doData S.r.l.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

Approvato dall'Amministratore Unico di doData S.r.l. in data 12/05/2023

INDICE

1. PREMESSA

Il presente documento, corredato di tutti i suoi allegati, costituisce il Modello di organizzazione, gestione e controllo (di seguito anche il "Modello") adottato da doData S.r.l. (di seguito anche "doData" o la "Società"), con delibera dell'Amministratore Unico del 12/05/2023, ai sensi del Decreto Legislativo 8 giugno 2001 n. 231 (di seguito denominato "Decreto" o "D.Lgs. 231/2001").

Il Modello è così articolato:

- il contesto normativo di riferimento;
- la **Parte Generale**, che contiene:
  - il Modello di Governo della Società e gli strumenti aziendali esistenti a supporto del Modello;
  - le finalità perseguite con l'adozione del Modello;
  - la metodologia adottata per l'analisi delle attività sensibili ai reati di cui al D.Lgs. 231/2001 e dei relativi presidi;
  - l'individuazione e la nomina dell'Organismo di Vigilanza di doData (di seguito anche "OdV") con indicazione dei poteri, dei compiti e dei flussi informativi che lo riguardano;
  - il sistema disciplinare e il relativo apparato sanzionatorio;
  - il piano di informazione e formazione da adottare al fine di garantire la conoscenza delle misure e delle disposizioni del Modello;
  - i criteri di aggiornamento e adeguamento del Modello;
- la **Parte Speciale**, contenente i protocolli di decisione.

Costituiscono, inoltre, parte integrante del Modello i seguenti Allegati e Documenti interni:

- Documento Codice Etico del Gruppo doValue (di seguito anche "Codice Etico") disponibile sul sito web istituzionale della Capogruppo;
- Documento "Linee Guida di Gruppo in materia di responsabilità da reato degli Enti", nella quale vengono fornite le linee guida e le direttrici alle Società del Gruppo doValue attive in Italia – compresa doData – affinché le stesse concorrano all'implementazione di un "Sistema 231" coordinato a livello di Gruppo, atto a consentire una gestione integrata e omogenea dei rischi in materia di responsabilità amministrativa degli Enti, ferma comunque restando l'autonomia e la specificità delle singole Società. Inoltre, fornisce linee guida in materia di responsabilità da reato degli Enti alle Società del Gruppo, sia italiane sia estere, affinché – nel rispetto della propria autonomia e del quadro normativo locale di riferimento – possano osservare standard minimi di prevenzione e gestione dei rischi in materia;
- Allegato "Reati presupposto del D.Lgs. 231/2001";
- Allegato "Elenco reati corruttivi";
- Matrice di collegamento Attività Sensibile – Reati presupposto 231.

2. CONTESTO NORMATIVO

2.1. Natura e caratteristiche della responsabilità amministrativa prevista dal D.Lgs. 231/2001

Il D.Lgs. n. 231/2001, emanato l'8 giugno 2001, in attuazione della legge delega 29 settembre 2000, n. 300, disciplina la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica (c.d. Enti[1]).

Tale legge delega ratifica, tra l'altro, la Convenzione sulla tutela finanziaria delle Comunità europee del 26 luglio 1995, la Convenzione U.E. del 26 maggio 1997 relativa alla lotta contro la corruzione e la Convenzione OCSE del 17 settembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali e ottempera agli obblighi previsti da siffatti strumenti internazionali e, in specie, comunitari i quali dispongono appunto la previsione di paradigmi di responsabilità delle persone giuridiche e di un corrispondente sistema sanzionatorio, che colpisca la criminalità d'impresa.

L'istituzione della responsabilità amministrativa delle società nasce dalla considerazione empirica che frequentemente le condotte illecite, commesse all'interno dell'impresa, lungi dal conseguire a un'iniziativa privata del singolo, rientrano piuttosto nell'ambito di una diffusa politica aziendale e conseguono a decisioni di vertice dell'Ente medesimo.

Si tratta di una responsabilità "amministrativa" *sui generis*, poiché, pur comportando sanzioni amministrative (si veda il successivo capitolo 2.3.4), consegue da reato e presenta le garanzie proprie del procedimento penale.

La sanzione amministrativa per gli Enti può essere applicata esclusivamente dal giudice penale e solo se sussistono tutti i requisiti oggettivi e soggettivi fissati dal legislatore: la commissione di determinati Reati elencati nel Decreto, nell'interesse[2] o a vantaggio[3] dell'Ente, da parte di:

- 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 (cosiddetti "Soggetti Apicali");
- persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali (cosiddetti "Soggetti Sottoposti").

La responsabilità dell'Ente si aggiunge a quella della persona fisica che ha commesso materialmente l'illecito e sussiste in maniera autonoma rispetto a quest'ultima, anche quando l'autore materiale del reato non è stato identificato o non è imputabile ovvero nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

L'Ente, però, non è responsabile se il fatto illecito è stato commesso da uno dei soggetti indicati dal Decreto "nell'interesse esclusivo proprio o di terzi"[4].

---

[1] Nell'ambito della definizione di Ente rientrano sia gli Enti dotati di personalità giuridica (SpA, Srl, società consortili, cooperative, associazioni riconosciute, fondazioni, altri enti privati e pubblici economici) sia gli Enti privi di personalità giuridica (Snc e Sas, consorzi, associazioni non riconosciute), mentre non si rientrano lo Stato, gli enti pubblici territoriali, gli altri enti pubblici non economici nonché gli enti che svolgono funzioni di rilievo costituzionale (art. 1, comma 3 del D.Lgs. 231/2001).

[2] Favorire l'Ente, senza che sia in alcun modo necessario il conseguimento effettivo e concreto dell'obiettivo. Si tratta dunque di un criterio che si sostanzia nella finalità – anche non esclusiva – con la quale il reato o l'Illecito è stato realizzato.

[3] Beneficio che l'Ente ha obiettivamente tratto dalla commissione del reato o dell'Illecito, a prescindere dall'intenzione di chi l'ha commesso.

[4] La responsabilità dell'Ente si configura anche in relazione a Reati commessi all'estero, purché per la loro repressione non proceda lo Stato del luogo in cui siano stati commessi e l'Ente abbia nel territorio dello Stato italiano la sede principale.

In forza dell'art. 4 del Decreto, l'Ente può essere chiamato a rispondere in Italia di Reati presupposto commessi all'estero. Il Decreto, tuttavia, subordina questa possibilità alle seguenti condizioni, che si aggiungono a quelle già evidenziate:

- sussistono le condizioni generali di procedibilità previste dagli artt. 7[5], 8[6], 9[7], 10[8] del Codice Penale per poter perseguire in Italia un reato commesso all'estero;
- l'Ente ha la propria sede principale nel territorio dello Stato italiano;
- lo Stato del luogo in cui è stato commesso il reato non procede nei confronti dell'Ente.

Si evidenzia inoltre che, qualora il reato venga commesso nell'ambito di un ente appartenente ad un gruppo, il concetto di interesse o vantaggio può essere esteso in senso sfavorevole alla società capogruppo, sussistendo potenziali profili di rischio di risalita della responsabilità per reati presupposto commessi da una o più società controllate. La giurisprudenza si è espressa in proposito ritenendo che è configurabile, ai sensi dell'art. 5 del Decreto, una responsabilità amministrativa della capogruppo di un gruppo societario per reati commessi nello svolgimento delle attività aziendali da parte delle società da essa controllate laddove, fra l'altro, possa ritenersi che la capogruppo abbia ottenuto un concreto vantaggio o perseguito un effettivo interesse a mezzo del reato commesso nell'ambito delle attività imputabili alla controllata (Cass Pen., Sez. V, sentenza n. 24583/2011). L'interesse o vantaggio della capogruppo non può essere pertanto identificato in un generico interesse di gruppo che si esaurisca nell'accrescimento della redditività dello stesso ma è necessario che sussista un interesse o vantaggio specifico della capogruppo (Cass Pen., Sez. II, sentenza n. 52316 del 2016).

Ai fini dell'affermazione della responsabilità dell'Ente, oltre all'esistenza dei richiamati requisiti che consentono di collegare oggettivamente il reato all'Ente, il legislatore impone l'accertamento della colpevolezza dell'Ente. Tale condizione si identifica con una colpa da organizzazione, intesa come violazione di adeguate regole di diligenza autoimposte dall'Ente medesimo e volte a prevenire lo specifico rischio da reato.

---

[5] L'art. 7 c.p., "Reati commessi all'estero", statuisce che: "È punito secondo la legge italiana il cittadino o lo straniero che commette in territorio estero taluno dei seguenti reati: 1) delitti contro la personalità dello Stato italiano; 2) delitti di contraffazione del sigillo dello Stato e di uso di tale sigillo contraffatto; 3) delitti di falsità in monete aventi corso legale nel territorio dello Stato, o in valori di bollo o in carte di pubblico credito italiano; 4) delitti commessi da pubblici ufficiali a servizio dello Stato, abusando dei poteri o violando i doveri inerenti alle loro funzioni; 5) ogni altro reato per il quale speciali disposizioni di legge o convenzioni internazionali stabiliscono l'applicabilità della legge penale italiana".

[6] L'art. 8 c.p., "Delitto politico commesso all'estero", statuisce che: "Il cittadino o lo straniero, che commette in territorio estero un delitto politico non compreso tra quelli indicati nel numero 1 dell'articolo precedente, è punito secondo la legge italiana [112], a richiesta del Ministro della giustizia. Se si tratta di delitto punibile a querela della persona offesa, occorre, oltre tale richiesta, anche la querela. Agli effetti della legge penale, è delitto politico ogni delitto, che offende un interesse politico dello Stato, ovvero un diritto politico del cittadino. È altresì considerato delitto politico il delitto comune determinato, in tutto o in parte, da motivi politici".

[7] L'art. 9 c.p., "Delitto comune del cittadino all'estero", statuisce che: "Il cittadino, che, fuori dei casi indicati nei due articoli precedenti, commette in territorio estero un delitto per il quale la legge italiana stabilisce l'ergastolo, o la reclusione non inferiore nel minimo a tre anni, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato. Se si tratta di delitto per il quale è stabilita una pena restrittiva della libertà personale di minore durata, il colpevole è punito a richiesta del Ministro della giustizia ovvero a istanza o a querela della persona offesa. Nei casi preveduti dalle disposizioni precedenti, qualora si tratti di delitto commesso a danno delle Comunità europee, di uno Stato estero o di uno straniero, il colpevole è punito a richiesta del Ministro della giustizia, sempre che l'estradizione di lui non sia stata conceduta, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto".

[8] L'art. 10 c.p., "Delitto comune dello straniero all'estero", statuisce che: "Lo straniero, che, fuori dei casi indicati negli articoli 7 e 8, commette in territorio estero, a danno dello Stato o di un cittadino, un delitto per il quale la legge italiana stabilisce l'ergastolo, o la reclusione non inferiore nel minimo a un anno, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato, e vi sia richiesta del Ministro della giustizia, ovvero istanza o querela della persona offesa. Se il delitto è commesso a danno delle Comunità europee, di uno Stato estero o di uno straniero, il colpevole è punito secondo la legge italiana, a richiesta del Ministro della giustizia, sempre che: 1) si trovi nel territorio dello Stato; 2) si tratti di delitto per il quale è stabilita la pena [di morte o] dell'ergastolo ovvero della reclusione non inferiore nel minimo a tre anni; 3) l'estradizione di lui non sia stata conceduta, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto, o da quello dello Stato a cui egli appartiene".

Specifiche disposizioni sono state dettate dal legislatore per i casi di trasformazione[9], fusione[10], scissione[11] e cessione d'azienda[12] (artt. 28-33 del D.Lgs. 231/2001).

2.2. Illeciti e reati che determinano la responsabilità amministrativa degli Enti

Originariamente prevista per i reati contro la Pubblica Amministrazione (di seguito anche "P.A.") o contro il patrimonio della P.A., la responsabilità dell'ente è stata estesa – per effetto di provvedimenti normativi successivi al D.Lgs. 231/2001 – a numerosi altri reati e illeciti amministrativi. Relativamente proprio a questi ultimi, si precisa sin d'ora che, ogni qualvolta all'interno del presente documento si fa riferimento ai "reati presupposto" o "reati", tale riferimento è da intendersi comprensivo anche degli illeciti introdotti dal legislatore, quali ad esempio quelli previsti dalla normativa di *market abuse* (artt. 187 *bis* e 187 *ter* D.Lgs. 58/1998 – Testo Unico delle disposizioni in materia di intermediazione finanziaria [13]).

