Information Type: Open Distribution/Public Document
Company Name: NTT DATA Italia
Information Owner: Compliance

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

AI SENSI DEL D. LGS. 231/2001

DI NTT DATA ITALIA S.P.A.

PARTE GENERALE

Approvato dal Consiglio di Amministrazione del 5 dicembre 2025

SOMMARIO

DEFINIZIONI

Attività sensibili	Si tratta delle attività aziendali nel cui ambito può profilarsi il rischio di commissione dei reati contemplati dal D. Lgs. 231/2001
CCNL	Contratto collettivo nazionale di lavoro applicabile ai dipendenti non dirigenti di NTT Data Italia S.p.A.
CCNL Dirigenti	Contratto collettivo nazionale di lavoro applicabile ai Dirigenti di NTT Data Italia S.p.A.
Codice Etico di NTT DATA o Codice Etico	Complesso di principi diritti, doveri e responsabilità a cui deve essere ispirata l'azione di tutti coloro che concorrono, con il proprio lavoro allo svolgimento dell'attività sociale
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	Decreto Legislativo 8 giugno 2001 n. 231 e successive modifiche e integrazioni
Destinatari	Componenti degli organi sociali (ad esempio: assemblea, C.d.A.) e degli organismi interni di governance aziendali (ad esempio: Comitati), 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, clienti)
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 NTT DATA Italia S.p.A.
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	Il presente Modello di Organizzazione, Gestione e Controllo ex D. Lgs. n. 231/2001 adottato da NTT DATA Italia S.p.A.
NTT DATA Inc.	NTT DATA Inc. (Japan), società controllante al 100% di NTT DATA EMEAL

NTT DATA EMEAL	NTT DATA Europe & Latam S.L.U.
NTT DATA EMEA Ltd.	NTT DATA EMEA Ltd. (London), società che esercita attività di direzione e coordinamento di NTT DATA Italia S.p.A.
Gruppo NTT DATA	NTT DATA Group Corporation 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 Amministratore Delegato di NTT DATA Italia S.p.A.

1 QUADRO NORMATIVO

1.1 Il Decreto Legislativo n. 231/2001

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 questi ultimi commettano – nell'ambito delle proprie attività – i Reati elencati dal medesimo (**All. 3**).

Secondo quanto previsto dal Decreto, gli enti possono essere ritenuti "responsabili" per alcuni reati commessi o tentati nel loro interesse o a loro vantaggio, da parte di esponenti dei vertici aziendali (i c.d. soggetti "in posizione apicale" o "apicali") e di coloro che sono "sottoposti alla direzione o vigilanza" di questi ultimi (art. 5, comma 1 D. Lgs. 231/2001)1.

La responsabilità amministrativa degli enti è autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato e, a determinate condizioni, si affianca a quest'ultima.

L'ampliamento di responsabilità introdotto con l'emanazione del D.Lgs. 231/2001 mira - sostanzialmente - a coinvolgere, nella punizione di determinati reati, il patrimonio delle società e, in ultima analisi, gli interessi economici dei soci, i quali, fino all'entrata in vigore del D.Lgs. 231/2001, non pativano dirette conseguenze dalla realizzazione di reati commessi, nell'interesse o a vantaggio della propria società.

Tuttavia, la responsabilità amministrativa è esclusa se l'ente ha, tra l'altro, adottato ed efficacemente attuato, prima della commissione dei reati, un modello di organizzazione, gestione e controllo idoneo a prevenire reati della stessa specie di quello verificatosi.

1.2 Apparato sanzionatorio

Gli artt. 9 - 23 del D.Lgs. 231/2001 prevedono a carico dell'ente, in conseguenza della commissione o tentata commissione dei Reati, le seguenti sanzioni:

- sanzione pecuniaria (e sequestro conservativo in sede cautelare);
- sanzioni interdittive (applicabili anche quali misure cautelari) di durata non inferiore a tre mesi e non superiore a due anni (con la precisazione che, ai sensi dell'art. 14, comma 1, D.Lgs. 231/2001, *"Le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente"*) che, a loro volta, possono consistere in:
  - interdizione dall'esercizio dell'attività;
  - sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;

[1] Art. 5, comma 1, del d.lgs. 231/2001: "Responsabilità dell'ente – L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)".

- esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;
- divieto di pubblicizzare beni o servizi;
- confisca (e sequestro preventivo in sede cautelare);
- pubblicazione della sentenza (in caso di applicazione di una sanzione interdittiva).

La sanzione pecuniaria viene determinata da parte del Giudice attraverso un sistema basato su "quote" in numero non inferiore a cento e non superiore a mille e di importo variabile fra un minimo di euro 258,22 ad un massimo di euro 1.549,37. Nella commisurazione della sanzione pecuniaria il Giudice determina:

- il numero delle quote, in considerazione della gravità del fatto, del grado della responsabilità dell'ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti;
- l'importo della singola quota, in base alle condizioni economiche e patrimoniali dell'ente.

Le sanzioni interdittive si applicano in relazione ai soli illeciti amministrativi per i quali siano espressamente previste e purché ricorra almeno una delle seguenti condizioni:

a) l'ente ha tratto un profitto di rilevante entità dalla consumazione del reato e questo è stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in tale ultimo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;

b) in caso di reiterazione degli illeciti.

Il Giudice determina il tipo e la durata della sanzione interdittiva tenendo in considerazione l'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso e, se necessario, può applicarle congiuntamente (art. 14, comma 1 e comma 3, D.Lgs. 231/2001).

Le sanzioni dell'interdizione dall'esercizio dell'attività, del divieto di contrattare con la Pubblica Amministrazione e di pubblicizzare beni o servizi possono essere applicate - nei casi più gravi - in via definitiva[2].

Inoltre, ai sensi e alle condizioni di cui all'art. 15 del D.Lgs. 231/20013, è possibile la prosecuzione dell'attività dell'ente (in luogo dell'irrogazione della sanzione) da parte di un commissario nominato dal Giudice ai sensi e alle condizioni di cui all'art. 15 del D.Lgs.

---

[2] Si veda, a tale proposito, l'art. 16 D.Lgs. 231/2001, secondo cui: "*1. Può essere disposta l'interdizione definitiva dall'esercizio dell'attività se l'ente ha tratto dal reato un profitto di rilevante entità ed é già stato condannato, almeno tre volte negli ultimi sette anni, alla interdizione temporanea dall'esercizio dell'attività. 2. Il giudice può applicare all'ente, in via definitiva, la sanzione del divieto di contrattare con la Pubblica Amministrazione ovvero del divieto di pubblicizzare beni o servizi quando è già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni. 3. Se l'ente o una sua unità organizzativa viene stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione di reati in relazione ai quali é prevista la sua responsabilità é sempre disposta l'interdizione definitiva dall'esercizio dell'attività e non si applicano le disposizioni previste dall'articolo 17*".

[3] "*Commissario giudiziale – Se sussistono i presupposti per l'applicazione di una sanzione interdittiva che determina l'interruzione dell'attività dell'ente, il giudice, in luogo dell'applicazione della sanzione, dispone la prosecuzione dell'attività dell'ente da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, quando ricorre almeno una delle seguenti condizioni: a) l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività; b) l'interruzione dell'attività dell'ente può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione. Con la sentenza che dispone la prosecuzione dell'attività, il giudice indica i compiti ed i poteri del commissario, tenendo conto della specifica attività in cui è stato posto in essere l'illecito da parte dell'ente. Nell'ambito dei compiti e dei poteri indicati dal giudice, il commissario cura l'adozione e l'efficace attuazione dei modelli di organizzazione e di controllo idonei a prevenire reati della specie di quello verificatosi. Non può compiere atti di straordinaria amministrazione senza autorizzazione del giudice. Il profitto derivante dalla prosecuzione dell'attività viene confiscato. La prosecuzione dell'attività da parte del commissario non può essere disposta quando l'interruzione dell'attività consegue all'applicazione in via definitiva di una sanzione interdittiva*".

231/2001.

Nei casi in cui i delitti puniti ai sensi del D.Lgs. 231/2001 vengano commessi in forma tentata, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di durata) vengono ridotte da un terzo alla metà (artt. 12 e 26 D.Lgs. 231/2001).

Non insorge alcuna responsabilità in capo all'ente qualora lo stesso impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 D.Lgs. 231/2001). In tal caso, l'esclusione di sanzioni si giustifica in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e per suo conto.

1.3 Reati commessi all'estero

Ai sensi dell'art. 4 del D.Lgs. 231/2001, l'ente può essere chiamato a rispondere in Italia in relazione a reati - contemplati dal Decreto - commessi all'estero[4].

I presupposti su cui si fonda la responsabilità dell'ente per reati commessi all'estero sono:

i. il reato deve essere commesso da un soggetto funzionalmente legato all'ente, ai sensi dell'art. 5, comma 1, del D.Lgs. 231/2001;

ii. l'ente deve avere la propria sede principale nel territorio dello Stato italiano;

iii. l'ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p. (nei casi in cui la legge prevede che il colpevole - persona fisica - sia punito a richiesta del Ministro della Giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti dell'ente stesso) e, anche in ossequio al principio di legalità di cui all'art. 2 del D.Lgs. 231/2001, solo a fronte dei reati per i quali la sua responsabilità sia prevista da una disposizione legislativa *ad hoc*;

iv. sussistendo i casi e le condizioni di cui ai predetti articoli del codice penale, nei confronti dell'ente non proceda lo Stato del luogo in cui è stato commesso il fatto.

