruments that make up the Model itself.

17.1.4 Personnel training

Personnel training for the purposes of implementing the Model is managed by the Human Resources Manager in close collaboration with the Legal & Compliance department and the Supervisory Board. The principles and contents of Model 231 are also disseminated through training courses in which the persons identified above are required to participate. The structure of the training courses is defined by the Head of Human Resources/Human Resources together with the Legal & Compliance department and with the advice of the Supervisory Board.

The following training tools are also used:

- Periodic note Internal information
- Information in the letters/documents in the recruitment phase for newly hired employees (e.g. "Welcome Kit/Your Guidebook" or similar tool)
- Intranet access
- Circular letter also sent by mail/email.

17.2 Communication to third parties

Information may be provided to parties outside NTT DATA Italia (for example: Representatives, Consultants and Business Partners) on the policies and procedures adopted by the company on the basis of this Organisational Model, as well as the texts of the contractual clauses normally used in this regard.

The commitment to comply with the reference principles of Model 231 on the part of third parties having contractual relationships with NTT DATA Italia is in fact stipulated by means of a specific clause in the relevant contract, which is accepted by the third party, with termination *ipso jure* in the event of non-compliance.

17.2.1 Training of external collaborators

The external collaborators which NTT DATA Italia could involve in the development and management of projects due to the need for know-how or the unavailability of internal resources, must be aware of the provisions of Legislative Decree 231/2001 and, where required, declare that they have adopted Model 231 or, at least, appropriate procedures to avoid in any way the involvement of NTT DATA Italia in the event of the commission of the offences stipulated by the above-mentioned legislation.

18 DISCIPLINARY SYSTEM

18.1 General principles and criteria for imposing sanctions

The disciplinary mechanisms indicated herein form an integral part of the Company's organisational model.

In general, the application of disciplinary sanctions does not depend on whether or not criminal proceedings for the commission of one of the offences stipulated in Legislative Decree 231/2001 have been initiated and concluded. 231/2001.

In individual cases, the application of specific sanctions is defined and applied in proportion to the severity of the

assessed non-compliance, in accordance with the general principles governing labour law.

In individual cases, the type and extent of specific penalties is applied in proportion to the severity of the non-compliance and, in any case, on the basis of the following general criteria which may be cumulated:

l) subjective element of the conduct (willful misconduct or negligence, the latter due to imprudence, negligence or inexperience also in view of the event's predictability or lack of);

m) importance of the breached obligations;

n) gravity of the danger created;

o) recidivism in the two-year period;

p) the extent of any damage caused to the Company by the possible application of the sanctions stipulated by Legislative Decree 231/2001 and subsequent amendments and additions;

q) level of hierarchical and/or technical responsibility;

r) presence of aggravating or mitigating circumstances, with particular regard to previous work performance and previous disciplinary actions in the last two years;

s) sharing of responsibility with other workers who have contributed to the non-compliance;

t) where more than one offence has been committed by a single act and is punishable by different penalties, the most serious penalty shall apply;

u) recidivism in the two-year period automatically entails the application of the most serious sanction within the foreseen typology;

v) The principles of timeliness and immediacy require the imposition of disciplinary sanctions, irrespective of the outcome of any criminal proceedings.

RECIPIENTS

This disciplinary system is divided by category of recipients, under Article 2095 of the Italian Civil Code, as well as the possible autonomous or parasubordinate nature of the relationship between the recipients themselves and the Company and refers to:

c) persons who hold positions of representation, administration or management of the Company (so-called "*Executives*");
d) persons subject to the management or supervision of one of the above mentioned persons (so-called "*Employees*"), as well as to the persons referred to in paragraph 9.2.4 (the so-called), "*External collaborators*).

In any case, the imposition of the sanction implies the involvement of the Supervisory Board, which assesses the existence and seriousness of the violation.