Segnatamente, la responsabilità amministrativa degli enti può conseguire dai reati/illeciti elencati dal D.Lgs. 231/2001, come di seguito riportati:

1) Reati contro la Pubblica Amministrazione (artt. 24 e 25);
2) Reati informatici e trattamento illecito di dati (art. 24-*bis*);
3) Delitti di criminalità organizzata (art. 24-*ter*);
4) Reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis*);
5) Delitti contro l'industria e il commercio (art. 25-*bis*.1);
6) Reati societari (art. 25-*ter*);
7) Reati commessi con finalità di terrorismo o di eversione dall'ordine democratico (art. 25-*quater*);
8) Pratiche di mutilazione degli organi genitali femminili (art. 25-*quater*.1);
9) Reati contro la personalità individuale (art. 25-*quinquies*);

[9] In caso di trasformazione dell'Ente resta ferma la responsabilità per i Reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto. Il nuovo Ente sarà quindi destinatario delle sanzioni applicabili all'Ente originario, per fatti commessi anteriormente alla trasformazione.

[10] In caso di fusione, l'Ente risultante dalla fusione stessa, anche per incorporazione, risponde dei Reati dei quali erano responsabili gli enti che hanno partecipato alla fusione. Se essa è avvenuta prima della conclusione del giudizio di accertamento della responsabilità dell'Ente, il giudice dovrà tenere conto delle condizioni economiche dell'Ente originario e non di quelle dell'Ente risultante dalla fusione.

[11] Nel caso di scissione, resta ferma la responsabilità dell'Ente scisso per i Reati commessi anteriormente alla data in cui la scissione ha avuto effetto e gli Enti beneficiari della scissione sono solidalmente obbligati al pagamento delle sanzioni pecuniarie inflitte all'Ente scisso nei limiti del valore del patrimonio netto trasferito ad ogni singolo Ente, salvo che si tratti di Ente al quale è stato trasferito anche in parte il ramo di attività nell'ambito del quale è stato commesso il Reato; le sanzioni interdittive si applicano all'Ente (o agli Enti) in cui sia rimasto o confluito il ramo d'attività nell'ambito del quale è stato commesso il Reato. Se la scissione è avvenuta prima della conclusione del giudizio di accertamento della responsabilità dell'Ente, il giudice dovrà tenere conto delle condizioni economiche dell'Ente originario e non di quelle dell'Ente risultante dalla fusione.

[12] In caso di cessione o di conferimento dell'azienda nell'ambito della quale è stato commesso il Reato, salvo il beneficio della preventiva escussione dell'Ente cedente, il cessionario è solidalmente obbligato con l'Ente cedente al pagamento della sanzione pecuniaria, nei limiti del valore dell'azienda ceduta e nei limiti delle sanzioni pecuniarie che risultano dai libri contabili obbligatori o dovute per illeciti di cui il cessionario era comunque a conoscenza.

[13] In diritto penale si definisce "reato" un fatto umano, commissivo o omissivo, al quale l'ordinamento giuridico ricollega una sanzione penale in ragione del fatto che tale comportamento sia stato definito come antigiuridico perché costituisce un'offesa a un bene giuridico o un insieme di beni giuridici (che possono essere beni di natura patrimoniale o anche non patrimoniali) tutelati dall'ordinamento da una apposita norma incriminatrice. Rientra, quindi, nella più ampia categoria dell'illecito.

10) Reati ed illeciti amministrativi in tema di abusi di mercato (art. 25-*sexies*);

11) Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies*);

12) Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art. 25-*octies*);

13) Delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1);

14) Delitti in materia di violazione del diritto d'autore (art. 25-*novies*);

15) Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25-*decies*);

16) Reati ambientali (art. 25-*undecies*);

17) Reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 25-*duodecies*);

18) Razzismo e xenofobia (art. 25-*terdecies*);

19) Reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-*quaterdecies*);

20) Reati tributari (25-*quinquiesdecies*);

21) Reati di contrabbando (art. 25-*sexiesdecies*);

22) Delitti contro il patrimonio culturale (art. 25-septiesdiecies);

23) Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art. 25 duodevicies);

24) Reati transnazionali (art. 10 L.16 marzo 2006, n. 146);

25) Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato per gli enti che operano nell'ambito della filiera degli oli vergini di oliva (Art. 12 L. 9/2013).

Per maggiori dettagli si rimanda a quanto meglio specificato nell'Allegato del presente Modello "Reati presupposto del D.Lgs. 231/2001".

2.3. L'adozione del Modello come possibile esimente della responsabilità amministrativa

Il Decreto prevede una forma specifica di esonero dalla responsabilità amministrativa dipendente dai Reati (c.d. condizione esimente), a seconda che il reato sia commesso dai Soggetti Apicali o dai Soggetti Sottoposti.

2.3.1. I Reati e gli Illeciti commessi dai Soggetti Apicali

Per i Reati commessi da Soggetti Apicali l'Ente, per essere esente da colpa, dovrà dimostrare che (art. 6, comma 1 del D.Lgs. n. 231/2001):

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di organizzazione, gestione e controllo idoneo a prevenire Reati della specie di quelli verificatosi;
- il compito di verificare il funzionamento e l'osservanza del Modello nonché di curarne l'aggiornamento sia stato affidato ad un organo dell'Ente, dotato di autonomi poteri di iniziativa e controllo;
- le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il Modello;
- non vi sia stata omessa o insufficiente vigilanza da parte dell'organo di cui al secondo punto.

Le condizioni sopra elencate devono concorrere tutte e congiuntamente affinché la responsabilità dell'Ente possa essere esclusa.

2.3.2. I Reati e gli Illeciti commessi dai Soggetti Sottoposti

Per i Reati commessi da Soggetti Sottoposti alla direzione o alla vigilanza di uno dei soggetti apicali, l'Ente è responsabile se la "commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza" dei soggetti apicali, inosservanza che è in ogni caso esclusa "se l'Ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello di organizzazione, gestione e controllo idoneo a prevenire Reati della specie di quello verificatosi".

La responsabilità dell'Ente è pertanto ricondotta alla c.d. "colpa da organizzazione", ossia alla mancata adozione o al mancato rispetto di standard doverosi attinenti all'organizzazione e all'attività dell'Ente medesimo.

2.3.3. I Reati commessi all'estero

Secondo quanto espressamente stabilito nel Decreto 231, l'Ente può essere chiamato a rispondere sul territorio dello Stato italiano di Reati commessi all'estero.

I presupposti su cui si fonda tale responsabilità sono:

- il Reato deve essere commesso all'estero da un soggetto funzionalmente legato all'Ente;
- l'Ente deve avere la propria sede principale nel territorio dello Stato italiano;
- l'Ente risponde solo nei casi ed alle condizioni previste dagli artt. 7, 8, 9, 10 c.p. (norme del codice penale che disciplinano i reati commessi all'estero; qualora la legge preveda che l'autore del com- portamento illecito sia punito a richiesta del Ministro della Giustizia, si procede contro l'Ente solo se la richiesta è formulata anche nei confronti dell'Ente medesimo);
- l'Ente risponde purché nei suoi confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

2.3.4. L'efficace attuazione del Modello

L'art. 6, co. 1 del D.Lgs. 231/2001 prevede la cosiddetta "condizione esimente", ovvero le condizioni che l'ente deve dimostrare per non essere imputabile della responsabilità ai sensi del D.Lgs. 231/2001. In particolare l'ente non risponde della responsabilità ex D.Lgs. 231/2001 se dimostra che l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione, gestione e controllo idonei a prevenire reati della specie di quello verificatosi". Di conseguenza, la mera adozione del Modello non è sufficiente a garantire l'esonero dalla responsabilità per l'Ente, ma il Modello dev'essere implementato nel rispetto delle seguenti condizioni previste dall'art. 6, co. 2 del Decreto:

- individuazione delle attività nel cui ambito esiste la possibilità che vengano commessi Reati previsti dal D.Lgs. n. 231/2001;
- previsione di specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai Reati da prevenire;
- individuazione delle modalità di gestione delle risorse finanziarie idonee a impedire la commissione di Reati;
- previsione degli obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;

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

Deve inoltre rispondere al requisito dell'efficace attuazione, il quale, come previsto dall'art. 7, co. 4 del D.Lgs. 231/2001, richiede fra l'altro la verifica periodica nonché l'eventuale modifica del Modello, ogniqualvolta l'Ente modifichi la propria struttura organizzativa o l'oggetto delle attività sociali o si rilevino significative violazioni delle prescrizioni.

2.4. Le sanzioni irrogabili all'Ente

A carico dell'Ente che ha tratto vantaggio dalla commissione del reato, o nel cui interesse sono stati compiuti i Reati, sono irrogabili (art. 9 del D.Lgs. n. 231/2001) le seguenti misure sanzionatorie:

- sanzione pecuniaria: si applica ogniqualvolta è riconosciuta la responsabilità dell'Ente ed è determinata dal giudice penale attraverso un sistema basato su «quote». Per i Reati previsti dall'art. 25-*sexies* del D.Lgs. n. 231/2001 e gli Illeciti Amministrativi di cui all'art. 187-*quinquies* del TUF, se il prodotto o il profitto conseguito dall'Ente è di rilevante entità "la sanzione pecuniaria è aumentata fino a dieci volte tale prodotto o profitto".

  Il Decreto prevede altresì l'ipotesi di riduzione della Sanzione pecuniaria, allorquando l'autore del reato abbia commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne abbia ricavato un vantaggio ovvero ne abbia ricavato un vantaggio minimo, oppure quando il danno cagionato risulti di particolare tenuità.

  La Sanzione pecuniaria, inoltre, è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado, l'Ente ha risarcito integralmente il danno ed ha eliminato le conseguenze dannose o pericolose del reato, o si è comunque adoperato in tal senso.

  Infine, la sanzione pecuniaria è ridotta nel caso in cui l'Ente abbia adottato un modello idoneo alla prevenzione di reati della specie di quello verificatosi.

  Del pagamento della Sanzione pecuniaria inflitta risponde soltanto l'Ente, con il suo patrimonio; si esclude, pertanto, una responsabilità patrimoniale diretta dei soci o degli associati, indipendentemente dalla natura giuridica dell'Ente;

- sanzione interdittiva: si applica per alcune tipologie di reati e per le ipotesi di maggior gravità. Si traduce:
  - nell'interdizione dall'esercizio dell'attività aziendale;
  - nella sospensione e nella revoca delle autorizzazioni, delle licenze o delle concessioni funzionali alla commissione dell'illecito;
  - nel divieto di contrattare con la Pubblica Amministrazione (salvo che per ottenere le prestazioni di un pubblico servizio);
  - nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli concessi;
  - nel divieto di pubblicizzare beni o servizi.

  In ogni caso, le sanzioni interdittive non si applicano (o sono revocate, se già applicate in via cautelare) qualora l'Ente – prima della dichiarazione di apertura del dibattimento di primo grado:
  - abbia risarcito il danno, o lo abbia riparato;
  - abbia eliminato le conseguenze dannose o pericolose del reato (o, almeno, si sia adoperato in tal senso);
  - abbia messo a disposizione dell'Autorità Giudiziaria, per la confisca, il profitto del reato;

- abbia eliminato le carenze organizzative che hanno determinato il reato, adottando modelli organizzativi idonei a prevenire la commissione di nuovi reati.

Qualora ricorrano tutti questi comportamenti – considerati di ravvedimento operoso – anziché la sanzione interdittiva si applicherà quella pecuniaria;

- confisca: consiste nell'acquisizione del prezzo o del profitto del reato da parte dello Stato o nell'acquisizione di somme di danaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato; non investe, tuttavia, quella parte del prezzo o del profitto del reato che può restituirsi al danneggiato. La confisca è sempre disposta con la sentenza di condanna;
- pubblicazione della sentenza: può essere disposta quando all'Ente viene applicata una sanzione interdittiva; viene effettuata a cura della cancelleria del Giudice, a spese dell'Ente, ai sensi dell'articolo 36 del codice penale nonché mediante affissione nel comune ove l'Ente ha la sede principale[14].