1.4 La responsabilità da reato nei gruppi di imprese

Il Decreto non affronta espressamente gli aspetti connessi alla responsabilità dell'ente appartenente a un gruppo di imprese, nonostante tale fenomeno sia ampiamente diffuso.

Come evidenziato anche dalle Linee Guida di Confindustria nella loro versione aggiornata, la *holding*/controllante potrà essere ritenuta responsabile per il reato commesso nell'attività della controllata qualora:

- sia stato commesso un Reato presupposto nell'interesse o vantaggio immediato e diretto, oltre che della controllata, anche della controllante;
- persone fisiche collegate in via funzionale alla controllante abbiano partecipato alla commissione del reato presupposto recando un contributo causalmente rilevante (Cass. Pen., Sez. V, sent. n. 24583/2011), provato in maniera concreta e specifica.

[4] L'art. 4 del D.Lgs. 231/2001 prevede quanto segue: "*1. Nei casi e alle condizioni previsti dagli articoli 7, 8, 9 e 10 del codice penale, gli enti aventi nel territorio dello Stato la sede principale rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto. 2. Nei casi in cui la legge prevede che il colpevole sia punito a richiesta del Ministro della giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti di quest'ultimo.*"

Occorre, pertanto, non solo che ciascuna società italiana di un gruppo disponga di un modello di organizzazione, gestione e controllo effettivo ed efficace, ma che lo stesso sia coerente con il sistema dei protocolli di controllo della holding e che sia garantito un adeguato scambio di informazioni tra i rispettivi organismi di vigilanza.

1.5 Modelli di Organizzazione, Gestione e Controllo

Come detto sopra (cfr. Par. 1.1), elemento caratteristico dell'apparato normativo dettato dal D. Lgs. 231/2001 è l'attribuzione di un valore esimente al modello di organizzazione, gestione e controllo adottato dall'ente.

In caso di reato commesso da un soggetto in posizione apicale, infatti, la società non risponde se prova che (art. 6, comma 1, del D.Lgs. 231/2001):

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del reato, modelli di organizzazione e gestione idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un organismo della società dotato di autonomi poteri di iniziativa e di controllo;
- le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;
- non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di vigilanza.

Nel caso di reato commesso da soggetti apicali sussiste in capo all'ente una presunzione di responsabilità dovuta al fatto che tali soggetti esprimono e rappresentano la politica e, quindi, la volontà dell'ente stesso.

Per essere esente da responsabilità, l'ente dovrà, dunque, dimostrare la sua estraneità ai fatti contestati al soggetto apicale provando la sussistenza dei sopra elencati requisiti tra loro concorrenti e, di riflesso, la circostanza che la commissione del reato non deriva da una propria "colpa organizzativa".

Nel caso, invece, di un reato commesso da soggetti sottoposti alla direzione o vigilanza di un apicale, la società risponde se la commissione del reato è stata resa possibile dalla violazione degli obblighi di direzione o vigilanza alla cui osservanza la società è tenuta.

In tal caso, dunque, si assisterà ad un'inversione dell'onere della prova. L'accusa sarà, pertanto, tenuta a provare la mancata adozione ed efficace attuazione di un modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello verificatosi.

L'art. 7 co. 4 D.Lgs. 231/2001 definisce, inoltre, i requisiti dell'efficace attuazione dei modelli di organizzazione, gestione e controllo:

- la verifica periodica e l'eventuale modifica del modello di organizzazione, gestione e controllo quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione e nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione, gestione e controllo.

I modelli di organizzazione, gestione e controllo adottati ai sensi del D.Lgs. 231/2001, in

relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, devono:

- individuare le attività nel cui ambito possono essere commessi reati (cfr. Parte Speciale del presente modello di organizzazione, gestione e controllo, di seguito "Modello");
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire (delineati per ciascuna attività sensibile, nella Parte Speciale del presente Modello);
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati (cfr. l'attività sensibile "Gestione dei flussi finanziari (pagamenti e incassi)" della Parte Speciale del presente Modello);
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello di organizzazione, gestione e controllo.

Con riferimento ai reati in materia di salute e sicurezza sul lavoro, l'art. 30 del D.Lgs. 81/2008 (cd. Testo Unico Sicurezza) prevede che il modello di organizzazione, gestione e controllo deve essere adottato attuando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:

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

1.6 Linee Guida per la predisposizione dei Modelli di Organizzazione, Gestione e Controllo

L'art. 6 co. 3 D.Lgs. 231/2001 prevede che "*I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati*".

Nella predisposizione e aggiornamento del presente Modello, NTT DATA Italia S.p.A. si è

ispirata alle Linee Guida di Confindustria emanate il 7 marzo 2002, parzialmente modificate il 31 marzo 2008, aggiornate il 23 luglio 2014 e da ultimo nel mese di giugno 2021, approvate da parte del Ministero della Giustizia.

In particolare, le Linee Guida elaborate da Confindustria, nella loro ultima versione, suggeriscono di utilizzare, nella costruzione dei Modelli di Organizzazione, Gestione e Controllo, le attività di *risk assessment* e *risk management*, prevedono le seguenti fasi:

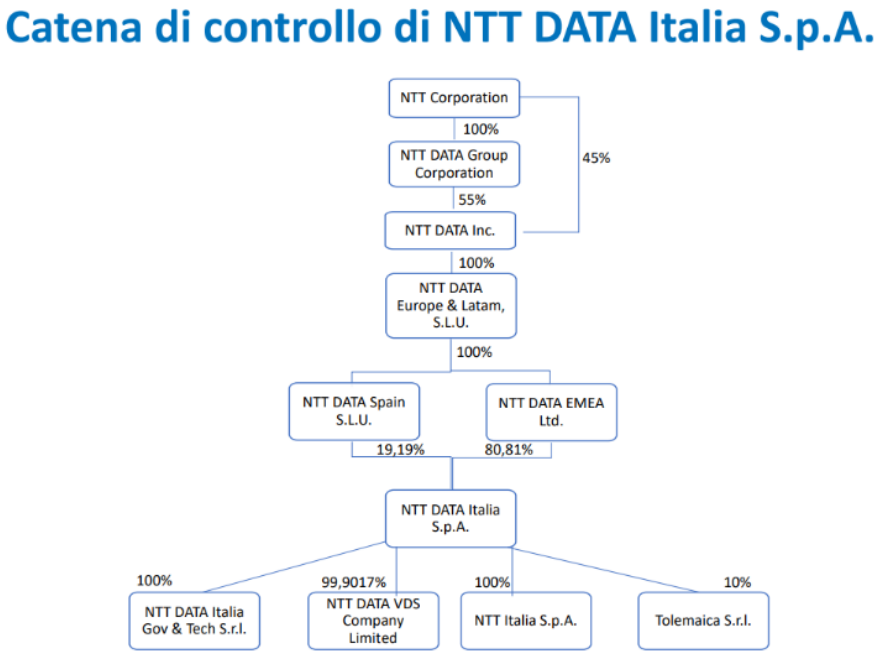
- individuazione delle attività cd. sensibili, ossia quelle nel cui ambito possono essere commessi i reati, e dei relativi rischi;
- analisi del sistema di controllo esistente prima dell'adozione/aggiornamento del modello di organizzazione, gestione e controllo;
- valutazione dei rischi residui, non coperti dai presidi di controllo precedenti;
- previsione di specifici protocolli diretti a prevenire i reati, al fine di adeguare il sistema di controllo preventivo.

L'eventuale scostamento da specifici punti delle Linee Guida utilizzate come riferimento non inficia, di per sé, la validità del modello di organizzazione, gestione e controllo adottato dall'ente.

Ogni modello di organizzazione, gestione e controllo, infatti, dovendo essere redatto con riferimento alla realtà concreta dell'ente cui si riferisce, può discostarsi dalle Linee Guida (che, per loro natura, hanno carattere generale), per rispondere maggiormente alle esigenze di prevenzione proprie del Decreto.

2 IL MODELLO DI GOVERNANCE, ASSETTO ISTITUZIONALE E ORGANIZZATIVO DI NTT DATA ITALIA S.P.A.

2.1 NTT DATA Italia S.p.A.



NTT DATA Italia fa parte - dal 2011 - di NTT DATA Group Corporation, 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 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.

NTT DATA Italia esercita altresì, a sua volta, attività di direzione e coordinamento nei confronti di NTT Italia S.p.A. e NTT DATA Italia Gov & Tech S.r.l., entrambe controllate al 100%. In particolare, NTT Italia S.p.A. fornisce prodotti, servizi IT e consulenza tecnologica per vari settori, tra cui telecomunicazioni ed energia e NTT DATA Italia Gov & Tech si occupa di digitalizzazione per il settore pubblico e privato, con focus su PNRR e innovazione.