18.2 Penalties

18.2.1 Penalties for employees (Executives - employees)

1.SCOPE OF APPLICATION

Under the combined provisions of Articles 5(b) and 7 of Legislative Decree 231/2001, without prejudice to the prior contestation and the procedure prescribed by art. 7 of Law no. 300 of 20 May 1970 (the so-called Employees' Statute), the sanctions stipulated in this Section apply to executives and employees of the Company who commit disciplinary offences deriving from:

g) failure to comply with the procedures and requirements contained in the Organisational Model due to serious non-compliance with the provisions aimed at guaranteeing the performance of the activity in compliance with the law and at promptly discovering and eliminating risk situations, under Legislative Decree 231/2001;

h) serious or repeated violation of the internal procedures contained in the Organisational Model, by behaving in such a way as to tolerate significant irregularities or to omit to carry out the controls and/or checks provided for in the individual procedures, even if the Company's interests have not been prejudiced;

i) violation and/or circumvention of the internal control system, carried out by removing, destroying or modifying the procedure documentation or by preventing the control of or access to the information and documentation to the persons in charge, including the Control Body;

j) serious or repeated failure to comply with the rules contained in the Code of Ethics;

k) repeated failure to comply with the obligation to inform the Control Body and/or the direct hierarchical superior of the failure to comply with the procedures and requirements of the Organisational Model;

l) conduct aimed at committing an offence stipulated by Legislative Decree 231/2001 and subsequent amendments and additions.

2.SANCTIONS

Failure to comply with the procedures and requirements contained in this Section of the Disciplinary System, paragraph 1 letters a) to f) by executives and employees, depending on the seriousness of the offence, is sanctioned with the following disciplinary measures indicated per levels and in full compliance with the applicable Collective Labour Contracts:

(a) verbal reprimand;

(b) written reprimand;

(c) a fine not exceeding the amount of three hours' pay;

(d) suspension from work;

(e) dismissal with notice;

(f) dismissal without notice.

If the above-mentioned employees have a power of attorney with the power to represent the Company externally, the imposition of the most serious sanction of the fine will also result in the automatic revocation of the power of

attorney.

2.A) Verbal reprimand

The sanction of a verbal reprimand is imposed in cases of negligent and slight violation of the procedures and/or requirements contained in the Organisational Model as well as of the rules contained in the Code of Ethics that have no consequences for the Company.

2.B) Written Reprimand

The sanction of a written reprimand is imposed in case of:

c) recidivism in the two-year period in cases of willful misconduct violation of procedures and/or requirements contained in the Organisational Model, as well as of the rules contained in the Code of Ethics;

d) minor procedural errors due to negligence on the part of the worker having external significance.

2.C) FINES

In addition to the cases of recidivism in the commission of the offences referred to in letter b) of point 2 b) above, a fine may be applied in cases where, due to the level of hierarchical or technical responsibility, or in the presence of aggravating circumstances, willful misconduct and/or negligent behaviour may undermine, albeit at a potential level, the effectiveness of the Organisational Model; such as, by way of example but not limited to:

c) failure to comply with the obligation to inform the Control Body and/or the direct hierarchical or functional superior of the failure to comply with the procedures and requirements of the Organisational Model;

d) failure to comply with the requirements of the procedures and rules indicated in the Organisational Model, as well as with the rules contained in the Code of Ethics, in the event that they concerned or concern a procedure of which one of the necessary parties is the Public Administration.

2.D) SUSPENSION FROM OFFICE

The sanction of suspension from office is imposed, as well as in cases of recidivism in the commission of offences which may result in the application of the fine, in cases of serious violations of procedures and requirements contained in the Organisational Model as well as of the rules contained in the Code of Ethics such as to expose the Company to risks and responsibilities under Law 231/01.

2.E) DISMISSAL WITH NOTICE

The sanction of dismissal with notice is imposed in cases of repeated serious violation of the procedures and requirements contained in the Organisational Model and of the rules of the Code of Ethics having external relevance in the performance of activities in the areas/activities at risk of crime under Legislative Decree 231/2001 and subsequent amendments and additions.

2.F) DISMISSAL WITHOUT NOTICE

The sanction of dismissal without notice is imposed for such serious misconduct as not to allow the continuation, even on a provisional basis, of the employment relationship (so-called just cause) such as, by way of example, but not limited to:

d) a conduct aimed at committing an offence included among those stipulated in Legislative Decree 231/2001 and subsequent amendments and additions

e) violation and/or fraudulent circumvention of procedures and requirements contained in the Organisational Model and of the rules of the Code of Ethics having external relevance for the purpose of committing or facilitating crimes under Law 231/01 and such as to eliminate the fiduciary relationship with the employer

f) violation and/or circumvention of the internal control system, carried out by removing, destroying or altering the procedure documentation or by preventing the control of or access to information and documentation to the persons in charge, including the Control Body in order to commit, contribute to or facilitate crimes under Law 231/01 and in such a way as to prevent If the worker has committed one of the offences stipulated in this article, the Company may decide the precautionary dismissal with immediate effect.