2.5. Linee guida delle associazioni di categoria

Per espressa previsione legislativa (art. 6 comma 3, D.Lgs. 231/2001), i modelli di organizzazione, gestione e controllo possono essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia.

In attuazione di siffatto disposto normativo, l'ABI (Associazione Bancaria Italiana) ha redatto e successivamente aggiornato le "Linee guida per l'adozione dei modelli organizzativi sulla responsabilità amministrativa delle banche". In aggiunta si richiamano anche le Linee Guida dell'associazione di categoria Confindustria che ha provveduto con l'emanazione e il successivo aggiornamento delle Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001, delineando le *best practices* applicabili alla generalità dei Modelli ex D.Lgs. 231/2001.

Si sono altresì tenuti in espressa considerazione i provvedimenti giurisprudenziali in materia di responsabilità amministrativa degli enti. In particolare, nella definizione del Modello ci si è altresì ispirati, oltre alle Linee Guida sopra enunciate, al c.d. "Decalogo 231[15]" . Per la predisposizione del proprio Modello di organizzazione, gestione e controllo, la Società ha espressamente tenuto conto - oltre che delle disposizioni normative - anche delle suddette linee guida delle associazioni di categoria.

[14] La Legge Finanziaria di Luglio 2011 ha modificato l'art. 36 del Codice Penale, richiamato dall'art. 18 del D. Lgs. 231/2001. A seguito di tale modifica, la sanzione relativa alla "pubblicazione della sentenza penale di condanna" è stata ridotta in termini di severità, prevedendo che la pubblicazione avverrà esclusivamente nel sito del Ministero della Giustizia e non anche nei quotidiani nazionali.

[15] Cfr. Ordinanza emessa dal Giudice per le Indagini Preliminari presso il Tribunale di Milano, dott.ssa Secchi, in data 20 settembre 2004.

PARTE GENERALE

3. IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI doData

3.1. Funzione e scopo del Modello

Benché la legge non ne preveda l'obbligo, doData ha ritenuto opportuno adottare uno specifico Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001 nella convinzione che ciò costituisca, oltre che un valido strumento di sensibilizzazione di tutti coloro che operano per conto della Società, affinché tengano comportamenti corretti e lineari, anche un più efficace mezzo di prevenzione contro il rischio di commissione dei Reati e degli Illeciti di cui al Decreto.

In particolare, attraverso l'adozione del presente Modello, la Società intende perseguire le seguenti finalità:

- adeguarsi alla normativa sulla responsabilità amministrativa degli Enti, nonché verificare e valorizzare i presidi già in essere, atti a prevenire la realizzazione di condotte illecite rilevanti ai sensi del D.Lgs. 231/2001;
- informare tutti coloro che operano per conto della Società del contenuto del Decreto, della sua rilevanza e delle sanzioni penali e amministrative che possono essere comminate alla Società e nei loro confronti, in caso di violazione degli obblighi impartiti in materia, nonché delle conseguenze disciplinari e/o contrattuali che possono derivarne nei loro confronti;
- rendere noto che doData non tollera condotte che, anche se possono apparentemente favorire l'interesse della Società, sono contrarie – oltre che alle disposizioni di legge, alla normativa di settore e aziendale – anche ai principi etici ai quali la Società intende attenersi nell'esercizio dell'attività aziendale;
- assumere le iniziative necessarie per prevenire o contrastare comportamenti illeciti e contrari al proprio Modello.

Il Modello di doData:

- è costituito dall'insieme delle regole interne di cui la Società si è dotata, in relazione ai rischi connessi all'attività specifica svolta;
- individua le attività nel cui ambito possono essere commessi i Reati e gli Illeciti e definisce i principi comportamentali necessari per evitare che siano commessi;
- si poggia sui principi fondamentali della:
  - trasparenza dei comportamenti riferibili alle aree sensibili, come di seguito individuate, sia all'interno di doData che nei rapporti con le controparti esterne;
  - tracciabilità delle operazioni relative alle aree sensibili, finalizzata a garantire la verificabilità delle congruenze e coerenza delle stesse, anche attraverso un adeguato supporto documentale;
  - correttezza da parte di tutti i soggetti facenti capo a doData, garantita dal rispetto delle disposizioni di legge, di regolamenti, della normativa e delle procedure organizzative interne.

3.2. Destinatari

I principi e le disposizioni del Modello devono essere rispettate da tutti i soggetti interni alla Società, nonché da tutti i soggetti esterni che, in forza di rapporti contrattuali, prestino la loro collaborazione a doData per la realizzazione delle sue attività, intendendosi per:

- **soggetti interni**:
  - componenti degli Organi sociali della Società;

- tutto il Personale di doData intendendosi per tale:
  - il personale dipendente, compreso il top management;
  - i collaboratori legati da contratto dipendente a termine;
  - il personale dipendente della Capogruppo e/o di altre Società del Gruppo che opera in regime di distacco in nome e per conto di doData o in favore della stessa (di seguito anche "personale distaccato");

- **soggetti esterni**, nei limiti del rapporto in essere con la Società, quali a titolo esemplificativo e non esaustivo:
  - lavoratori autonomi o parasubordinati;
  - fornitori di beni e servizi (e.g. società volte a fornire servizi di infoproviding), inclusi professionisti e consulenti;
  - partner commerciali.

La Società richiede ai soggetti esterni il rispetto del Modello, nonchè del Codice Etico, mediante la documentata presa visione dello stesso e l'apposizione di una clausola contrattuale che impegni il contraente ad attenersi ai principi in essi riportati.

Con specifico riferimento a eventuali partner commerciali, inoltre, la Società verifica che i principi etici su cui si basano le attività degli stessi risultino allineati a quelli di cui al presente Modello e al Codice Etico.

L'insieme dei soggetti interni e dei soggetti esterni costituisce i "**Destinatari**" del Modello e del Codice Etico.

3.3. Il Modello di Governo della Società e gli strumenti aziendali esistenti a supporto del Modello

Il presente Modello si integra all'interno della normativa, delle procedure e dei sistemi di controllo già esistenti ed operanti in doData.

Il contesto organizzativo della Società è costituito dall'insieme di regole, strutture e procedure che ne garantiscono il corretto funzionamento; si tratta dunque di un sistema articolato che rappresenta già di per sé uno strumento a presidio della prevenzione di comportamenti illeciti in genere, inclusi quelli previsti dalla normativa specifica che dispone la responsabilità amministrativa degli Enti.

In particolare, quali specifici strumenti diretti a programmare la formazione e l'attuazione delle decisioni aziendali e ad effettuare i controlli, la Società fa riferimento:

- alle regole di corporate governance;
- al Sistema dei Controlli Interni;
- al sistema dei poteri e delle deleghe;
- al Codice Etico e alla normativa interna (ivi compreso il Sistema Anticorruzione).

Inoltre, la Società ha formalizzato in specifici protocolli di decisione:

- il risultato della ricognizione delle "attività sensibili" nell'ambito delle quali può verificarsi il rischio di commissione dei reati presupposto;
- i principi di comportamento e le regole di controllo volti a prevenire i reati.

3.3.1. Il Modello di governance di doData

In linea con il Modello di Governance del Gruppo doValue, doData ha adottato un modello di amministrazione di tipo "tradizionale", caratterizzato dalla presenza di un Amministratore Unico a cui compete l'individuazione degli indirizzi strategici della Società e la gestione aziendale, la cui nomina e revoca compete all'Assemblea dei Soci.

La revisione legale dei conti è affidata a una società di revisione esterna e indipendente, in applicazione delle disposizioni normative e statutarie vigenti in materia.

L'assetto organizzativo del Gruppo risponde all'esigenza di assicurare, in funzione dell'attività di direzione e coordinamento ai sensi degli artt. 2497 e seguenti del codice civile, una costante attività di supervisione da parte della Capogruppo nei confronti delle società del Gruppo, sotto il profilo strategico, gestionale e tecnico-operativo, tenendo in adeguata considerazione gli impatti derivanti dalla diversa articolazione organizzativa delle Funzioni Aziendali di Controllo nell'ambito delle Controllate Vigilate e le peculiarità connesse al loro status regolamentare.

3.3.2. Il Sistema dei Controlli Interni

Il Sistema dei Controlli Interni di doData si colloca nel più ampio Sistema dei Controlli Interni del Gruppo doValue, il quale, ispirandosi ai principi di integrazione, proporzionalità ed economicità, prevede l'accentramento presso la Capogruppo delle Funzioni Aziendali di Controllo di secondo livello (i.e. Dirigente Preposto) e di terzo livello (i.e. Group AML, Funzione Group Internal Audit). Tale scelta è originata dall'esigenza di attuare, unitamente a un forte coordinamento strategico, anche una costante attività di supervisione da parte della Capogruppo nei confronti di tutte le società del Gruppo, tenendo in adeguata considerazione gli impatti derivanti dalla diversa articolazione organizzativa delle Funzioni Aziendali di Controllo nell'ambito delle Controllate Vigilate e le peculiarità connesse al loro status regolamentare. Il Sistema dei Controlli Interni del Gruppo doValue prevede altresì la presenza di Funzioni Aziendali con Compiti di Controllo, che consistono nell'insieme delle Strutture/Funzioni coinvolte nella gestione del sistema dei controlli interni, a presidio di specifici ambiti normativi/di rischio, quali Group Enterprise Risk Management, GROUP AML e Group Compliance & Global DPO. Tale scelta è originata dall'esigenza di attuare, unitamente a un forte coordinamento strategico, anche un altrettanto incisivo coordinamento nel Sistema dei Controlli Interni di Gruppo.

Le Funzioni Aziendali di Controllo di Gruppo, indipendenti dal punto di vista organizzativo e nettamente separate dalle altre unità organizzative, dispongono dell'autorità, delle risorse economiche e fisiche, nonché delle competenze necessarie per lo svolgimento dei loro compiti.

Riportano gerarchicamente agli Organi con funzioni di supervisione strategica e di gestione della Capogruppo – nello specifico, le Funzioni Aziendali di Controllo di secondo livello riportano all'Amministratore Delegato della Capogruppo, mentre la Funzione Aziendale di Controllo di terzo livello riporta al Consiglio di Amministrazione – e funzionalmente agli Organi con funzioni di supervisione strategica delle Società del Gruppo, nonché coordinano le proprie attività con gli Organi di controllo delle stesse, eventualmente istituiti.

Gli elementi fondanti del Sistema dei Controlli Interni sono definiti nell'ambito del Regolamento sul Sistema dei Controlli integrati del Gruppo doValue, adottato con delibera del Consiglio di Amministrazione della Capogruppo e applicabile anche alle Società del Gruppo – inclusa doData – che si impegnano a recepirne, per il tramite del proprio Organo con funzioni di supervisione strategica, principi e linee guida tenendo conto delle proprie peculiarità aziendali.

In tale contesto è previsto che le Funzioni Aziendali di Controllo includano nei rispettivi piani di attività, ciascuna per la propria mission, verifiche e/o attività di consulenza a livello consolidato volte ad accertare la rispondenza dei comportamenti delle Controllate in relazione agli indirizzi impartiti dalla Capogruppo nell'ambito della direzione e coordinamento nonché delle normative specifiche loro applicabili.

In particolare, il Sistema dei Controlli Interni è costituito dall'insieme di strumenti, strutture organizzative, norme e regole aziendali volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei rischi aziendali, una conduzione dell'impresa sana, corretta e coerente con gli obiettivi prefissati di performance e la salvaguardia del patrimonio aziendale nel suo complesso. Il Sistema dei Controlli Interni di Gruppo è dunque volto a consentire il perseguimento di obiettivi:

- strategici, verificando il grado di attuazione delle strategie e delle politiche aziendali definite a livello di Gruppo da parte del Consiglio di Amministrazione della Capogruppo;
- gestionali, verificando l'efficacia, l'efficienza e l'economicità delle attività espletate, al fine di ottimizzare, anche mediante tempestivi interventi correttivi, il rapporto tra le stesse e gli obiettivi strategici;
- di performance, rendendo maggiormente efficienti i processi aziendali, salvaguardando il valore delle attività e dei flussi di reddito anche attraverso la minimizzazione e prevenzione delle perdite;
- di prevenzione del rischio, evitando, pertanto, che la Società possa essere coinvolta, anche involontariamente, in attività illecite (con particolare riferimento a quelle connesse al riciclaggio e finanziamento al terrorismo);
- di conformità delle operazioni con le disposizioni di Legge e con le Disposizioni di Vigilanza nonché con le politiche, i regolamenti e le procedure interne;
- di sicurezza, migliorando l'affidabilità e la sicurezza delle informazioni aziendali e delle procedure informatiche.