2.2 Il modello di *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 – mantenendo comunque le caratteristiche di efficacia e trasparenza – a seguito della decisione di rinviare la quotazione in Borsa.

In ogni caso, il sistema di governo adottato dalla Società è conforme alla normativa vigente

ed è in linea con i più autorevoli indirizzi e con le migliori prassi attualmente esistenti in materia. Esso è volto ad assicurare la massima e più equilibrata collaborazione tra le sue componenti attraverso un contemperamento armonico dei diversi ruoli di indirizzo, gestione e controllo.

Tale sistema risulta orientato a garantire una conduzione responsabile dell'impresa e trasparente nei confronti del pubblico e del mercato, nella prospettiva di creazione di valore e del perseguimento di obiettivi di sviluppo sostenibile in favore delle comunità e dell'ambiente in cui NTT DATA Italia opera.

I componenti degli organi aziendali orientano la propria attività ai principi di correttezza ed integrità, astenendosi dall'agire in situazioni di conflitto di interesse nell'ambito dell'attività da loro svolta nella Società. Ai relativi componenti è altresì richiesto un comportamento ispirato ai principi di autonomia, di indipendenza e di rispetto delle linee di indirizzo che la Società fornisce nelle relazioni che essi intrattengono con le Istituzioni Pubbliche e con qualsiasi soggetto privato.

2.2.1 Codice Etico

NTT DATA ha raccolto e descritto all'interno del Codice Etico, approvato e aggiornato nel tempo da parte del competente organo gestorio, i valori comuni a tutti coloro che operano all'interno del Gruppo NTT DATA, così come a tutti i clienti, fornitori, partner, terze parti e stakeholder in genere, che collaborano con la Società.

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

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

2.2.2 *Policy*, procedure e istruzioni

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

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

2.2.3 Sistema di gestione certificato

NTT DATA Italia si è dotata di diversi sistemi di certificazione (tra cui, ISO 9001, ISO 14001, ISO 45001, ISO 27001, ISO 37001, SA 8000, UNI PdR/125), al fine di disciplinare i processi aziendali in conformità agli Standard di riferimento.

Tali certificazioni garantiscono che l'organizzazione operi nel pieno rispetto delle disposizioni vigenti, assicurando il massimo dell'efficacia e dell'efficienza dei processi, delle attività e delle risorse.

In particolare, NTT DATA Italia ha implementato e mantiene attivo un Sistema di Gestione Integrato Qualità, Prevenzione della Corruzione e Ambiente (Sistema di Gestione Integrato).

Il Sistema di Gestione Integrato rappresenta uno strumento strategico per il business aziendale, in grado di generare un effettivo valore aggiunto per l'organizzazione sia in termini economici sia in termini reputazionali e di affidabilità verso l'esterno.

2.2.4 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.

2.2.5 Sostenibilità e sviluppo sostenibile

Il Modello richiama principi etici e comportamentali che traggono origine anche dalle politiche di responsabilità sociale che caratterizzano l'agire di NTT DATA Italia.

In quest'ottica, gli strumenti di compliance si raccordano con le strategie aziendali, promuovendo diversi livelli di responsabilità e un impegno condiviso verso lo sviluppo sostenibile, nel rispetto dei valori protetti dalla Costituzione italiana e dalle Carte Costituzionali europee.

A conferma di tale impegno, NTT DATA Italia ha ottenuto la certificazione ISO 14001, che attesta l'adozione di un sistema di gestione ambientale volto a monitorare e migliorare in modo sistematico, coerente ed efficace gli impatti ambientali dell'organizzazione. Inoltre, la certificazione WELL riflette l'attenzione dell'azienda al benessere e alla salute degli occupanti degli edifici, attraverso parametri che favoriscono ambienti sani, confortevoli e sostenibili.

L'adesione al piano di decarbonizzazione "NTT DATA Net Zero Vision 2040", promosso dal Gruppo NTT DATA, rappresenta un ulteriore passo verso la sostenibilità. Il piano affronta l'impatto ambientale delle tecnologie digitali – hardware, software, servizi cloud e infrastrutture dei data center – e si basa su obiettivi validati dall'iniziativa Science-Based Targets (SBTi), in linea con gli standard NetZero e con i principi dell'Accordo di Parigi, per limitare l'aumento della temperatura globale a 1,5 °C. In tale contesto, NTT DATA Italia si impegna a ridurre del 90% le proprie emissioni di gas serra entro il 2040, attraverso obiettivi di breve, medio e lungo termine.

Fino al 2024, la Società ha redatto annualmente il Bilancio di Sostenibilità, in conformità ai Global Reporting Sustainability Standards, riportando le performance relative all'esercizio fiscale di competenza. A partire da aprile 2024, la rendicontazione è confluita nel Bilancio di Sostenibilità di Gruppo, che include anche il perimetro di NTT DATA Italia, rafforzando ulteriormente l'approccio integrato alla sostenibilità.

2.3 L'assetto istituzionale

La Società adotta un assetto istituzionale "tradizionale" che si caratterizza per la presenza:

- dell'Assemblea dei Soci a cui spettano le deliberazioni secondo quanto previsto dalla Legge e dallo Statuto;
- del Consiglio di Amministrazione (attualmente composto da tre membri: un Presidente del Consiglio di Amministrazione, un Amministratore Delegato e un Consigliere Delegato) incaricato di gestire l'impresa con i più ampi poteri per l'amministrazione ordinaria e straordinaria, esclusi quelli riservati dalla legge o dallo Statuto all'assemblea dei soci;
- del Collegio Sindacale (composto da tre membri effettivi più supplenti, con nomina e funzioni a norma di legge), chiamato a vigilare:
  - ai sensi del Codice Civile, sull'osservanza della legge e dello Statuto e sul rispetto dei principi di corretta amministrazione, ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento;
  - ai sensi del D.Lgs. 39/2010, sull'efficacia dei sistemi di controllo interno, di revisione interna e di gestione del rischio, sull'indipendenza della società di revisione legale, in particolare per quanto concerne la prestazione di servizi diversi dalla revisione;
- della Società di Revisione iscritta nell'albo speciale tenuto dalla Consob a cui è affidata l'attività di revisione legale dei conti ed il giudizio sul bilancio, ai sensi di legge e di Statuto.

I poteri attribuiti agli Organi Societari sono definiti all'interno dello Statuto.

Fermi restando tutti i poteri attribuiti dalla legge e dallo Statuto, ivi inclusa la legale rappresentanza della Società, al Presidente e all'Amministratore Delegato sono attribuiti poteri e rapporti gerarchici con le direzioni/funzioni aziendali, così come disciplinato all'interno della documentazione della Società (in particolare, sistema di procure, organigramma).

Sono stati costituiti Comitati Aziendali e di Gruppo. In particolare, sono attivi:

- un comitato di Executive che affronta temi strategici per lo sviluppo della Società in sede di Business Review, in cui sono definite priorità commerciali ed elaborato il budget annuale, nonché condiviso l'andamento economico alla luce degli obiettivi;
- il Country Leadership Team composto dall'Amministratore Delegato e da tutti i suoi primi riporti, tramite cui viene fornito alle prime linee ogni opportuno aggiornamento relativo alla Società e raccolte eventuali criticità nella gestione di determinati progetti o attività;
- il comitato per la gestione delle violenze e molestie sul lavoro (Funzioni Compliance, H&S, Diversity & Inclusion) con il compito principale di proporre iniziative formative volte alla prevenzione e alla sensibilizzazione sui temi delle violenze e molestie nei luoghi di lavoro, monitorare l'efficacia delle misure adottate dalla Società in materia e fornire supporto nella gestione delle segnalazioni ricevute;

- i comitati ad hoc per le singole opportunità commerciali, istituiti per presidiare e approvare specifiche iniziative strategiche o opportunità commerciali;
- i comitati ad hoc per la gestione di situazioni critiche, istituiti con l'obiettivo di coordinare tempestivamente le attività di risposta in caso di incidenti o eventi critici, valutare l'impatto dell'evento e supportare l'identificazione delle misure correttive e preventive da adottare.

2.4 L'assetto organizzativo

All'interno dell'organizzazione aziendale di NTT DATA Italia sono state identificate le principali Funzioni preposte alla gestione dei sistemi di controllo interno, ciascuna con competenze specifiche.

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.

La governance operativa è affidata all'Amministratore Delegato (CEO), che può interpellare i componenti del Country Leadership Team.