The HR/Personnel Department communicates the enforcement of the sanction to the Supervisory Board. The disciplinary system is constantly monitored by the Supervisory Board and the Human Resources/HR department.

All legal and contractual obligations relating to the imposition of disciplinary sanctions are complied with.

18.2.2 Measures against Executives

1.SCOPE OF APPLICATION

Under the combined provisions of Articles 5(b) and 7 of Legislative Decree 231/2001, and, limited to these rules, in compliance with the procedure stipulated in art. 7 of Law no. 300 of 20 May 1970, the sanctions indicated in this Section apply to executives who commit disciplinary offences deriving from:

g) violation of the internal procedures contained in the Organisational Model by behaving in a way that consists in tolerating irregularities in work or in not complying with work duties or obligations even in the event that there has been no prejudice to the Company's activity or interests;

h) serious non-compliance with the procedures and requirements contained in the Organisational Model such as to involve situations of risk, under Legislative Decree 231/2001;

i) violation and/or circumvention of the internal control system, carried out by removing, destroying or altering the procedure documentation or by preventing the control or access to information and documentation to the persons in charge, including the Control Body, in order to commit, contribute to or facilitate crimes under Law 231;

j) serious breach of the rules contained in the Code of Ethics;

k) repeated failure to comply with the obligation to inform the Control Body and/or the direct hierarchical superior of the failure to comply with the procedures and requirements of the Organisational Model;

l) serious or repeated failure to supervise as "hierarchical manager" the compliance with the procedures and requirements of the Organisational Model by their subordinates in order to verify their actions within the areas at risk of crime and, in any case, in the performance of activities instrumental to operational processes at risk of crime;

2.SANCTIONS

In the event of failure to comply with the procedures and requirements contained in this Section of the Disciplinary

System paragraph 1 letters a) to h), depending on the seriousness of the offence, the most appropriate measures will be applied against those responsible in accordance with the provisions of the applicable National Collective Work Agreement for Executives. Specifically:

- in the event of a minor violation of one or several procedural or behavioural rules set out in the Model, the manager shall be required in writing to comply with the Model, which is a necessary condition for maintaining the relationship of trust with the Company
- in the event of a serious or repeated violation of one or several provisions of the Model such as to constitute a significant breach, the manager shall be dismissed with notice;
- where the violation of one or several provisions of the Model is so serious as to irreparably damage the relationship of trust, not allowing the continuation, even temporary, of the employment relationship, the employee shall be dismissed without notice.

If the manager has a power of attorney with the power to represent the Company externally, the imposition of the disciplinary sanction will also result in the automatic revocation of the power of attorney.

18.2.3 Measures against "Top Management" and Statutory Auditors

1.SCOPE OF APPLICATION

For the purposes of Legislative Decree 231/2001, in the current organisation of the Company the following persons are considered *"Top Management":*

- the Managing Director
- The Directors with legal representation
- the other Directors
- the General Directors, if appointed.

Under the combined provisions of Articles 5(a) and 6 of Legislative Decree 231/2001 the sanctions stipulated in this Section shall apply to *"Top Management"* in the following cases:

d) serious or repeated failure to comply with the specific protocols (procedures and requirements) stipulated in the Organisational Model under Legislative Decree 231/2001, aimed at planning the formation and implementation of the Company's decisions in relation to the crimes to be prevented, and the rules contained in the Code of Ethics, including the violation of the provisions relating to the powers of signature and, in general, the system of proxies as well as the violation of the measures regarding the management of financial resources;

e) violation and/or circumvention of the internal control system stipulated in the Code of Ethics and in the Organisational Model, by removing, destroying or altering the documentation stipulated in the protocols (procedures and requirements) or by preventing the control of or access to information and documentation by the persons in charge, including the Control Body;

f) serious or repeated violation of the disclosure obligations stipulated in the Organisational Model towards the Supervisory Body and/or any supervised person; failure, in the exercise of the hierarchical powers and within the limits deriving from the system of proxies, to comply with the obligations of control and supervision of the behaviour of the direct subordinates, meaning only those who, under the direct and immediate authority of the top management, operate within the areas at risk of crime.

2.PROTECTION MEASURES

Depending on the seriousness of the offence committed by the Director, the Board of Directors, having heard the opinion of the Board of Statutory Auditors, will take the most appropriate measures, including the revocation of the transactions falling within the scope of the proxies, the modification or revocation of the proxies themselves and in the most serious cases, convening the Shareholders' Meeting for the adoption of the measures under Articles 2383 and 2393 of the Italian Civil Code.