La responsabilità primaria della completezza, adeguatezza, funzionalità e affidabilità del complessivo Sistema dei Controlli Interni è rimessa agli organi di governo, ed in particolare al Consiglio di Amministrazione della Capogruppo, cui spettano compiti di pianificazione strategica, gestione, valutazione e monitoraggio del complessivo Sistema dei Controlli Interni.

L'architettura del Sistema dei Controlli Interni della Capogruppo fa riferimento ai seguenti livelli di controllo:

- **Controlli di 1° livello** (i.e. "controlli di linea"), che sono diretti ad assicurare il corretto svolgimento delle operazioni, sono effettuati dalle stesse strutture produttive, incaricate del relativo espletamento (e.g. controlli di tipo gerarchico sistematici e a campione) o incorporate nelle procedure – anche automatizzate – ovvero eseguito nell'ambito dell'attività di back office. Tali strutture, in quanto prime responsabili del processo di controllo interno e di gestione dei rischi, sono chiamate, nel corso dell'operatività giornaliera, a identificare, misurare o valutare, monitorare, attenuare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi e le procedure interne applicabili
- **Controlli di 2° livello,** volti ad assicurare, tra le altre:
  - la corretta attuazione del processo di gestione dei rischi operativi;
  - il rispetto dei limiti operativi assegnati alle varie Funzioni aziendali;
  - la coerenza della operatività delle singole aree produttive con gli obiettivi di rischio-rendimento assegnati e la corretta attuazione del processo di gestione dei rischi;
  - la conformità della operatività aziendale alle disposizioni di Legge (incluse quelle di autoregolamentazione) ed ai Regolamenti interni;
  - l'adeguatezza del sistema di controllo interno sull'informativa finanziaria nell'ambito del Gruppo e delle procedure amministrative e contabili per la formazione del bilancio d'esercizio e del bilancio consolidato, nonché di ogni altra comunicazione di carattere finanziario.

Le Funzioni preposte a tali controlli sono distinte da quelle produttive e concorrono alla definizione delle politiche di governo dei rischi e dei processi di gestione dei rischi;

- **Controlli di 3° livello** (Internal Audit), volti a valutare periodicamente la completezza, adeguatezza, funzionalità e affidabilità in termini di efficienza ed efficacia del Sistema dei Controlli Interni e del sistema informativo, con cadenza predefinita e in relazione alla natura e all'intensità dei rischi ed alle esigenze aziendali, individuando, altresì, eventuali violazioni delle misure organizzative (procedure e Regolamenti) adottate dal Gruppo

Con particolare riferimento ai controlli di primo livello, questi caratterizzano tutti i processi aziendali e sono di competenza, come anzidetto, delle strutture operative della Società.

Con riferimento, invece, ai controlli di secondo livello, le responsabilità sono attribuite alle seguenti funzioni aziendali di controllo di Gruppo, attribuite alle competenti strutture di Capogruppo:

- GROUP AML, responsabile di garantire il rispetto, ove applicabili, delle normative interne ed esterne in materia di contrasto al riciclaggio e al finanziamento del terrorismo nonché presidiarne e mitigarne i relativi rischi;
- Dirigente Preposto alla redazione dei documenti contabili ai sensi della L. 262/05, responsabile di verificare l'adeguatezza e l'effettiva operatività delle procedure con impatto amministrativo-contabile, coerentemente con gli standard comunemente accettati in tema di controlli interni, attraverso il disegno e l'implementazione di un coerente modello basato su attività di controllo a livello di entità e di testing periodici.

Sono altresì attribuite responsabilità nella gestione del sistema dei controlli interni, a presidio di specifici ambiti normativi/di rischio, a talune Funzioni Aziendali con compiti di controllo. In particolare:

- l'Unità Organizzativa GROUP Enterprise Risk Management, ha il compito di presiedere la gestione dei rischi rilevanti cui sono esposte le attività della Capogruppo, con particolare riferimento ai rischi operativi, attraverso la definizione delle relative linee guida nonché l'identificazione ed il monitoraggio dei predetti rischi, avvalendosi a tale scopo di approcci metodologici, procedure e strumenti idonei e garantendo l'opportuna informativa agli Organi Aziendali;
- l'Unità Organizzativa GROUP Compliance & Global DPO, è responsabile di curare la rilevazione e il monitoraggio del rischio di non conformità alle norme negli ambiti di propria competenza (e.g. protezione dei dati personali, anticorruzione), fornendo consulenza e supporto alle strutture operative e di business, nonché predispondendo la necessaria informativa periodica agli Organi Aziendali.

Infine, per quanto concerne i controlli di terzo livello, gli stessi sono di responsabilità della Funzione Internal Audit di Gruppo, collocata nell'ambito della Direzione Controlli Interni, a diretto riporto del Consiglio di Amministrazione della Capogruppo, con la mission di assicurare il coordinamento a livello unitario del governo dei rischi – in coerenza con le linee di sviluppo strategico della Capogruppo – e garantire nel continuo una valutazione di sintesi dell'adeguatezza dei controlli implementati nei processi e nei sistemi aziendali. La Funzione Internal Audit di Gruppo è incaricata di:

- assicurare un'azione di sorveglianza costante ed indipendente sul regolare andamento dell'operatività e dei processi della Capogruppo e delle Controllate – compresa doData – con l'obiettivo di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose;
- effettuare la valutazione del Sistema dei Controlli Interni, la funzionalità degli stessi e l'idoneità a garantire l'efficacia e l'efficienza dei processi aziendali, la salvaguardia del valore delle attività e la protezione dalle perdite, l'affidabilità e l'integrità delle informazioni contabili e gestionali, la conformità delle operazioni sia alle politiche stabilite dagli organi di governo aziendali che alle normative interne ed esterne;
- supportare la governance aziendale e assicurare una tempestiva e sistematica informativa sullo stato del sistema dei controlli e sulle risultanze dell'attività svolta agli Organi aziendali.

3.3.3. Il sistema dei poteri e delle deleghe

doData ha strutturato un sistema coerente di deleghe e di sub-deleghe all'interno del quale sono individuati i poteri di cui è investito l'Amministratore Unico[16], il quale a sua volta può sub-delegare i propri poteri e le proprie attribuzioni, unitamente ai limiti quantitativi[17] e qualitativi[18], nonché alle relative modalità di esercizio da parte dei soggetti delegati.

E' prevista l'informativa da parte dei soggetti delegati all'Amministratore Unico relativamente all'attività svolta nell'esercizio delle deleghe conferite.

Al fine di garantire coerenza all'intero sistema:

- i poteri sono stati assegnati in maniera graduata;
- l'assuzione di decisioni eccedenti i limiti quantitativi/qualitativi delle deleghe attribuite necessita del preventivo parere del livello gerarchico superiore.

La Società ha altresì definito un processo di gestione e autorizzazione delle spese garantendo il rispetto dei principi di trasparenza, verificabilità, inerenza all'attività aziendale e la coerenza fra i poteri autorizzativi di spesa e le responsabilità organizzative e gestionali.

3.3.4. Codice Etico

La Società, riconoscendo e promuovendo i più elevati standard di comportamento, ha recepito, i principi declinati dal Codice Etico, a cui tutti i dipendenti devono uniformarsi nello svolgimento delle proprie attività lavorative.

Tale Codice, che costituisce parte integrante del Modello, definisce i principi di condotta generale. Questo insieme di norme di comportamento su aspetti chiave dell'integrità morale vuole promuovere la cultura della compliance e guidare le azioni tese a promuovere l'impegno etico della Società.

3.3.5. Sistema Anticorruzione

Al fine di garantire il rispetto dei principi di etica, legalità e trasparenza e di prevenire qualsiasi forma di corruzione attiva e passiva, la Società ha altresì adottato uno specifico Sistema Anticorruzione che individua i principi, identifica le aree sensibili e definisce i ruoli, le responsabilità e i macro-processi per la gestione del rischio di corruzione da parte del Gruppo doValue. Prevede inoltre l'assegnazione della responsabilità di presidio della materia ad una Struttura individuata nell'ambito dell'organizzazione aziendale, che corrisponde alla "Funzione di Conformità per la prevenzione della corruzione" (che sostituisce il precedente Responsabile Aziendale Anticorruzione).

Il Sistema Anticorruzione integra – in chiave anticorruzione e contrasto ai fenomeni di *maladministration* – le misure previste nel presente Modello di Organizzazione, Gestione e controllo ex D. Lgs. n. 231/2001, inclusivo del Codice Etico adottato dal Gruppo, estendendone il perimetro di prevenzione dei rischi, fra l'altro, a tutte le più ampie fattispecie di reato contemplate dalla Legge n. 190/2012.

In linea con le migliori prassi internazionali la Capogruppo doValue ha altresì implementato un Sistema di gestione per la prevenzione della corruzione conforme allo Standard UNI ISO

[16] L'Amministratore Unico è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società, con facoltà di compiere tutte le operazioni commerciali, mobiliari, immobiliari e finanziarie ritenute opportune per il conseguimento dell'oggetto sociale, con la sola esclusione degli atti riservati dalla Legge ovvero dallo Statuto all'Assemblea dei Soci.

[17] Per limiti quantitativi / di valore si intendono i limiti di importo delle singole operazioni che ciascun soggetto delegato può autorizzare.

[18] I limiti qualitativi sono volti a limitare l'operatività del sinfolo soggetto delegato a specifiche e definite attività.

37001:2016 e, ad esito di un processo di verifica e validazione, ha ottenuto la relativa certificazione.

Per rispondere in maniera efficace ai requisiti previsti dallo standard ISO 37001:16 la Capogruppo doValue si è attivata attraverso:

- una chiara definizione dei propri processi;
- una univoca identificazione dei ruoli e delle funzioni;
- un trasparente sistema di deleghe e procure;
- un lineare sistema di regole, valori, procedure e prassi suggerite dall'esperienza, per favorire il processo decisionale all'interno dell'organizzazione;
- un adeguato sistema di controlli interno rivolto al comportamento di tutti i propri dipendenti e collaboratori; un adeguato sistema di controlli esterno rivolto ai processi ed alle operazioni con gli stakeholder esterni, in particolare con Società controllate del Gruppo, italiane ed estere, e con i fornitori.

Più nel dettaglio, con delibera dell'Amministratore Delegato in data 24/09/21 è stata istituita, all'interno della struttura Compliance & Global DPO di Gruppo, la Funzione di Conformità per la prevenzione della corruzione, a cui sono stati attribuiti tutti i compiti e le responsabilità disciplinati dalla normativa interna di riferimento, in conformità a quanto previsto dallo Standard ISO 37001:16.

Contemporaneamente, è stata attribuita alla struttura Compliance & DPO della Country Italy doValue il compito di supportare operativamente la Funzione di Conformità per la prevenzione della corruzione, nell'attuazione del Sistema all'interno del Gruppo doValue ed in generale, l'applicazione dei principi della Policy.

Le responsabilità per l'esecuzione dei compiti in ambito anticorruzione sopra declinati sono state assegnate in capo ad un Soggetto responsabile, cui è stato attribuito il ruolo di Focal Point Anticorruption a livello di Gruppo.

Nonostante il sistema di gestione per la prevenzione della corruzione implementato ai sensi dello Standard ISO 37001:16 sia al momento in capo a doValue S.p.A., l'obiettivo della Policy è quello di attuare misure volte a coinvolgere attivamente tutte le Società del Gruppo, *decentralizzando*, nei limiti previsti dal suo ruolo di direzione e coordinamento, ruoli e responsabilità alle funzioni delle Controllate. Tale sistema consente di definire presidi di controllo e gestione periferici puntuali che possano quindi dialogare con tempestività con la Capogruppo e, al contempo, fruire dei sistemi di gestione del framework di prevenzione della corruzione, declinati nelle singole realtà organizzative con le dovute specificità.

Rispetto alla configurazione societaria del Gruppo e alle previsioni dello Standard ISO 37001:16, la Funzione di Conformità per la prevenzione della corruzione è istituita:

- presso doValue, dove - in funzione della direzione e coordinamento espletata come Capogruppo nei confronti di tutte le Società del Gruppo - assicura anche un ruolo di coordinamento e supervisione; nonché

- presso le Region doValue Spain e doValue Greece.