Le funzioni di prima linea includono:

- General Counsel, responsabile della supervisione legale della Società, garantisce la conformità normativa e coordina le attività legali a supporto delle diverse funzioni aziendali;
- Responsabile Corporate Services, a capo delle attività di supporto organizzativo e gestionale della Società;
- Responsabile People & Culture, con il compito di definire e attuare le politiche di gestione delle risorse umane, promuovendo lo sviluppo del capitale umano, la cultura aziendale e il benessere organizzativo;
- Responsabile Marketing & Communications, responsabile della definizione e dell'attuazione delle strategie di comunicazione interna ed esterna, nonché delle attività di marketing e branding;
- Chief Financial Officer (CFO), a capo della Funzione Amministrazione, Finanza e Controllo (Funzione che gestisce e controlla le risorse finanziarie della Società), il quale 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;
- Chief Risk Officer (CRO), il quale è responsabile della gestione del rischio aziendale, ovvero dell'insieme di strategie, processi e strumenti finalizzati all'identificazione, valutazione e mitigazione dei rischi; rispondono direttamente al CRO i diversi responsabili dei mercati in cui opera la Società, ovvero: Energy &Utilities, Financial Services Institutions, Industry, Public & Health, Telco & Media;
- Chief Operating Officer (COO), con il compito di coordinare i diversi settori aziendali affinché operino in modo efficiente e coordinato; rispondono direttamente al COO:

CISO, Data Protection, Delivery Assurance, Quality & Methods, Resource Planning and Technical Training e le diverse aree della Delivery.

Segregazione dei ruoli

La Società adotta, quale principio fondamentale del proprio sistema di controllo interno e di organizzazione, il principio della segregazione dei ruoli ("*segregation of duties*"), che si traduce nella chiara attribuzione, separazione e tracciabilità delle responsabilità, dei poteri decisionali e delle funzioni operative. In particolare, la segregazione dei ruoli è tale da assicurare che le attività non siano mai gestite in autonomia da una sola persona. Le stesse, infatti, vedono una separazione tra Funzioni che autorizzano, che eseguono e che controllano le attività.

I poteri, le deleghe e le procure (v. sotto "*Sistema delle deleghe e delle procure*") sono formalizzati e attribuiti in coerenza con l'organigramma aziendale, le funzioni operative e i livelli autorizzativi, così da garantire che ciascuna funzione operi entro limiti chiari, definiti e documentati. Il sistema è strutturato per assicurare che chi propone o richiede una determinata operazione sia distinto da chi la autorizza, che l'esecuzione sia separata dal controllo, e che le verifiche siano in grado di accertare la conformità dell'operazione, la correttezza delle decisioni assunte e la tracciabilità documentale dell'intero processo.

È inoltre garantita la tracciabilità delle decisioni, degli atti e dei flussi informativi, al fine di consentire una ricostruzione ex post delle responsabilità, delle motivazioni e delle modalità operative, anche in presenza di situazioni potenzialmente a rischio reato. Nei casi in cui, per ragioni organizzative, non sia possibile assicurare una segregazione completa delle funzioni, la Società adotta misure alternative di mitigazione (come la doppia firma, la supervisione da parte di una funzione indipendente o la rotazione dei compiti) al fine di garantire comunque l'efficacia del modello di controllo.

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 e/o procuratori.

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:

- per la gestione delle opportunità commerciali, la firma dei contratti è affidata a procuratori con poteri di spesa crescenti, determinati in base al ruolo ricoperto all'interno della Società;

- è prevista una chiara segregazione dei poteri lato attivo e lato passivo, i poteri lato passivo sono attribuiti esclusivamente alla funzione Procurement;
- si applica il principio del "four eyes", che prevede la separazione tra il soggetto che approva e quello che esegue l'azione;
- le procure speciali vengono rilasciate solo in circostanze eccezionali, previa valutazione specifica;
- 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 da esercitare nel rispetto del Modello Organizzativo e Codice Etico della Società, nonché nel rispetto delle matrici autorizzative di quest'ultima o del relativo Gruppo;
- gli acquisti per importi elevati (soglie indicate negli atti di delega) devono essere autorizzati dall'Amministratore Delegato.

2.5 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 identificato nel Consiglio di Amministrazione, cui spetta pertanto la competenza in merito a successive modifiche e integrazioni del MOG.

I principi base descritti nella Parte Generale del Modello si applicano a NTT DATA Italia e sono condivisi dalle Società controllate; essi devono essere rispettati in tutte le attività aziendali svolte sia in Italia sia all'estero. I Modelli di organizzazione, gestione e controllo delle Società controllate si ispirano infatti agli stessi valori e agli stessi principi generali di seguito descritti.

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

Sono destinatari del presente documento tutti coloro che operano per il conseguimento dello scopo e degli obiettivi di NTT DATA Italia, in particolare, come specificato nelle "Definizioni" che precedono.

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 nel 2002 e da ultimo aggiornato nel 2021.

Questo documento è stato redatto con l'intento di supportare la comprensione del sistema organizzativo, di gestione e controllo della Società attraverso un framework di riferimento che evidenzi anche dove siano reperibili le informazioni più aggiornate sulle scelte e sugli strumenti in essere. Per questo motivo, spesso, contiene rinvii ad altri documenti aziendali (ad esempio: **All. 2** in cui è presente l'elenco delle policy, procedure, linee guida ed istruzioni operative adottate dalla Società e che potrebbe essere nel tempo integrato e modificato).

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

3 MAPPATURA DEI RISCHI

La metodologia scelta dalla Società per l'aggiornamento del Modello, in termini di organizzazione, definizione delle modalità operative e strutturazione in fasi, è stata elaborata al fine di rispettare quanto delineato dalle best practices esistenti in materia e, comunque, tenendo in considerazione quanto previsto dalle linee guida applicabili.

Il Progetto si è articolato nelle fasi di seguito riportate:

Fase 1) – Analisi documentale e interviste

Raccolta ed analisi della documentazione rilevante; rilevazione delle attività sensibili; realizzazione delle interviste ai referenti individuati.

***Fase 2) - Gap analysis ed Action plan*:**

Analisi delle attività sensibili rilevate e dell'ambiente di controllo con riferimento ad un modello di organizzazione, gestione e controllo "a tendere" conforme a quanto previsto dal D.Lgs. 231/2001; predisposizione di una sintesi delle differenze tra protocolli di controllo esistenti e modello di organizzazione, gestione e controllo "a tendere" (c.d. Gap analysis); individuazione delle proposte di adeguamento e delle azioni di miglioramento; condivisione del documento con i referenti individuati e l'Amministratore Delegato.

In particolare, il documento di Gap analysis è finalizzato a rilevare gli standard di controllo che devono essere necessariamente rispettati per consentire alla Società di instaurare un'organizzazione volta ad evitare la commissione di reati. Gli standard di controllo sono fondati sui seguenti principi generali che devono essere rispettati nell'ambito di ogni attività sensibile individuata:

- Esistenza di procedure/linee guida formalizzate: esistenza di regole formali o prassi consolidate idonee a fornire principi di comportamento e modalità operative per lo svolgimento delle attività sensibili;
- Tracciabilità e verificabilità ex post delle transazioni tramite adeguati supporti documentali/informativi: verificabilità ex post del processo di decisione, autorizzazione e svolgimento dell'attività sensibile, anche tramite apposite evidenze archiviate;
- Segregazione dei compiti e ruoli: ripartizione delle attività poste in essere dalle varie funzioni tra chi esegue, chi autorizza e chi controlla, in modo tale che nessuno possa gestire in autonomia l'intero svolgimento di un processo;
- Esistenza di un sistema di deleghe coerente con le responsabilità organizzative assegnate: formalizzazione di poteri di firma e di rappresentanza coerenti con le responsabilità organizzative nonché chiaramente definiti e conosciuti all'interno della Società.

In aggiunta, sono stati definiti principi di controllo specifici, ossia regole di comportamento (eventualmente anche sotto forma di divieti) che tutti coloro che sono coinvolti nelle attività della Società devono seguire.

Il documento di Gap analysis include, altresì, un Action plan, contenente le misure da implementare per l'adeguamento dei sistemi di controllo a fronte dei dati raccolti e dei gap rilevati.

Fase 3) - Risk Assessment

Alla luce delle informazioni raccolte, valutazione in merito al potenziale rischio di commissione dei reati richiamati dal D.Lgs. 231/2001 associati a ciascuna attività sensibile rilevata (c.d. rischio inerente).

La valutazione del livello di esposizione al c.d. rischio inerente è stata effettuata secondo la tabella che segue, considerando congiuntamente:

- incidenza attività: valutazione della frequenza e/o della rilevanza economica dell'attività;
- rischio astratto di reato: valutazione circa la possibilità, in astratto, di condotte illecite nell'interesse o a vantaggio dell'ente.

Valutazione del rischio inerente all'attività			
	Rischio astratto reato		
Incidenza Attività	**Alto**	**Medio**	**Basso**
Basso	*Medio*	*Basso*	*Basso*
Medio	*Medio*	*Medio*	*Basso*
Alto	*Alto*	*Alto*	*Medio*

Alla luce dei principi di controllo generici e specifici presenti alla data delle interviste nella Società, è stata effettuata una rivalutazione del rischio dei reati associabili alla presente attività sensibile (c.d. rischio residuo), secondo la tabella che segue:

Valutazione del rischio residuo dell'attività			
	Livello di compliance alla data della gap analysis, action plan e risk assessment		
Rischio inerente all'attività	**Alto**	**Medio**	**Basso**
Basso	*Basso*	*Basso*	*Medio*
Medio	*Basso*	*Medio*	*Alto*
Alto	*Medio*	*Alto*	*Alto*

Fase 4) - Definizione del Modello e attività successive

Predisposizione della bozza del Modello; condivisione della bozza predisposta con l'Amministratore Delegato; approvazione del Modello da parte del Consiglio di Amministrazione.