If the reported violation is committed by two or several members of the Board of Directors, if it considers the report received from the Control Body to be justified and the Board of Directors has not done so, the Board of Statutory Auditors shall convene the Shareholders' Meeting under Article 2406 of the Italian Civil Code and, once the existence of the violation has been ascertained, it shall adopt the most appropriate measures, including, in the most serious cases, those under Articles 2383 and 2393 of the Italian Civil Code.

3.COEXISTENCE OF SEVERAL RESPONSIBILITIES OF THE SAME PERSON

In the event that the top management employee also holds the position of manager, in the event of violations carried out as top management, the sanctions of this Section will be applied to him, without prejudice, however, to the applicability of the various disciplinary actions applicable on the basis of the employment relationship with the Company and in compliance with the legal procedures, where applicable.

4.MEASURES AGAINST AUDITORS

In the event of violations committed by one or several Statutory Auditors, the Supervisory Board informs the Board of Directors and the Board of Statutory Auditors, so that they can proceed without delay and in accordance with the powers stipulated by law and/or the Articles of Association, to convene the Shareholders' Meeting to reach the necessary resolutions, which may also consist in revoking the appointment for just cause.

18.2.4 External collaborators

1.SCOPE OF APPLICATION

With regard to those who, in their capacity as collaborators, consultants and suppliers of NTT DATA Italia, are therefore required to comply with the obligations set out in Legislative Decree 231/2001, have committed the serious violations of the rules of the Code of Ethics and of the procedures and requirements contained in the Organisational Model indicated below, the termination of the contractual relationship for legal grounds may be decided under art. 1456 of the Italian Civil Code.

This is without prejudice, in any case, to any claim submitted by the Company for compensation for damages suffered.

2.NON-COMPLIANCE

c) fraudulent circumvention of company procedures and requirements and of the rules of the Code of Ethics concerning the object of the assignment having external relevance or violations carried out by means of

conduct aimed at committing an offence included among those stipulated in Legislative Decree 231/2001 and the subsequent amendments and additions;

d) lack of, incomplete or untrue documentation of the activity carried out, subject of the assignment, such as to prevent its transparency and verifiability.

3.CONTRACTUAL CLAUSES

The following is the text of the clause to be included - with the appropriate modifications - in the Orders to third party suppliers, in the contracts and in the Internal Covenants of the temporary companies consortia (RTI / ATI):

"With specific reference to Legislative Decree no. 231/2001 and subsequent amendments and additions. (**"Decree 231"**) and for the *purposes of prevention and repression of willful misconduct criminal offences stipulated and reported in it (**"Assumed Offences"**), the Supplier, the Collaborator and/or the third party supplier, having a business relationship with NTT DATA Italia under this Contract (the **"Supplier"**), declares it has been made aware and undertakes to comply with the key principles reflected in the NTT DATA Global Code of Business Conduct available on the NTT DATA Italia website http://emea.nttdata.com/en/chi-siamo/index.html ("**Code of Ethics"**), including the fight against corruption and counterfeiting of intellectual and industrial property assets, and also undertakes to comply with the minimum standards of conduct specified in Annex "A" to the Code of Ethics (collectively the **"Core Principles"**).*

The supplier also declares that he has read the Organisational Model (General Section) of NTT DATA Italia, which can be consulted on the website and/or on the Supplier Portal.

*In view of the above-mentioned facts, the supplier is aware that (a) the failure to comply or the partial failure to comply with the Basic Principles of the Code of Ethics and/or (b) the indictment for one of the alleged offences stipulated in Decree 231 (where they are punishable for willful misconduct) will constitute a serious breach of contract and will entitle NTT DATA Italia to **terminate this Contract ipso jure** under and for the purposes of Article 1456 of the Italian Civil Code, within the deadlines set out in this clause, without prejudice to claiming compensation for any damages caused to the Company.*

18.2.5 Measures to protect reports (Whistleblowing)

The following represent grounds for complaint and subsequent disciplinary sanction, if in the relationship with employees, directors and third parties the following occur:

- violation of the confidentiality of the identity of persons who under Law no. 179 of 30/11/2017, reported crimes of which they have become aware for work reasons.
- Making false reports by illegitimately making use of the means defined by Law No. 179 of 30/11/2017 to obtain personal benefits or benefits for related parties or to harm other persons.
- To cause undue prejudice to persons who may be the subject of reports received under Law 179/2017.