Diversamente, presso le altre controllate (doNext e doData, e le altre società sotto il controllo di doValue Spain e doValue Greece), sono previsti i Referenti anticorruzione locali, ai fini di garantire un efficace e diffuso presidio in materia di contrasto ai fenomeni di corruzione, nonché per supportare la Funzione di Conformità per la prevenzione della corruzione istituita presso la Capogruppo

Al Referente Locale spettano i seguenti compiti e responsabilità:

- supportare la Funzione di Conformità per la prevenzione della corruzione nell'aggiornamento del Sistema Anticorruzione, nello svolgimento dei controlli al fine di monitorare la corretta applicazione del Sistema Anticorruzione del Gruppo all'interno della Controllata;

- garantire l'attuazione presso la Controllata delle linee guida e istruzioni operative dettate dalla Funzione di Conformità per la prevenzione della corruzione della Controllante e relazionare periodicamente su tutte le tematiche di rilevanza anticorruzione;

- garantire l'attuazione del piano formativo in ambito anticorruzione all'interno della Controllata, definito dalla Controllante;

- essere figura di riferimento per ogni questione connessa al contrasto alla corruzione all'interno della Controllata ed informare tempestivamente la Funzione di Conformità per la prevenzione della corruzione di ogni questione rilevante;

- rendicontare secondo le frequenze stabilite alla Funzione di Conformità per la prevenzione della corruzione circa gli indicatori di prestazione ed il raggiungimento degli obiettivi previsti dal sistema di gestione per la prevenzione della corruzione adottato dal Gruppo.

Il sistema sopra descritto è dettagliato all'interno di un framework di cui la Società si è dotata per rispondere adeguatamente alle richieste dello Standard ISO 37001:16 e che trasferisce con efficacia alle Società controllate affinché il sistema stesso sia declinato a livello di Gruppo con le corrette modalità individuate.[19]

[19] Per consultare l'elenco delle principali fattispecie di reati corruttivi si rinvia all'Allegato II "Elenco reati corruttivi"

4. ADOZIONE, EFFICACE ATTUAZIONE, MODIFICAZIONE E AGGIORNAMENTO DEL MODELLO

4.1. Adozione del Modello

L'adozione e l'efficace attuazione del Modello costituiscono, ai sensi dell'art. 6, comma 1, lett. a) del Decreto, atti di competenza e di emanazione dell'Amministratore Unico che approva, mediante apposita delibera, il Modello.

In fase di adozione del Modello, l'Amministratore Unico definisce – in coerenza con il documento "Governance di Gruppo in materia di Modelli *ex* D.Lgs. 231/2001" – la struttura del Modello con il supporto, per gli ambiti di rispettiva competenza, delle Funzioni Aziendali.

4.2. Efficace attuazione, modificazione e aggiornamento del Modello

L'Amministratore Unico assicura l'efficace attuazione del Modello, mediante valutazione e approvazione delle azioni necessarie per implementarlo o modificarlo. Per l'individuazione di tali azioni, l'Amministratore Unico si avvale del supporto dell'Organismo di Vigilanza, in coerenza con le previsioni di cui al documento "Linee Guida di Gruppo in materia di responsabilità da reato degli Enti"

L'Amministratore Unico, sentito il parere dell'Organismo di Vigilanza, modifica il Modello qualora siano state individuate significative violazioni delle prescrizioni in esso contenute che ne evidenziano l'inadeguatezza, anche solo parziale, a garantire l'efficace prevenzione dei Reati di cui al Decreto e aggiorna, in tutto o in parte, i contenuti del Modello qualora intervengano mutamenti nell'organizzazione, nell'attività o nel contesto normativo di riferimento, nonché nelle situazioni espressamente previste nel documento "Governance di Gruppo in materia di Modelli 231".

L'efficace e concreta attuazione del Modello è garantita altresì dall'Organismo di Vigilanza, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti sulle attività svolte dalle singole Funzioni Aziendali, nonché dagli organi aziendali e dai responsabili delle varie Funzioni Aziendali, i quali propongono, alle competenti Funzioni le modifiche delle procedure di loro competenza, quando tali modifiche appaiano necessarie per l'efficace attuazione del Modello. Le procedure e le modifiche alle stesse devono essere tempestivamente comunicate all'Organismo di Vigilanza.

È facoltà comunque dell'Organismo di Vigilanza apportare le variazioni ritenute necessarie ai protocolli fornendone informativa all'Amministratore Unico e proporre variazioni ai flussi informativi da /verso l'Organismo di Vigilanza.

Nella gestione del Modello sono inoltre coinvolte le Funzioni – anche accentrate/esternalizzate presso la Capogruppo o altre Società del Gruppo – e i soggetti di seguito indicati, ai quali sono affidati, in tale ambito, specifici ruoli e responsabilità.

INTERNAL AUDIT

La Funzione Internal Audit – collocata nell'ambito della Direzione Controlli Interni della Capogruppo – supporta direttamente l'Organismo di Vigilanza ai fini dell'espletamento dei propri compiti di vigilanza sul funzionamento e sull'osservanza del Modello. A tal fine, porta all'attenzione dello stesso Organismo eventuali criticità riscontrate nel corso della proprie attività di verifica di terzo livello, con particolare riferimento a quelle potenzialmente connesse a profili di rischio di commissione di reati rilevanti ai sensi del Decreto, nonché monitora che le Funzioni competenti portino a termine le azioni di mitigazione individuate a fronte di tali criticità.

AML

La Funzione Antiriciclaggio (AML) – collocata nell'ambito della Direzione Controlli Interni della Capogruppo, in forza di contratto di esternalizzazione Intercompany – sovraintende le attività di prevenzione e gestione del rischio di riciclaggio e finanziamento al terrorismo, verificando nel continuo l'idoneità delle procedure interne in materia anche per le finalità di cui al D.Lgs.

231/2001. La funzione Antiriciclaggio supporta direttamente l'attività di controllo dell'Organismo di Vigilanza, monitorando nel tempo l'efficacia delle regole e dei principi di comportamento indicati nel Modello a prevenire i Reati di cui al Decreto e collaborando, insieme alle altre funzioni,al Datore di lavoro e al Committente ai sensi del D.Lgs. n. 81/2008, per quanto di loro competenza, all'aggiornamento del Modello, per quel che concerne in particolare la gestione dei rischi in materia di antiriciclaggio e di finanziamento al terrorismo. Porta altresì all'attenzione dell'Organismo di Vigilanza eventuali criticità riscontrate nel corso delle proprie attività di verifica di secondo livello, con particolare riferimento a quelle potenzialmente connesse a profili di rischio di commissione di reati rilevanti ai sensi del Decreto, nonché monitorando che le funzioni competenti portino a termine le azioni di mitigazione individuate a fronte di tali criticità.

La funzione Antiriciclaggio partecipa, inoltre, in raccordo con le altre funzioni aziendali competenti in materia di formazione, alla predisposizione di un adeguato piano di formazione.

DIRIGENTE PREPOSTO DI GRUPPO

Il Dirigente Preposto comunica periodicamente ai competenti Organi Aziendali delle Società del Gruppo le attività svolte con evidenza di eventuali punti di attenzione ed alle azioni intraprese per il loro superamento. Il Dirigente Preposto comunica – nell'ambito della propria relazione annuale – il perimetro delle società e dei processi sensibili oggetto di test svolti, specificando le eventuali valutazioni quantitive e qualitative che hanno portato ad una variazione degli stessi rispetto alla puntuale applicazione delle regole metodologiche. Comunica inoltre gli esiti delle valutazioni di affidabilità ed adeguatezza del sistema dei controlli interni sull'informativa contabile e finanziaria, funzionali alle attestazioni richieste dalla normativa.

FUNZIONE DI CONFORMITÀ PER LA PREVENZIONE DELLA CORRUZIONE

La Funzione di Conformità per la prevenzione della corruzione – collocata all'interno della struttura GROUP Compliance & GLOBAL DPO - provvede a sviluppare e mantenere costantemente aggiornato il Sistema Anticorruzione di Gruppo, in coordinamento con le competenti Strutture aziendali, curando altresì lo sviluppo e l'efficace attuazione di un programma di formazione in materia di anticorruzione, nonché delle attività di comunicazione interna connesse al contrasto ai fenomeni corruttivi. La Funzione di Conformità per la prevenzione della corruzione trasmette agli Organi Aziendali delle Società del Gruppo, ivi compresi gli Organismi di Vigilanza delle Società italiane del Gruppo, adeguati flussi informativi periodici connessi alla gestione del rischio di corruzione, nonché informative trasmesse al verificarsi di eventi particolarmente rilevanti con riferimento al rischio di corruzione.

COMPLIANCE & DPO

L'Unità Organizzativa Compliance & DPO – collocata nell'ambito della Funzione Legal & Compliance di Capogruppo, in forza di contratto di esternalizzazione Intercompany – supporta l'attività dell'Organismo di Vigilanza, monitorando nel tempo l'efficacia delle regole e dei principi di comportamento indicati nel Modello a prevenire i Reati di cui al Decreto e collaborando, insieme alle altre Funzioni, al Datore di lavoro e al Committente ai sensi del D.Lgs. n. 81/2008, per quanto di loro competenza, all'aggiornamento del Modello in coerenza con l'evoluzione della normativa di riferimento. Porta altresì all'attenzione dell'Organismo di Vigilanza l'esito (ed eventuali criticità riscontrate) delle proprie attività di monitoraggio sulle singole attività svolte dalle singole Funzioni competenti rispetto ad azioni di mitigazione individuate a fronte di criticità connesse a profili di rischio di commissione di reati rilevanti ai sensi del Decreto. L'U.O. Compliance & DPO partecipa, inoltre, in raccordo con le altre Funzioni Aziendali competenti in materia di formazione, alla predisposizione di un adeguato piano di formazione.

OPERATIONAL RISK MANAGEMENT

L'Unità Organizzativa Operational Risk Management di Capogruppo assicura periodici flussi informativi all'Organismo di Vigilanza in merito a carenze nel sistema di gestione dei rischi operativi, eventualmente rilevate nel corso della propria attività di verifica di secondo livello, che possano compromettere la corretta attuazione del Modello. In relazione a tali eventuali carenze, tiene altresì informato l'Organismo di Vigilanza circa lo stato di implementazione delle connesse azioni di mitigazione individuate.

LEGAL & COMPLIANCE

Per il perseguimento delle finalità di cui al Decreto, la Funzione Legal & Compliance di Capogruppo, in forza di contratto di esternalizzazione Intercompany, collabora con le altre Funzioni / Strutture Aziendali, con il Datore di lavoro e il Committente ai sensi del D.Lgs. n. 81/2008 all'adeguamento del Modello, segnalando anche eventuali estensioni dell'ambito della responsabilità amministrativa degli Enti nonché gli orientamenti giurisprudenziali in materia.

PEOPLE

Con riferimento al Decreto, la Funzione Risorse Umane, attribuita nell'ambito della Funzione People della Capogruppo doValue, in forza di contratto di esternalizzazione Intercompany:

- programma piani di formazione e interventi di sensibilizzazione rivolti a tutti i dipendenti sull'importanza di un comportamento conforme alle regole aziendali, sulla comprensione dei contenuti del Modello, del Codice Etico, nonché specifici corsi destinati al personale che opera nelle attività sensibili con lo scopo di chiarire in dettaglio le criticità, i segnali premonitori di anomalie o irregolarità, le azioni correttive da implementare per le operazioni anomale o a rischio;
- presidia, con il supporto delle Funzioni di Capogruppo Internal Audit, Antiriciclaggio, Legal & Corporate Affairs, Compliance & DPO, il processo di rilevazione e gestione delle violazioni del Modello, nonché il conseguente processo sanzionatorio e fornisce tutte le informazioni emerse in relazione ai fatti e/o ai comportamenti rilevanti ai fini del rispetto della normativa del Decreto all'Organismo di Vigilanza, il quale le analizza al fine di prevenire future violazioni, nonché di monitorare l'adeguatezza del Modello.