Le stesse fasi di progetto, in quanto applicabili, saranno poste in essere in occasione degli ulteriori aggiornamenti del Modello.

4 (SUB) FATTORI RILEVANTI PER L'AGGIORNAMENTO DEL MODELLO

Il Consiglio di Amministrazione, dopo aver consultato l'Organismo di Vigilanza, determina gli aggiornamenti del Modello ed il suo adeguamento in conseguenza di:

- modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività;
- cambiamenti delle aree di *business*;
- notizie di tentativi o di commissione dei reati considerati dal Modello;
- notizie di nuove possibili modalità di commissione dei reati considerati dal Modello;
- modifiche normative;
- risultanze dei controlli;
- significative violazioni delle prescrizioni del Modello.

Il Modello è, in ogni caso, sottoposto a procedimento di revisione periodica e, comunque, tutte le volte intervengano modifiche legislative e/o organizzative che necessitino un tempestivo intervento di modifica.

L'Organismo di Vigilanza viene informato tempestivamente in merito a qualsiasi modifica del Modello.

5 ORGANISMO DI VIGILANZA

Come sopra anticipato, in ottemperanza all'art. 6, comma 1, lett. a) e b) D.Lgs. 231/2001, l'ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti qualificati ex art. 5 D.Lgs. 231/2001, se l'organo dirigente ha, fra l'altro:

- adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e l'osservanza del modello di cui al punto precedente e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

L'affidamento dei suddetti compiti ad un organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi rappresentano, quindi, presupposti indispensabili per l'esonero dalla responsabilità prevista dal D.Lgs. 231/2001.

I requisiti principali dell'Organismo di Vigilanza, così come proposti dalle Linee Guida per la predisposizione dei modelli di organizzazione, gestione e controllo emanate da Confindustria, possono essere così identificati:

- autonomia e indipendenza: l'Organismo di Vigilanza si inserisce come unità di *staff* in massima posizione gerarchica con riporto diretto al massimo vertice dell'ente ed è privo di poteri decisionali ed operativi in merito all'attività aziendale;
- professionalità: l'OdV deve possedere specifiche competenze in ambito giuridico, economico, nell'ambito delle tecniche di analisi e di valutazione dei rischi;
- continuità di azione: la continuità di azione ha la finalità di garantire il costante controllo dell'efficace, effettiva e costante attuazione del Modello adottato dalla Società ai sensi D.Lgs. 231/2001.

5.1 Nomina, composizione e durata della carica dell'Organismo di NTT DATA Italia

L'Organismo di Vigilanza è nominato mediante delibera del Consiglio di Amministrazione, che assegna altresì un *budget* annuale affinché l'OdV possa svolgere le attività prescritte dal D. Lgs. 231/2001 quali, a titolo meramente esemplificativo e non esaustivo: analisi e verifiche, valutazione dei rischi, consulenze specialistiche.

Il *budget* permette all'Organismo di operare in autonomia e indipendenza e con gli strumenti opportuni per un efficace espletamento del compito assegnatogli dal presente Modello, secondo quanto previsto dal D. Lgs. 231/2001. In caso di necessità, l'OdV può richiedere integrazioni dell'importo assegnatogli.

Il Consiglio di Amministrazione della Società ha nominato un Organismo collegiale, composto da tre membri effettivi, dei quali uno con funzioni di Presidente. L'organo collegiale si compone come segue:

- due professionisti esterni con competenze in ambito giuridico, nonché nell'ambito delle tecniche di analisi e di valutazione dei rischi;
- un membro interno appartenente al Gruppo NTT DATA, non coinvolto in attività produttive o gestionali.

L'Organismo di Vigilanza della Società resta in carica per tre anni dalla nomina, salvo diversa decisione del Consiglio di Amministrazione, ed è rieleggibile. Lo stesso cessa per decorrenza del termine del periodo stabilito in sede di nomina, pur continuando a svolgere *ad interim* le proprie funzioni fino a nuova nomina dell'Organismo stesso.

Se, nel corso della carica, l'OdV cessa dal suo incarico, il Consiglio di Amministrazione provvede alla sostituzione.

Il compenso per il ruolo di componente dell'Organismo di Vigilanza è stabilito, per tutta la durata del mandato, dal Consiglio di Amministrazione.

5.2 Requisiti soggettivi dei componenti

Ogni componente dell'Organismo di Vigilanza deve possedere i requisiti di onorabilità[5], assenza di conflitto d'interessi, assenza di relazioni di parentela e/o di affari, ecc.

In particolare, i componenti dell'Organismo di Vigilanza non devono:

- avere relazioni di coniugio, parentela, affinità entro il quarto grado con gli Amministratori;
- essere titolari, direttamente o indirettamente, di quote della Società o delle controllate di entità tale da permettere di esercitare una notevole influenza sulla stessa;
- essere stati condannati con sentenza, anche di primo grado, per i delitti richiamati dal Decreto od altri delitti comunque incidenti sulla moralità professionale, salvo il caso di avvenuta estinzione del reato o della pena o in presenza di requisiti per l'ottenimento della riabilitazione.

Inoltre, la carica di membro dell'OdV non può essere ricoperta da coloro che:

- si trovino in una delle cause di ineleggibilità o decadenza previste dall'art. 2382 c.c.;
- abbiano incarichi all'interno o per conto della Società di natura o consistenza tale da limitare la più ampia indipendenza di giudizio.

5.3 Decadenza e revoca dalla carica

Il verificarsi - in data successiva all'intervenuta nomina - di una delle condizioni di cui sopra, relative all'indipendenza, autonomia ed onorabilità ostative alla nomina, comporta l'incompatibilità rispetto alla permanenza in carica e la conseguente decadenza automatica. Il sopravvenire di una delle cause di decadenza deve essere tempestivamente comunicato al Consiglio di Amministrazione da parte dell'interessato.

Costituiscono, invece, motivi di revoca per giusta causa dalla carica di componente dell'Organismo di Vigilanza:

- omessa partecipazione, non giustificata, a due riunioni dell'OdV regolarmente convocate per singolo anno o a quattro riunioni per tutti gli anni di mandato;
- inadempimento ai compiti delegati;
- grave negligenza nell'assolvimento dei compiti connessi all'incarico quale, a titolo meramente esemplificativo: l'omessa redazione della relazione informativa periodica; l'omessa segnalazione di violazioni accertate del Modello, con presunta commissione di reati;

5 Le persone fisiche sono in possesso dei requisiti di onorabilità se rispettano, congiuntamente, le seguenti condizioni: a) non si trovino in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese; b) non siano state sottoposte a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423 o della legge 31 maggio 1965, n. 575, e successive modificazioni ed integrazioni, salvi gli effetti della riabilitazione; c) non siano state condannate con sentenza irrevocabile, salvi gli effetti della riabilitazione, ad una delle seguenti pene: reclusione per un tempo superiore a sei mesi per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati, valori mobiliari e strumenti di pagamento, nonché per i reati previsti dal decreto legislativo 27 gennaio 2010, n. 39; reclusione per un tempo superiore a sei mesi per uno dei delitti previsti nel titolo XI del libro V del codice civile; reclusione per un tempo superiore ad un anno per un delitto contro la pubblica Amministrazione, contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria; reclusione per un tempo superiore a due anni per qualunque delitto non colposo; d) non abbiano riportato in Stati esteri condanne penali o altri provvedimenti sanzionatori per fattispecie e durata corrispondenti a quelle che comporterebbero, secondo la legge italiana, la perdita dei requisiti di onorabilità.

- omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza – secondo quanto previsto dall'art. 6, comma 1, lett. d), D. Lgs. 231/2001 – risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti della Società ai sensi del D.Lgs. 231/2001 ovvero da provvedimento che comunque ne accerti la responsabilità.

5.4 Funzioni e poteri

Le attività poste in essere dall'Organismo di Vigilanza non possono essere sindacate da alcun altro organismo o struttura della Società, posto però che il Consiglio di Amministrazione è chiamato a vigilare sull'adeguatezza del suo operato, in quanto lo stesso ha la responsabilità ultima del funzionamento e dell'efficacia del Modello.

Per lo svolgimento delle proprie attività, l'Organismo di Vigilanza adotta un Regolamento di funzionamento interno in cui definisce le proprie modalità operative.

L'OdV ha poteri di iniziativa e controllo necessari per assicurare un'effettiva ed efficiente vigilanza sul funzionamento e sull'osservanza del Modello secondo quanto stabilito dall'art. 6 del D.Lgs. 231/2001.

In particolare, l'Organismo di Vigilanza verifica:

- il funzionamento del Modello e l'osservanza delle prescrizioni in questo contenute da parte di tutti i destinatari;
- la reale efficacia e capacità del Modello di prevenire la commissione dei reati richiamati dal D.Lgs. 231/2001;
- l'opportunità di aggiornare il Modello, laddove vengano riscontrate esigenze di adeguamento dello stesso in relazione a modifiche organizzative o a novità normative.