ORGANIZATION E PROJECT & TRANSFORMATION

Le Unità Organizzative Organization e Project & Transformation – attribuite nell'ambito della Funzione IT-BO-ORGA & Trasformation della Capogruppo doValue, in forza di contratto di esternalizzazione Intercompany – al fine di meglio presidiare la coerenza della struttura organizzativa e dei meccanismi di governance rispetto agli obiettivi perseguiti col Modello, ha la responsabilità di:

- definire le regole per il disegno, la divulgazione e la gestione dei processi organizzativi;
- supportare la progettazione dei processi aziendali ovvero validare procedure definite da altre Funzioni, garantendone la coerenza con il disegno organizzativo complessivo;
- collaborare con le Strutture competenti in merito alla gestione delle risorse umane per la definizione e l'implementazione delle modifiche alla struttura organizzativa;
- collaborare con le Funzioni Internal Audit, Antiriciclaggio, Legal & Corporate Affairs, Compliance & DPO, il Datore di lavoro ed il Committente ai sensi del D.Lgs. n. 81/2008 e con le altre Funzioni Aziendali interessate, ognuna per il proprio ambito di competenza, all'adeguamento del sistema normativo e del Modello (a seguito di modifiche nella normativa applicabile, nell'assetto organizzativo aziendale e/o a livello di Gruppo e/o nelle procedure operative, rilevanti ai fini del Decreto);
- diffondere la normativa interna a tutta la Società.

DATORE DI LAVORO E COMMITTENTE AI SENSI DEL D.LGS. N. 81/2008

Il Datore di Lavoro e il Committente ai sensi del D.Lgs. n. 81/2008, limitatamente all'ambito di competenza per la gestione dei rischi in materia di salute e sicurezza nei luoghi di lavoro, individua e valuta l'insorgenza di fattori di rischio dai quali possa derivare la commissione di Reati di cui al Decreto e promuovono eventuali modifiche organizzative volte a garantire un presidio dei rischi individuati. Per gli ambiti di propria competenza, essi partecipano alla definizione della struttura del Modello e all'aggiornamento dello stesso, nonché alla predisposizione del piano di formazione.

4.3. Modalità operative seguite per la costruzione e l'aggiornamento del Modello

Tenendo conto anche delle linee guida delle associazioni di categoria e in coerenza con il documento "Governance di Gruppo in materia di Modelli 231", si è provveduto a identificare i principi di comportamento e le regole di controllo volti a prevenire la commissione dei reati presupposto e a formalizzarli in specifici protocolli di decisione rispondenti all'operatività delle strutture organizzative ed avendo riguardo alle specificità di ogni settore di attività.

In particolare, i cantieri progettuali funzionali alla costruzione e predisposizione del Modello si sono basati su una metodologia uniforme che ha previsto la realizzazione delle seguenti attività:

Fase I - Raccolta e analisi della documentazione

Al fine di una puntuale comprensione del sistema di governance e controllo in essere presso la Società, si è proceduto ad analizzare l'insieme dei documenti in vigore presso la stessa che forniscono le indicazioni circa il sistema di regole e normative a governo dei processi aziendali. Particolare attenzione è stata attribuita all'analisi della seguente documentazione:

- organigramma e documenti descrittivi delle funzioni della struttura organizzativa;
- sistema dei poteri e delle deleghe;
- Codice Etico;
- procedure e disposizioni operative;
- sistema sanzionatorio esistente.

Fase II - Identificazione delle attività "sensibili" e dei presidi in essere (Risk assessment) e di eventuali ambiti di rafforzamento degli stessi (Gap analysis)

Successivamente alla raccolta di tutto il materiale di cui alla Fase I, si è proceduto – tenuto conto della specifica operatività della Società – alla individuazione e rappresentazione in apposite schede di Risk assessment & Gap analysis delle attività "sensibili" o "a rischio" di realizzazione dei reati e illeciti amministrativi rilevanti ai sensi del Decreto.

L'identificazione delle attività sensibili è stata effettuata con il diretto coinvolgimento dei Responsabili delle strutture organizzative della Società. I risultati degli incontri sono stati documentati nelle schede di Risk assessment & Gap analysis, debitamente validate e archiviate.

Una volta identificate le attività sensibili, sono stati rilevati – sempre tramite analisi documentale e interviste ai referenti – i presidi di controllo in essere aventi efficacia in termini di prevenzione dei rischi-reato, verificando quindi l'adeguatezza degli stessi presidi e individuando eventuali ambiti di adeguamento e/o rafforzamento, formalizzati nell'apposito documento "Action plan 231" (inerenti, a titolo esemplificativo e non esaustivo, al rafforzamento dei presidi rilevati in riferimento a processi definiti e formalizzati, alla definizione e/o formalizzazione nel corpo normativo interno dei processi a cui sono connesse prassi operative non puntualmente definite/strutturate e/o formalizzate, al rafforzamento del sistema dei poteri e delle deleghe).

Fase III - Elaborazione dei protocolli

I protocolli, riportati nella Parte Speciale del Modello, contengono i principi di controllo e di comportamento (che trovano declinazione nei presidi di controllo rilevati in fase di Risk assessment & Gap analysis) definiti con l'obiettivo di stabilire le regole, cui la Società deve adeguarsi con riferimento all'espletamento delle attività definite sensibili.

In particolare, i protocolli identificano:

- la segregazione funzionale delle attività operative e di controllo;
- la documentabilità delle operazioni a rischio e dei controlli posti in essere per impedire la commissione dei reati e/o degli illeciti amministrativi;

- la ripartizione e attribuzione dei poteri autorizzativi e decisionali, nonché delle responsabilità delle strutture della Società, basate su principi di trasparenza, chiarezza e verificabilità delle operazioni, in conformità al Sistema dei poteri e delle deleghe adottato dalla Società stessa.

La scelta di seguire tale approccio è stata effettuata considerando che tale modalità consente di valorizzare al meglio il patrimonio conoscitivo della Società in termini di regole e normative interne che indirizzano e governano la formazione e l'attuazione delle decisioni della Società in relazione agli illeciti da prevenire e, più in generale, la gestione dei rischi e l'effettuazione dei controlli. Inoltre tale approccio permette di gestire con criteri univoci le regole operative aziendali, incluse quelle relative alle aree "sensibili" e, da ultimo, rende più agevole la costante implementazione e l'adeguamento tempestivo dei processi e dell'impianto normativo interni ai mutamenti della struttura organizzativa e dell'operatività aziendale, assicurando un elevato grado di "dinamicità" del Modello.

Il presidio dei rischi rivenienti dal D.Lgs. 231/2001 è pertanto assicurato dal presente documento ("Modello di organizzazione, gestione e controllo") e dall'impianto normativo esistente, che ne costituisce parte integrante e sostanziale. In tale contesto, il presidio dei rischi è facilitato da apposite matrici di collegamento tra i protocolli del Modello e i documenti di normativa interna contenenti presidi di controllo, nonché tra i protocolli stessi e le attività a rischio-reato individuate nelle schede di Risk assessment & Gap analysis, ove per ciascuna di tali attività è indicata la normativa interna ove sono formalizzati i presidi.

Quanto definito nei protocolli di decisione viene verificato e confermato tramite la condivisione da parte dei soggetti titolari delle attività sensibili ivi descritte, delle matrici descrittive delle attività a rischio-reato e dei presidi in essere.

5. ORGANISMO DI VIGILANZA

5.1 Composizione e nomina dell'OdV

In attuazione di quanto previsto dal Decreto e in coerenza con le norme statutarie, l'Amministratore Unico della Società nomina l'Organismo di Vigilanza (di seguito anche "OdV"), al quale è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello, nonché di curarne l'aggiornamento.

Si evidenzia che, in considerazione delle dimensioni e della complessità organizzativa della Società, di quanto previsto in materia dalle linee guida delle associazioni di categoria, nonché in assenza di specifiche indicazioni prescrittive in argomento da parte del Decreto, l'Amministratore Unico ha optato per l'istituzione di un organismo a composizione monocratica, affidando l'incarico di componente dell'OdV a un soggetto identificato tra i sindaci effettivi dei Collegi Sindacali della Capogruppo e/o delle altre società del Gruppo doValue.

La rinuncia da parte del componente dell'OdV può essere esercitata in qualsiasi momento e deve essere comunicata all'Amministratore Unico per iscritto unitamente alle motivazioni che l'hanno determinata.

La durata in carica dell'OdV coincide, ove non diversamente previsto, con quella dell'Amministratore Unico che l'ha nominato, con possibilità di rielezione.

Al fine di assicurare l'operatività dell'Organismo di Vigilanza anche nei casi di sospensione ovvero di temporaneo impedimento del componente, l'Amministratore Unico nomina altresì un componente supplente, che subentra al componente effettivo che si venga a trovare in una delle predette situazioni.

Il funzionamento dell'Organismo di Vigilanza è disciplinato da un apposito Regolamento, approvato dal medesimo Organismo.

In ossequio a quanto previsto dal D.Lgs. 231/2001, è necessario che l'Organismo di Vigilanza improntì le proprie attività a criteri di autonomia e indipendenza, professionalità e continuità di azione, così da assicurare un'effettiva ed efficace attuazione del Modello.

5.2 Requisiti

Requisiti soggettivi di eleggibilità

La nomina quale componente dell'OdV è condizionata alla presenza dei requisiti soggettivi di eleggibilità.

Costituiscono motivi di ineleggibilità e/o di decadenza da componente dell'OdV di doData:

- trovarsi in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;
- trovarsi in una delle condizioni di ineleggibilità o decadenza previste dall'art. 2382 del codice civile;
- avere titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere di esercitare una notevole influenza su doData o su società dalla stessa controllate;
- essere stato sottoposto a misure di prevenzione ai sensi della legge 27 dicembre 1956, n. 1423 o della legge 31 maggio 1965, n. 575 e successive modificazioni e integrazioni, salvi gli effetti della riabilitazione;
- aver riportato sentenza di condanna o patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:
  - per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267 (legge fallimentare);
  - per uno dei delitti previsti dal titolo XI del Libro V del codice civile (società e consorzi);

- per un delitto non colposo, per un tempo non inferiore a un anno.
- per un delitto contro la P.A., contro la fede pubblica, contro il patrimonio, contro l'economia pubblica ovvero per un delitto in materia tributaria;
- per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;

- aver riportato, in Italia o all'estero, sentenza di condanna o di patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione, per le violazioni rilevanti ai fini della responsabilità amministrativa degli enti ex D.Lgs. 231/2001;
- essere destinatario di un decreto che dispone il giudizio per tutti i reati/illeciti previsti dal D.Lgs. 231/2001.

Autonomia e indipendenza

L'autonomia e l'indipendenza dell'OdV sono garantite:

- dal posizionamento, indipendente da qualsiasi Funzione, all'interno della struttura organizzativa aziendale;
- dal possesso dei requisiti di indipendenza, onorabilità e professionalità del componente dell' OdV;
- dalle linee di riporto verso il Vertice aziendale attribuite all'OdV;
- dalla insindacabilità, da parte di alcun altro organismo o struttura aziendale, delle attività poste in essere dall'OdV;
- dall'autonomia nello stabilire le proprie regole di funzionamento mediante l'adozione di un proprio Regolamento;
- da specifici poteri di spesa in capo all'OdV, sulla base di un budget annuale.

L'OdV dispone di autonomi poteri di spesa sulla base di un budget annuale, approvato dall'Amministratore Unico, su proposta dell'OdV stesso. In ogni caso, quest'ultimo può richiedere un'integrazione del budget assegnato, qualora non sufficiente all'efficace espletamento delle proprie incombenze, e può estendere la propria autonomia di spesa di propria iniziativa in presenza di situazioni eccezionali o urgenti, che saranno oggetto di successiva relazione all'Amministratore Unico.

All'OdV e alla struttura della quale esso si avvale sono riconosciuti, nel corso delle verifiche ed ispezioni, i più ampi poteri al fine di svolgere efficacemente i compiti affidatigli, l'OdV deve altresì godere di garanzie tali da impedire che esso stesso o il suo componente possano essere rimossi o penalizzati in conseguenza dell'espletamento dei loro compiti.

Nell'esercizio delle sue funzioni, il componente dell'OdV non deve trovarsi in situazioni, anche potenziali, di conflitto di interesse con doData e le altre società del Gruppo derivanti da qualsivoglia ragione (ad esempio di natura personale o familiare). In tali ipotesi, esso è tenuto ad astenersi dall'adottare delibere in materia e ad informare immediatamente l'Amministratore Unico, il quale, in tale ambito, assume gli opportuni provvedimenti.

Professionalità

L'OdV deve essere composto da un soggetto dotato di adeguata esperienza aziendale e delle cognizioni tecniche e giuridiche necessarie per svolgere efficacemente le attività proprie dell'Organismo.

In particolare il componente dell'OdV deve possedere una consistente esperienza aziendale, maturata all'interno di doData ovvero in società con connotazioni simili per quanto attiene l'attività svolta.

L'OdV può essere coadiuvato, nell'ambito delle proprie attività di vigilanza, dalle Funzioni della Società (eventualmente accentrate presso la Capogruppo e/o esternalizzate presso le altre Società del Gruppo), per gli ambiti di rispettiva competenza, e in primis della Funzione Compliance, con il supporto della Funzione Internal Audit.

Ove necessario, l'OdV può avvalersi, con riferimento all'esecuzione delle operazioni tecniche necessarie per lo svolgimento della funzione di controllo, anche di consulenti esterni. In tal caso, i consulenti dovranno sempre riferire i risultati del loro operato all'OdV.

Continuità di azione

L'OdV deve essere in grado di garantire la necessaria continuità nell'esercizio delle proprie funzioni, anche attraverso la programmazione e pianificazione dell'attività e dei controlli, la verbalizzazione delle riunioni e la disciplina dei flussi informativi provenienti dalle strutture aziendali.

5.3 Definizione dei compiti e dei poteri dell'Organismo di Vigilanza

All'Organismo di Vigilanza è affidato il compito di:

- vigilare sull'efficienza, efficacia e adeguatezza del Modello nel prevenire e contrastare la commissione degli illeciti di cui al Decreto;
- vigilare costantemente sull'osservanza delle prescrizioni contenute nel Modello da parte dei Destinatari, rilevando la coerenza e gli eventuali scostamenti dei comportamenti attuati, attraverso l'analisi dei flussi informativi e le segnalazioni pervenute dai Destinatari del Modello nonché da soggetti tenuti al rispetto dei principi etici societari e alle norme specifiche di cui al Modello;
- effettuare un'adeguata attività ispettiva per accertare il verificarsi di violazioni del Modello, coordinandosi di volta in volta con le Funzioni interessate per acquisire tutti gli elementi utili all'indagine;
- vigilare, a seguito dell'accertata violazione del Modello, sull'avvio e sullo svolgimento del procedimento di irrogazione di un'eventuale sanzione disciplinare;
- curare l'aggiornamento del Modello nel caso in cui si riscontrino esigenze di adeguamento, formulando proposte agli organi societari competenti, ovvero laddove si rendano opportune modifiche e/o integrazioni in conseguenza di significative violazioni delle prescrizioni del Modello stesso, di significativi mutamenti dell'assetto organizzativo e procedurale della Società, di novità legislative intervenute in materia, nonché in ogni altra situazione prevista ai sensi del documento "Governance di Gruppo in materia di Modelli 231";
- verificare l'attuazione del piano di formazione del personale di cui al successivo capitolo 7.2;
- conservare tutta la documentazione relativa alle attività sopra specificate.

Nello svolgimento delle predette attività, l'OdV può avvalersi del supporto di altre Funzioni interne della Società e di consulenti esterni con specifiche competenze, il cui apporto professionale si renda di volta in volta necessario, senza necessità di ottenere specifiche autorizzazioni da parte del vertice societario.

L'Amministratore Unico dà incarico all'Organismo di Vigilanza di curare l'adeguata comunicazione alle strutture aziendali del Modello, dei compiti dell'OdV e dei suoi poteri.

Il componente dell'OdV, nonché i soggetti dei quali l'OdV stesso, a qualsiasi titolo, si avvale, sono tenuti a rispettare l'obbligo di riservatezza su tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni (fatte salve le attività di reporting all'Amministratore Unico previste dal Modello).

Il componente dell'Organismo di Vigilanza assicura la riservatezza delle informazioni di cui venga in possesso, in particolare se relative a segnalazioni che allo stesso dovessero pervenire in ordine a presunte violazioni del Modello. Il componente dell'Organismo di Vigilanza si astiene dal

ricevere e utilizzare informazioni riservate per fini diversi da quelli compresi nel presente paragrafo, e comunque per scopi non conformi alle funzioni proprie dell'Organismo di Vigilanza, fatto salvo il caso di espressa e consapevole autorizzazione.

Ogni informazione in possesso del componente dell'Organismo di Vigilanza deve essere comunque trattata in conformità con la vigente legislazione in materia e, in particolare, in conformità al D.Lgs. 196/2003 ("Codice Privacy") e al Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation - Regolamento UE 2016/679) e successivi aggiornamenti.

Ogni informazione, segnalazione, report, relazione previsti nel Modello sono conservati dall'OdV in un apposito archivio (informatico e/o cartaceo).

5.4 Reporting dell'Organismo di Vigilanza

Al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'OdV relaziona direttamente all'Amministratore Unico della Società.

L'OdV riferisce all'Amministratore Unico annualmente, in merito alle seguenti tematiche:

- esiti dell'attività di vigilanza espletata nel periodo di riferimento, con l'indicazione di eventuali problematiche o criticità emerse e degli interventi opportuni sul Modello;
- eventuali mutamenti del quadro normativo e/o significative modificazioni dell'assetto organizzativo di doData e/o delle modalità di svolgimento delle attività, che richiedono aggiornamenti del Modello (tale segnalazione ha luogo qualora non si sia previamente proceduto a sottoporla all'Amministratore Unico al di fuori della relazione annuale);
- resoconto delle segnalazioni ricevute, ivi incluso quanto direttamente riscontrato, in ordine a presunte violazioni delle previsioni del Modello e dei protocolli, nonché all'esito delle conseguenti verifiche effettuate;
- provvedimenti disciplinari e sanzioni eventualmente applicate da doData, con riferimento alle violazioni delle previsioni del Modello e dei protocolli;
- rendiconto delle spese sostenute;
- attività pianificate a cui non si è potuto procedere per giustificate ragioni di tempo e risorse;
- piano delle verifiche predisposto per l'anno successivo.

L'OdV potrà in ogni momento chiedere di essere sentito dall'Amministratore Unico qualora accerti fatti di particolare rilevanza, ovvero ritenga opportuno un esame o un intervento in materie inerenti al funzionamento e all'efficace attuazione del Modello.

L'OdV può, a sua volta, essere convocato in ogni momento dall'Amministratore Unico per riferire su particolari eventi o situazioni relative al funzionamento e al rispetto del Modello.

5.5 Flussi informativi nei confronti dell'Organismo di Vigilanza

5.5.1. Flussi informativi ad evento

I flussi informativi hanno a oggetto tutte le informazioni e tutti i documenti che devono essere portati a conoscenza dell'OdV, secondo quanto previsto dal Modello e dai protocolli di decisione, che ne costituiscono parte integrante. Sono stati istituiti in proposito obblighi di comunicazione, gravanti sugli Organi sociali, su tutto il Personale di doData, sui Responsabili delle Strutture Organizzative a cui sono attribuite le Funzioni Aziendali e, in generale, sui Destinatari del Modello.

In particolare, i Responsabili delle strutture organizzative, che svolgono attività sensibili in accordo con le rispettive attribuzioni organizzative, devono comunicare all'OdV, con la necessaria tempestività ed in forma scritta, ogni informazione riguardante:

- eventuali documenti di reporting predisposti dalle Strutture Organizzative/ Organi di Controllo (compresa la Società di Revisione) nell'ambito delle rispettive attività di verifica, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza del D.Lgs. 231/01 e/o del Modello. Si fa riferimento, in particolare, a documenti differenti rispetto a quelli già oggetto di "Flussi informativi periodici" verso l'OdV (ad esempio, verbali delle verifiche delle FAC relativi a temi non presenti nelle relazioni periodiche inviate/ in corso di invio entro la scadenza del presente flusso);
- le indagini disciplinari avviate per presunte violazioni del Modello. Successivamente, a esito delle indagini, evidenza dei provvedimenti disciplinari eventualmente applicati ovvero dei provvedimenti di archiviazione e delle relative motivazioni;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D.Lgs. 231/2001 e che possano coinvolgere doData;
- notizie:
  - dello svolgimento di procedimenti giudiziari aventi a oggetto la responsabilità amministrativa degli enti *ex* D.Lgs. 231/01 in cui sia coinvolta doData e, alla loro conclusione, i relativi esiti;
  - di eventuali sentenze di condanna di dipendenti di doData a seguito del compimento di reati rientranti tra quelli presupposto del D.Lgs. 231/01;
- notizie dell'avvio di visite, ispezioni e accertamenti da parte degli enti competenti (quali, ad esempio, Guardia di Finanza, Agenzia delle Entrate, ASL, INPS, INAIL) o da parte di Autorità di Vigilanza e, alla loro conclusione, i relativi esiti;
- segnalazioni di incidenti/infortuni, anche derivanti da fattori esterni (ad esempio, rapine), che hanno comportato lesioni gravi o gravissime a dipendenti e/o a terzi;
- variazioni intervenute nel Sistema dei Poteri e delle Deleghe della Società con impatti rilevanti ai fini del *Risk Assessment* e del Modello *ex* D.Lgs. 231/01 di doData (a titolo esemplificativo, le variazioni devono intendersi rilevanti ai fini del flusso in oggetto laddove interessino deleghe di poteri e/o procure che costituiscono livelli autorizzativi nell'ambito di attività sensibili/Protocolli);
- variazioni intervenute nella struttura organizzativa con impatti rilevanti ai fini del *Risk Assessment* e del Modello *ex* D.Lgs. 231/01 di doData (a titolo esemplificativo, le variazioni devono intendersi rilevanti ai fini del flusso in oggetto laddove interessino Strutture Organizzative in relazione all'operatività delle quali sono state individuate attività sensibili in fase di *Risk Assessment*).

Tutti i Destinatari del Modello devono inoltre segnalare tempestivamente all'OdV gli eventi di seguito riportati dei quali vengano direttamente o indirettamente a conoscenza:

la commissione, la presunta commissione o il ragionevole pericolo di commissione di reati o illeciti previsti dal D.Lgs. 231/2001;

le violazione o le presunte violazioni del Modello o dei protocolli di decisione;

ogni fatto/comportamento/situazione con profili di criticità e che potrebbe esporre doData alle sanzioni di cui al D.Lgs. 231/2001.

I soggetti esterni, come definiti nel paragrafo "*Destinatari*", sono tenuti a informare immediatamente l'OdV con riguardo a notizie relative a fatti/atti che potrebbero determinare profili di criticità ai sensi del D.Lgs. 231/01 e/o violazioni o presunte violazioni del Modello di doData, emerse nell'ambito del rapporto tra gli stessi e doData (ad esempio, ricezione in modo diretto o indiretto, da parte di un dipendente/ rappresentante di doData, di richieste di comportamenti che potrebbero determinare una violazione del Modello). Detto obbligo deve essere specificato, a cura della struttura competente, nei contratti che legano tali soggetti a doData.

L'obbligo di informazione su eventuali comportamenti contrari alle disposizioni contenute nel Modello e nei protocolli di decisione rientra nel più ampio dovere di diligenza e obbligo di fedeltà del prestatore di lavoro.

Il corretto adempimento dell'obbligo di informazione da parte del prestatore di lavoro non può dar luogo all'applicazione di sanzioni disciplinari.

Le informazioni di cui sopra possono essere segnalate, anche in forma anonima, e pervenire all'OdV tramite una delle seguenti modalità:

- casella di posta elettronica: FlussiOdv-doData@dovalue.it
- posta cartacea, anche in forma anonima, al seguente indirizzo:

  doData S.r.l.
  C/A Organismo di Vigilanza 231/2001
  Lungotevere Flaminio, 18
  00196 Roma

- attraverso altri canali alternativi interni di segnalazione delle violazioni (c.d. "whistleblowing"), eventualmente implementati a livello locale: accesso all'applicativo dedicato presente sul sito istituzionale della Capogruppo www.dovalue.it.

L'Organismo di Vigilanza valuta le segnalazioni ricevute, comprese quelle anonime purché presentino elementi fattuali, e adotta gli eventuali provvedimenti conseguenti a sua ragionevole discrezione e responsabilità, ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna. L'OdV può dare luogo a tutti gli accertamenti e le indagini che ritenga necessarie ad appurare il fatto segnalato. Le determinazioni dell'OdV in ordine all'esito dell'accertamento devono essere motivate per iscritto.