A tale fine, l'Organismo di Vigilanza può svolgere, direttamente o tramite propri incaricati, verifiche su ogni atto, informazione, dato, anche contabile, procedure della Società, ritenuti utili.

Per garantire una vigilanza quanto più efficace possibile sul funzionamento e il rispetto del Modello, rientrano fra i compiti dell'OdV, a titolo meramente esemplificativo e non tassativo:

- attivare un piano di verifica volto ad accertare la concreta attuazione del Modello da parte di tutti i Destinatari;
- monitorare la necessità di un aggiornamento della mappatura dei rischi e del Modello, in caso di significative variazioni organizzative o di estensione della tipologia di reati presi in considerazione dal D.Lgs. 231/2001, informandone il Consiglio di Amministrazione;
- eseguire periodicamente verifiche mirate su determinate operazioni o atti specifici posti in essere nell'ambito delle aree di rischio;
- monitorare le iniziative di informazione/formazione finalizzate alla diffusione della conoscenza e della comprensione del Modello nella Società;
- analizzare le informazioni rilevanti (comprese le eventuali segnalazioni) in ordine al rispetto del Modello;

- convocare le funzioni aziendali per un migliore monitoraggio delle aree a rischio;
- condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del Modello;
- segnalare prontamente ogni criticità relativa all'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto, proponendo le opportune soluzioni operative;
- segnalare al Consiglio di Amministrazione eventuali violazioni di regole contenute nel Modello o le carenze rilevate in occasione delle verifiche svolte, affinché questi possa adottare i necessari interventi di adeguamento;
- vigilare sull'applicazione coerente delle sanzioni previste dalle normative interne nei casi di violazione del Modello, ferma restando la competenza dei Procuratori per l'applicazione dei provvedimenti sanzionatori;
- rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni.

5.5 Regole di condotta

L'attività dell'OdV deve essere improntata ai principi di integrità, obiettività, riservatezza. Tali regole di condotta possono esplicarsi nei termini che seguono:

- integrità: l'OdV deve operare con onestà, diligenza e senso di responsabilità;
- obiettività: l'OdV non deve partecipare ad alcuna attività che possa pregiudicare l'imparzialità della propria valutazione. Deve riportare tutti i fatti significativi di cui sia venuto a conoscenza e la cui omissione possa dare un quadro alterato e/o incompleto delle attività analizzate;
- riservatezza: i componenti dell'OdV devono esercitare tutte le opportune cautele nell'uso e nella protezione delle informazioni acquisite. L'OdV non deve usare le informazioni ottenute né per vantaggio personale né secondo modalità che siano contrarie alla Legge. Tutti i dati di cui sia titolare la Società devono essere trattati nel pieno rispetto delle disposizioni di cui al D.Lgs. 196/2003 e s.m.i. e al Regolamento Europeo n. 2016/679 (di seguito, il "GDPR"), nonché in linea con quanto previsto dall'atto di nomina a soggetto autorizzato al trattamento che la Società conferisce a ciascun componente dell'OdV, per adeguarsi a quanto affermato dall'Autorità Garante per la protezione dei dati personali nel "*Parere sulla qualificazione soggettiva ai fini privacy degli Organismo di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231*" del 21 maggio 2020.

5.6 Obblighi di informazione nei confronti dell'Organismo di Vigilanza

La trasmissione di informazioni all'Organismo di Vigilanza è un ulteriore strumento per agevolare l'attività di vigilanza sull'efficacia del Modello.

L'OdV è contattabile al seguente indirizzo *e-mail*: **odv@emeal.nttdata.com**.

In ogni caso, l'Organismo di Vigilanza approva uno schema di flussi informativi, che deve essere compilato e inviato dalle funzioni aziendali responsabili delle attività sensibili e che deve tenere conto: ***a)*** delle risultanze periodiche dell'attività di controllo poste in essere

(report riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.); ***b)*** delle 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, cfr. All. 5**) o ad evento (**flussi informativi straordinari**).

In particolare, i flussi informativi straordinari devono essere obbligatoriamente e tempestivamente trasmessi all'OdV, a prescindere dalla periodicità programmata, al verificarsi di situazioni e/o eventi particolari o determinati che possano avere rilevanza ai fini della efficace attuazione del Modello organizzativo e delle misure di prevenzione in esso previste.

L'eventuale omessa o ritardata comunicazione all'OdV dei flussi informativi 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.

5.7 Segnalazione di reati, violazioni o irregolarità (cd. *whistleblowing*)

La Società, in linea con quanto previsto dal D.Lgs. 24/2023, recante "*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*", ha implementato un sistema che consente la possibilità di segnalare atti o fatti che possano costituire violazioni del D.Lgs. 231/2001 e del Modello non riconducibili alle violazioni del diritto dell'UE definite nell'art. 2, comma 1 lett. a) nn. 3-6) del suddetto decreto[6].

[6] L'art. 2, comma 1, lett. a) nn. 2-6):
"*1. Ai fini del presente decreto, si intendono per:*
a) «violazioni»: comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:
1) (omissis);
2) condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazioni dei modelli di organizzazione e gestione ivi previsti, che non rientrano nei numeri 3), 4), 5) e 6);
3) illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al presente decreto ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato al presente decreto, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
4) atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;
5) atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
6) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei numeri 3), 4) e 5)".

Tale sistema garantisce la riservatezza e la protezione dell'identità del soggetto che effettua la segnalazione, dei facilitatori[7] e del soggetto eventualmente segnalato.

Infine, consente che le segnalazioni siano ricevute, esaminate e valutate attraverso canali di segnalazione specifici, autonomi e indipendenti che differiscono dalle ordinarie linee di *reporting*[8].

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

- la possibilità di segnalare le violazioni – cioè comportamenti, atti od omissioni che ledono l'interesse dell'ente – che si ritiene siano state commesse, tra cui rientrano: (*i*) gli illeciti amministrativi, contabili, civili e penali e (*ii*) le condotte illecite rilevanti ai sensi del Decreto 231, o violazioni dei modelli di organizzazione e gestione;
- l'individuazione di una persona, di un ufficio interno autonomo dedicato o di un soggetto esterno e autonomo per la gestione del canale di segnalazione;
- l'individuazione di specifici canali, anche informatici, di segnalazione interna delle violazioni, in forma scritta e/o orale;
- la riservatezza e la confidenzialità delle informazioni ricevute e la protezione dei dati personali del segnalante e del segnalato;
- precise tempistiche per l'avvio, lo svolgimento e la conclusione dell'attività istruttoria effettuata dal soggetto che gestisce la segnalazione;
- il divieto di ritorsioni nei confronti del segnalante, cioè di qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, che provoca o può provocare alla persona segnalante, in via diretta o indiretta, un danno ingiusto;
- la nullità degli atti di ritorsione eventualmente posti in essere nei confronti del segnalante;
- la previsione di sanzioni disciplinari: (*i*) per coloro che violino la riservatezza del segnalante; (*ii*) per coloro che inviino, con dolo o colpa grave, segnalazioni infondate (*iii*) nel caso di commissione di una ritorsione nei confronti del segnalante e (*iv*) nel caso in cui la segnalazione sia stata ostacolata o vi sia stato il tentativo di ostacolarla.

La Società ha implementato una **procedura specifica per le segnalazioni del *whistleblower* ai sensi del D. Lgs. 24/2023**, pubblicata sulla intranet aziendale e disponibile per tutti i dipendenti e alla quale si rinvia integralmente. Tale procedura costituisce parte integrante del Modello 231.

La Procedura, in particolare, disciplina le modalità e i canali di trasmissione delle segnalazioni, le quali devono essere trasmesse attraverso l'apposito canale rappresentato

---

[7] Ai sensi dell'art. 2, comma 1 let. h) il facilitatore è definito come segue: "*una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata*".

[8] In particolare, il comma 2 *bis* dell'articolo 6 D.Lgs. 231/2001 prevede per le società l'obbligo di adottare sistemi interni di segnalazione delle violazioni, ossia di procedure specifiche che permettano al personale delle società di dar nota della presenza di atti o fatti che possono costituire violazioni potenziali o effettive garantendo tutte le tutele di cui al D.Lgs. 24/2023. Nello specifico: "*2-bis. I modelli di cui al comma 1, lettera a), prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e)*".

dalla **Piattaforma SpeakUp**, uno strumento che garantisce l'anonimato e la riservatezza e che consente di effettuare le segnalazioni in forma scritta o in forma orale.

L'applicativo garantisce, anche attraverso il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

L'organo deputato alla ricezione e alla gestione delle segnalazioni è un Comitato autonomo (il "Comitato Segnalazioni"), i cui componenti sono individuati nella Procedura, a cui vengono attribuite le seguenti funzioni:

- rilasciare alla persona segnalante un avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione;
- mantenere le interlocuzioni con la persona segnalante e richiede a quest'ultima, se necessario, integrazioni;
- dare diligentemente seguito alle segnalazioni ricevute;
- fornire riscontro alla segnalazione entro 3 mesi dall'avviso di ricevimento o, in mancanza di tale avviso, entro 3 mesi dalla scadenza del termine di 7 giorni dalla presentazione della segnalazione;
- dare informativa in merito al canale di segnalazione, alle modalità e ai presupposti per effettuare le segnalazioni, rendendo tali informazioni facilmente visibili: i) nei luoghi di lavoro nonché accessibili alle persone che, pur non frequentando i luoghi di lavoro, intrattengono un rapporto giuridico con la Società, ii) in una sezione del sito internet della Società.

La Società, al fine di incentivare l'uso dei sistemi interni di segnalazione e di favorire la diffusione di una cultura della legalità, illustra al proprio personale dipendente e ai propri collaboratori in maniera chiara, precisa e completa il procedimento di segnalazione interno adottato.

La Società assicura la puntuale informazione di tutto il personale dipendente e dei soggetti che con la stessa collaborano, non soltanto in relazione alle modalità di segnalazione adottate, ma anche con riferimento alla conoscenza, comprensione e diffusione degli obiettivi e dello spirito con cui la segnalazione deve essere effettuata.

Almeno una volta all'anno, l'Organismo di Vigilanza recepisce una relazione del Comitato.

5.8 Verifiche periodiche e report dell'OdV

L'Organismo di Vigilanza riferisce in merito all'efficacia e osservanza del Modello, all'emersione di eventuali aspetti critici, alla necessità di interventi modificativi. A tal fine, l'Organismo di Vigilanza predispone:

- con cadenza annuale una relazione informativa, relativa all'attività svolta, da presentare al Consiglio di Amministrazione;
- immediatamente, al verificarsi di violazioni accertate del Modello, con presunta commissione di reati, una comunicazione da presentare al Consiglio di Amministrazione.

Nell'ambito del reporting annuale vengono affrontati, tra gli altri, i seguenti aspetti:

- controlli e verifiche svolti dall'Organismo di Vigilanza ed esito degli stessi;
- eventuali innovazioni legislative o modifiche organizzative che richiedono aggiornamenti;
- eventuali sanzioni disciplinari irrogate a seguito di violazioni del Modello;
- altre informazioni ritenute significative;
- valutazione di sintesi sull'adeguatezza del Modello rispetto alle previsioni del D.Lgs. 231/2001.

Gli incontri con gli organi della Società cui l'Organismo di Vigilanza riferisce sono documentati. L'OdV cura l'archiviazione della relativa documentazione.

5.9 Raccolta e conservazione delle informazioni

Ogni informazione in possesso dell'OdV è trattata in conformità al D.Lgs. 196/2003 e s.m.i. e al GDPR.

A tal proposito, in forza del parere espresso dall'Autorità Garante per la Protezione dei Dati Personali in data 12 maggio 2020 circa la qualificazione soggettiva ai fini privacy dei componenti dell'Organismo di Vigilanza, in ragione del trattamento dei dati personali che l'esercizio dei compiti e delle funzioni affidate all'OdV comporta, la Società – nell'ambito delle misure organizzative da porre in essere in attuazione del principio di accountability – in qualità del Titolare del Trattamento (art. 24 del GDPR) designa ogni componente dell'OdV quale soggetto autorizzato al trattamento dei dati personali (artt. 29 GDPR ed art. 2 quaterdecies D.Lgs. 196/2003).

Tutte le informazioni, la documentazione, ivi compresa la reportistica prevista dal Modello, e le segnalazioni raccolte dall'Organismo di Vigilanza – e allo stesso pervenute - nell'espletamento dei propri compiti istituzionali, vengono custodite a cura della Funzione *Legal* in un apposito *database* informatico, in ottemperanza ai principi di cui all'art. 5 del GDPR, per il tempo necessario rispetto agli scopi per i quali è stato effettuato il trattamento e comunque per un periodo non superiore a dieci anni.

5.10 Rapporti con gli organismi di vigilanza delle società controllate

Al fine di esaminare e condividere le esperienze significative maturate nel corso della propria attività di vigilanza, l'Organismo di Vigilanza della Società promuove un incontro periodico con gli organismi di vigilanza delle altre società del Gruppo.

In tale occasione, gli Organismi si scambiano reciprocamente le informazioni eventualmente utili rispetto ad eventi o circostanze rilevanti per lo svolgimento delle attività di competenza degli stessi.

6 DIFFUSIONE DEL MODELLO. FORMAZIONE E INFORMAZIONE

6.1 Modalità operative

6.1.1 Comunicazione ai componenti degli organi sociali

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

6.1.2 Comunicazione e formazione del personale

Pur in mancanza di una specifica previsione all'interno del D.Lgs. 231/2001, le Linee Guida sulla predisposizione dei modelli di organizzazione, gestione e controllo, precisano che la comunicazione al personale e la sua formazione sono due fondamentali requisiti del Modello ai fini del suo corretto funzionamento.

Infatti, al fine di dotare il Modello della massima efficacia, la Società assicura una corretta divulgazione dei contenuti e dei principi dello stesso sia all'interno che all'esterno della propria organizzazione.

Il personale è tenuto a: i) acquisire consapevolezza del D.Lgs. 231/2001 e dei contenuti del Modello messi a sua disposizione; ii) conoscere le modalità operative con le quali deve essere realizzata la propria attività.

L'attività di comunicazione e formazione è diversificata a seconda dei destinatari cui essa si rivolge, ma è, in ogni caso, improntata a principi di tempestività, efficienza (completezza, chiarezza, accessibilità) e continuità, al fine di consentire ai diversi destinatari la piena consapevolezza delle disposizioni che sono tenuti a rispettare e delle norme etiche che devono ispirare i loro comportamenti.

La possibilità di accedere e consultare la documentazione costituente il Modello, i protocolli di controllo e le procedure ad esso riferibili è garantita a tutto il personale dipendente, in quanto tutti i sopracitati documenti sono pubblicati sulla *intranet* aziendale.

Inoltre, al fine di agevolare la comprensione del Modello, il personale, con modalità diversificate secondo il grado di coinvolgimento nelle attività sensibili ai sensi del D.Lgs. 231/2001, è tenuto a partecipare alle specifiche attività formative promosse dalla Società.

La Società provvede ad adottare idonei strumenti di comunicazione per aggiornare il personale circa le eventuali modifiche apportate al presente Modello, nonché ogni rilevante cambiamento procedurale, normativo o organizzativo.

La partecipazione ai programmi di formazione è obbligatoria per il personale ed è gestita dalla Funzione People & Culture in stretta collaborazione con la funzione *Compliance*, nonché in condivisione con l'Organismo di Vigilanza.

6.2 Comunicazione ai terzi/collaboratori esterni

L'impegno al rispetto dei principi di riferimento del Modello 231 da parte dei terzi aventi rapporti contrattuali con NTT DATA Italia è previsto da apposita clausola contrattuale, che richiede il rispetto delle previsioni di cui al D.Lgs. 231/2001, nonché dei principi indicati nella Parte Generale del Modello e nel Codice Etico (cfr. entrambi i documenti sono

pubblicati sul sito *internet* della Società).

In particolare, 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, devono conoscere quanto previsto dal D. Lgs. 231/2001 e, ove tenuti, dichiarare di aver adottato il Modello 231 o, quanto meno, procedure idonee ad evitare in alcun modo il coinvolgimento di NTT DATA Italia in caso di commissione dei reati previsti dalla predetta normativa.

7 SISTEMA DISCIPLINARE E SANZIONATORIO

7.1 Principi generali e criteri di irrogazione delle sanzioni

L'art. 6, comma 2, lett. e) e l'art. 7, comma 4, lett. b) del D. Lgs. 231/2001 indicano, quale condizione per un'efficace attuazione del Modello di organizzazione, gestione e controllo, l'implementazione di un sistema idoneo a sanzionare il mancato rispetto delle misure indicate nel modello stesso.

Pertanto, la definizione di un adeguato sistema disciplinare e sanzionatorio, con sanzioni proporzionate alla gravità della violazione rispetto alle infrazioni delle regole di cui al presente Modello da parte dei Destinatari, costituisce un presupposto essenziale per l'efficacia del modello di organizzazione, gestione e controllo ai sensi del D. Lgs. 231/2001.

Tale sistema disciplinare e sanzionatorio si rivolge tanto al personale quanto ai terzi che operano per conto della Società, prevedendo idonee sanzioni di carattere disciplinare in un caso e di carattere contrattuale/negoziale (ad es. risoluzione del contratto, cancellazione dall'elenco fornitori, ecc.) nell'altro caso.

Con particolare riguardo ai lavoratori dipendenti, il sistema disciplinare rispetta i limiti connessi al potere sanzionatorio imposti dall'art. 7 della Legge n. 300 del 1970 (c.d. "Statuto dei lavoratori"), dal "Contratto Collettivo Nazionale Metalmeccanici" e dal "Contratto Collettivo Nazionale Terziario, Distribuzione e Servizi" (in generale, "CCNL applicabile"), sia per quanto riguarda le sanzioni irrogabili sia per quanto riguarda le forme di esercizio del potere sanzionatorio.

In ogni caso, l'applicazione delle sanzioni prescinde dall'avvio o dall'esito di un eventuale procedimento penale, in quanto i modelli di organizzazione e le procedure interne costituiscono regole vincolanti per i Destinatari, la violazione delle quali deve, al fine di ottemperare ai dettami del Decreto, essere sanzionata indipendentemente dall'effettiva realizzazione di un reato o dalla punibilità dello stesso.

7.2 Violazioni del sistema whistleblowing

Il mancato rispetto della "*SpeakUp & Whistleblowing Policy*" e del relativo "*Addendum Whistleblowing per le Società italiane*" comporta l'applicazione del presente sistema disciplinare e sanzionatorio.

In particolare, la Società intraprenderà ogni più opportuna azione disciplinare o sanzionatoria nei confronti di:

- tutti i soggetti che ostacolino o tentino di ostacolare le segnalazioni *whistleblowing*;

- chi approfondisce le segnalazioni: (i) quando non è stata svolta l'attività di verifica ed analisi delle segnalazioni ricevute; (ii) quando violi l'obbligo di riservatezza dell'identità del segnalante e di qualsiasi altra informazione di cui alle segnalazioni su indicate;
- tutti i soggetti segnalanti, nel caso in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per il reato di diffamazione commesso con la segnalazione o per i reati di calunnia o di diffamazione commessi con la denuncia all'autorità giudiziaria o contabile o qualora sia accertata la responsabilità civile del segnalante per comportamenti riconducibili ai reati sopra indicati in caso di dolo o colpa grave.

Al fine di promuovere l'efficacia dei canali di segnalazione *whistleblowing* di cui al paragrafo 5.7 del Modello, la Società pone il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante e delle altre persone a cui si estende la medesima tutela (ad es., facilitatore) per motivi che siano collegati, direttamente o indirettamente, alla segnalazione stessa e prevede sanzioni nei confronti di chi viola tali misure.

A titolo esemplificativo e non esaustivo, costituiscono ritorsioni, se intervengono in occasione o a causa della segnalazione:

a. il licenziamento, la sospensione o misure equivalenti;
b. la retrocessione di grado o la mancata promozione;
c. il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
d. la sospensione della formazione o qualsiasi restrizione all'accesso alla stessa;
e. le note di merito negative o le referenze negative;
f. l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
g. la coercizione, l'intimidazione, le molestie o l'ostracismo;
h. la discriminazione o comunque il trattamento sfavorevole;
i. la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
j. il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
k. i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
l. l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore nell'industria in futuro;
m. la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
n. l'annullamento di un permesso.

7.3 Procedimento disciplinare

L'irrogazione della sanzione disciplinare rappresenta l'ultima fase di un procedimento i cui tempi e modalità sono stabiliti dalla normativa vigente e dal CCNL applicabile. Tale procedimento disciplinare, avviato dal datore di lavoro o da altro Procuratore a ciò abilitato, nei confronti del dipendente che abbia violato le misure previste dal Modello, si articola nelle seguenti fasi:

1. contestazione disciplinare con cui il datore di lavoro o un altro Procuratore a ciò abilitato contesta tempestivamente al dipendente il comportamento tenuto che si considera infrazione. La contestazione deve indicare, tra le altre cose, anche il termine concesso al dipendente entro il quale presentare le proprie giustificazioni (termine non inferiore ai giorni prescritti da CCNL applicabile);
2. eventuale formulazione delle giustificazioni da parte del dipendente in forma scritta o tramite audizione orale;
3. valutazione da parte del datore di lavoro o di altro Procuratore a ciò abilitato delle eventuali giustificazioni presentate dal dipendente;
4. eventuale comminazione della sanzione disciplinare.

La Funzione People & Culture comunica l'irrogazione della sanzione all'Organismo di Vigilanza. Il sistema disciplinare viene costantemente monitorato dall'OdV e dalla Funzione People & Culture.

7.4 Sanzioni

7.4.1 Misure nei confronti dei lavoratori dipendenti non dirigenti (Quadri – Impiegati)

Ai sensi del combinato disposto degli artt. 5 lett. b) e 7 del D. Lgs. 231/2001, ferma la preventiva contestazione e la procedura prescritta dall'art. 7 della Legge 20 maggio 1970 n. 300 (c.d. Statuto dei Lavoratori), per i lavoratori dipendenti non dirigenti, il sistema disciplinare applicato è regolato dal CCNL Metalmeccanici.

Il mancato rispetto e/o la violazione delle singole disposizioni e regole comportamentali di cui al Modello, al Codice Etico e alle prassi esistenti nella Società da parte dei dipendenti costituisce illecito disciplinare e inadempimento alle obbligazioni derivanti dal rapporto di lavoro. Pertanto, possono essere comminate le sanzioni – modulate anche a seconda della gravità della violazione e tenuto conto dell'eventuale recidiva – previste dalla normativa vigente e dal CCNL di cui sopra.

Conformemente all'art. 7 dello Statuto dei Lavoratori e alle previsioni del CCNL, le disposizioni in materia di sanzioni disciplinari devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti.

L'accertamento delle suddette infrazioni, eventualmente su segnalazione dell'Organismo di Vigilanza, la gestione dei procedimenti disciplinari e l'irrogazione delle sanzioni restano di competenza del datore di lavoro o di altro Procuratore a ciò abilitato.

La Società, nella determinazione dei piani premianti, può definire degli obiettivi collegati al rispetto del presente Modello e delle regole ivi richiamate.

7.4.2 Misure nei confronti dei Dirigenti

Ai lavoratori dirigenti sono applicabili il CCNL Metalmeccanici e il CCNL Terziario, Distribuzione e Servizi.

In considerazione del particolare rapporto fiduciario con la Società, in caso di violazione dei principi generali del Modello adottato (da intendersi nello specifico anche con riferimento alle disposizioni inerenti al sistema *whistleblowing* indicate nel paragrafo 5.7 e all'interno della "*SpeakUp & Whistleblowing Policy*" e del relativo *Addendum Whistleblowing Addendum per le Società italiane*") e delle regole di comportamento imposte dal Codice Etico, il Consiglio di Amministrazione, oltre a quanto previsto dal CCNL applicato, assume nei confronti dei responsabili i provvedimenti ritenuti idonei in funzione delle violazioni commesse quali la revoca di deleghe e procure, il disconoscimento dei corrispettivi previsti nei piani premianti e il licenziamento, tenuto conto che le stesse costituiscono inadempimento alle obbligazioni derivanti dal rapporto di lavoro.

È passibile di licenziamento il dirigente che compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di chi abbia effettuato segnalazioni di violazioni del Modello o di commissione dei reati previsti dal D.Lgs. 231/2001 per motivi che siano collegati, direttamente o indirettamente, alla segnalazione stessa.

Analoga sanzione è prevista per il dirigente che effettui con dolo o colpa grave segnalazioni di violazioni del Modello o di commissione dei reati previsti dal D.Lgs. 231/2001 che si rivelino infondate.

La Società, nella determinazione dei piani premianti, può definire degli obiettivi collegati al rispetto del presente Modello e delle regole ivi richiamate.

7.4.3 Misure nei confronti dei componenti del Consiglio di Amministrazione

La Società valuta con particolare rigore le infrazioni di quanto previsto dal Modello e dal Codice Etico poste in essere dai componenti del Consiglio di Amministrazione, in quanto rappresentano il vertice della Società e, quindi, ne manifestano l'immagine verso i terzi.

In caso di violazione della normativa vigente, del Modello (da intendersi nello specifico anche con riferimento alle disposizioni inerenti al sistema whistleblowing) o del Codice Etico da parte di un 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.

Salva ogni altra azione a tutela della Società, è passibile di revoca del mandato l'Amministratore che compia atti di ritorsione o discriminatori, diretti o indiretti, nei confronti di chi abbia effettuato segnalazioni di violazioni del Modello o di commissione dei reati previsti dal D.Lgs. 231/2001 per motivi che siano collegati, direttamente o

indirettamente, alla segnalazione stessa.

Analoga sanzione è prevista per l'Amministratore che effettui con dolo o colpa grave segnalazioni di violazioni del Modello o di commissione dei reati previsti dal D.Lgs. 231/2001 che si rivelano infondate.

7.4.4 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.

7.4.5 Misure nei confronti di collaboratori, consulenti e soggetti terzi

I rapporti con collaboratori, consulenti e fornitori di NTT DATA Italia sono regolamentati da una specifica clausola contrattuale 231 inserita negli Ordini a fornitori terzi, nei contratti e nei Patti Interni di costituendi Raggruppamenti Temporanei di Impresa (RTI / ATI).

Tale clausola prescrive l'impegno al rispetto di tutte le disposizioni di legge, comprese quelle del D. Lgs. 231/2001, ma anche tutte le disposizioni applicabili del Modello Organizzativo, del Codice Etico, dell'Anti-Corruption Policy e della Politica Integrata ISO per la Qualità, la Prevenzione della Corruzione e l'Ambiente.

Nei confronti di tali soggetti, destinatari degli obblighi di cui al D. Lgs. 231/2001, che abbiano posto in essere le gravi violazioni delle regole del Codice Etico e delle procedure e prescrizioni contenute nel Modello organizzativo 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.