L'OdV agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi atto di ritorsione, discriminazione o penalizzazione o qualsivoglia conseguenza derivante dagli stessi. Tali atti nei confronti dei segnalanti sono assolutamente vietati. È altresì assicurata la riservatezza dell'identità dei segnalanti, fatti comunque salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Ogni informazione e segnalazione prevista nel Modello è conservata dall'OdV in un apposito archivio informatico e/o cartaceo per un periodo di dieci anni, in conformità alle vigenti disposizioni in materia di tutela dei dati personali (Regolamento generale per la protezione dei dati personali n. 2016/679, daGDPR). L'accesso al database è pertanto consentito esclusivamente all'OdV e ai soggetti da questo espressamente autorizzati per iscritto.

Oltre agli obblighi di segnalazione di cui sopra, l'Alta Direzione è tenuta a comunicare all'OdV ogni informazione rilevante per il rispetto, il funzionamento e l'adeguamento del presente Modello.

Le modalità e le tempistiche di flussi informativi diretti all'OdV per specifiche aree di attività a potenziale rischio-reato potranno essere meglio dettagliate dallo stesso OdV nel proprio Regolamento.

L'eventuale omessa o ritardata comunicazione all'OdV dei flussi informativi sopra elencati sarà considerata violazione del Modello e potrà essere sanzionata secondo quanto previsto dal sistema disciplinare di cui all'apposito successivo capitolo.

Fermi restando i suesposti canali di segnalazione, per i quali sono in ogni caso previste le misure di tutela dei segnalanti di seguito descritte, è presente un canale alternativo di segnalazione all'Organismo di Vigilanza delle informazioni di cui sopra idoneo a garantire, con modalità informatiche, la riservatezza dell'identità dei segnalanti. Le modalità di accesso a tale canale alternativo e di utilizzo dello stesso sono rappresentate nella regolamentazione interna

disciplinante il sistema interno di segnalazione delle violazioni (c.d. "**whistleblowing**[20]") adottato dalla Società, alla quale è fatto rimando. La citata procedura trova applicazione con riguardo alle segnalazioni[21] che hanno ad oggetto violazioni che possono avere impatto sulle Società del Gruppo doValue e sulle attività dalle stesse esercitate. Qualora la segnalazione riguardi violazioni del Modello Organizzativo adottato ai sensi del D. Lgs. 231/01 ovvero un reato contemplato dal citato Decreto, la Società ha individuato per la Capogruppo e per le controllate italiane, quale Responsabile della Segnalazione, l'Organismo di Vigilanza delle rispettive Società del Gruppo.

[20] In data 29 dicembre 2017 è entrata in vigore la Legge 30 novembre 2017, n. 179 recante le "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" che è intervenuta sull'art. 54-bis del D. Lgs. n. 165/2001 e sull'art. 6 del D. Lgs. n. 231/2001.

Il Legislatore, nel tentativo di armonizzare le disposizioni previste per il settore pubblico con la richiamata Legge, ha introdotto specifiche previsioni per gli enti destinatari del D. Lgs. n. 231/2001 ed ha inserito all'interno dell'art. 6 del D. Lgs. n. 231/2001 tre nuovi commi, ovvero il comma 2-bis, 2- ter e 2-quater.

In particolare l'art. 6 dispone:

• al comma 2-bis che i Modelli di Organizzazione, Gestione e Controllo devono prevedere:

- uno o più canali che consentano ai soggetti indicati nell'art. 5, comma 1, lettere a) e b) , di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto e fondate su elementi di fatto precisi e concordanti, ovvero di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

- almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;

- il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;

- nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate;

• al comma 2-ter prevede che l'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di ci al comma 2-bis può essere denunciata all'Ispettorato del Lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo;

• al comma 2-quater è disciplinato il licenziamento ritorsivo o discriminatorio del soggetto segnalante, che viene espressamente qualificato come "nullo". Sono altresì indicati come nulli il mutamento di mansioni ai sensi dell'art. 2103 c.c., nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante.

Il predetto articolo, inoltre, prevede che in caso di controversie legate all'erogazione di sanzioni disciplinari, demansionamenti, licenziamenti, trasferimenti ovvero sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi sulle condizioni di lavoro, spetta al datore di lavoro provare che tali misure siano state adottate sulla base di ragioni estranee alla segnalazione.

La Legge sul whistleblowing introduce nell'ordinamento giuridico italiano un apparato di norme volto a migliorare l'efficacia degli strumenti di contrasto ai fenomeni corruttivi, nonché a tutelare con maggiore intensità gli autori delle segnalazioni incentivando il ricorso allo strumento della denuncia di condotte illecite o di violazioni dei modelli di organizzazione, gestione e controllo gravando il datore di lavoro dell'onere di dimostrare - in occasione di controversie legate all'irrogazione di sanzioni disciplinari, demansionamenti, licenziamenti, trasferimenti o alla sottoposizione del segnalante ad altra misura organizzativa successiva alla presentazione della segnalazione avente effetti negativi, diretti o indiretti, sulla condizione di lavoro - che tali misure risultino fondate su ragioni estranee alla segnalazione stessa (c.d. "inversione dell'onere della prova a favore del segnalante").

In data 15 marzo 2023, è stato pubblicato in Gazzetta Ufficiale il Decreto Legislativo n. 24/2023 del 10 marzo 2023, recante "Attuazione della Direttiva UE n. 2019/1937 riguardante la protezione delle persone che segnalano le violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali" (di seguito il "Decreto" o "Decreto Legislativo"). Il Decreto coordina, in un unico testo normativo, la disciplina relativa alla tutela delle persone che segnalano violazioni nelle realtà lavorative appartenenti ai settori pubblico e privato.

Oltre alle normative sopraelencate, con riguardo al sistema interno per la segnalazione di violazioni, si fa riferimento alla seguente normativa di settore: D.lgs. n. 385/1993 "Testo Unico Bancario - TUB", Linee Guida n. EBA/GL/2021/05 DEL 02/07/2021 "Governance interna CRD", Circolare n. 288 del 3 aprile 2015 "Disposizioni di vigilanza per gli intermediari finanziari" di Banca d'Italia, D. L.gsanticorruzio. 231/2007 "Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE".

[21] Per "*Segnalazione rilevante*" si intende la comunicazione di possibili comportamenti illeciti, commissivi o omissivi che costituiscano o possano costituire una violazione, o induzione a violazione di leggi e/o regolamenti, valori e/o principi sanciti nel Codice Etico, nei principi di controllo interno, oltre che nelle policy e/o norme aziendali.

La procedura adottata dalla Società, alla quale si rimanda, illustra il funzionamento del sistema di segnalazione interno delle condotte illecite, i principi posti a salvaguardia dei soggetti segnalanti, le modalità di invio delle segnalazioni, il relativo processo di gestione, nonché ogni possibile azione conseguente alle violazioni riscontrate.

La Società e l'OdV agiscono in modo da garantire i segnalanti contro qualsiasi forma di ritorsione o comportamenti discriminatori, diretti o indiretti, per motivi collegati, direttamente o indirettamente, alla segnalazione.

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 il procedimento di segnalazione interno adottato, anche attraverso la predisposizione e l'aggiornamento – a cura delle competenti Strutture – di iniziative di formazione obbligatoria sul whistleblowing a favore di tutti i Dipendenti, così da evidenziare le specifiche procedure da seguire e le possibili conseguenze nel caso si verifichino comportamenti inappropriati.

5.5.2 Flussi informativi periodici

L'Organismo di Vigilanza esercita le proprie responsabilità di controllo anche mediante l'analisi di sistematici flussi informativi periodici trasmessi dalle Funzioni Internal Audit, Antiriciclaggio, People, nonché dalle U.O. Group Enterprise Risk Management, Compliance & DPO, dal Dirigente Preposto, dal Responsabile Anticorruzione di Gruppo e dal Datore di Lavoro/Committente ai sensi del D.Lgs. n. 81/2008, nonché dai Responsabili delle Strutture Organizzative a cui sono attribuite le Funzioni Aziendali diverse da quelle sopra enunciate. In particolare:

- Internal Audit di Capogruppo trasmette:
  - il Piano annuale delle Attività, con evidenza di quelle aventi "rilevanza 231" e della relativa pianificazione temporale. Per ciascuna attività rilevante anche ai fini dei compiti di vigilanza sul funzionamento e l'osservanza del Modello ex D.Lgs. 231/01 della Società – di competenza dell'Organismo di Vigilanza – indicazione della/e Parte/i e/o del/i Protocollo/i del Modello per cui l'attività assume rilevanza;
  - rendicontazioni/relazione trimestrali/annuale, contenenti un'informativa circa le verifiche svolte, le principali risultanze, le azioni riparatrici pianificate, gli ulteriori interventi di controllo in programma nel periodo successivo, in linea con il Piano annuale. Laddove ne ravvisi la necessità, l'Organismo di Vigilanza richiede alla Funzione Internal Audit copia dei report di dettaglio per i punti specifici che ritiene di voler meglio approfondire;
- Antiriciclaggio di Capogruppo trasmette:
  - il Piano annuale delle Attività, con evidenza di quelle aventi "rilevanza 231" e della relativa pianificazione temporale. Per ciascuna attività rilevante anche ai fini dei compiti di vigilanza sul funzionamento e l'osservanza del Modello ex D.Lgs. 231/01 della Società – di competenza dell'Organismo di Vigilanza – indicazione della/e Parte/i e/o del/i Protocollo/i del Modello per cui l'attività assume rilevanza;
  - rendicontazioni/relazione semestrali/annuale, concernenti un'informativa circa l'esito dell'attività svolta in relazione alle attività di prevenzione e gestione del rischio di riciclaggio e finanziamento al terrorismo, nonché agli interventi correttivi e migliorativi pianificati (inclusi quelli formativi) ed al loro stato di realizzazione;
  - una relazione annuale che sintetizza i risultati dell'esercizio di autovalutazione dell'esposizione al rischio di riciclaggio della Capogruppo per ciascuna linea di business / area geografica in cui opera la società;
- Dirigente Preposto di Capogruppo trasmette una relazione annuale contenente il perimetro delle Società e dei processi sensibili oggetto dei test svolti nel corso dell'anno, specificando le eventuali valutazioni quantitive e qualitative che hanno portato ad una variazione degli stessi rispetto alla puntuale applicazione delle regole metodologiche e comunicando gli esiti delle valutazioni di affidabilità ed adeguatezza;

- Group Enterprise Risk Management trasmette:
  - il Piano annuale delle Attività, con evidenza di quelle aventi "rilevanza 231" e della relativa pianificazione temporale. Per ciascuna attività rilevante anche ai fini dei compiti di vigilanza sul funzionamento e l'osservanza del Modello ex D.Lgs. 231/01 della Società – di competenza dell'Organismo di Vigilanza – indicazione della/e Parte/i e/o del/i Protocollo/i del Modello per cui l'attività assume rilevanza;
  - una relazione annuale, contenente un'informativa circa le verifiche svolte, le principali risultanze, le azioni riparatrici pianificate e il relativo stato di implementazione, gli ulteriori interventi di controllo in programma nel semestre successivo, in linea con il Piano annuale della Funzione;
- Responsabile Anticorruzione di Capogruppo trasmette:
  - una relazione annuale, in merito all'efficacia, all'adeguatezza e allo stato di implementazione del Sistema Anticorruzione;
  - un'informativa contenente gli esiti delle attività di verifica condotte al fine di monitorare la corretta applicazione del Sistema Anticorruzione del Gruppo;
- Compliance & DPO di Capogruppo trasmette una rendicontazione trimestrale contenente un'informativa circa le principali risultanze (azioni riparatrici, incluse quelle formative, e il relativo stato di implementazione) derivanti dallo svolgimento delle attività di monitoraggio relative ad eventuali piani d'azione contenenti interventi di adeguamento (in termini di struttura organizzativa, processi, procedure e altri elementi del Sistema dei Controlli Interni) necessari al fine di attuare effettivamente il Modello della Società. L'U.O. Compliance & DPO trasmette altresì le principali evidenze emerse dall'analisi consolidata delle Schede "Reporting informativo per l'Organismo di Vigilanza" prodotte dai Responsabili delle Strutture Organizzative, come specificate di seguito;
- Legal & Compliance di Capogruppo trasmette un flusso di rendicontazione annuale sullo stato di allineamento del Sistema dei Poteri e delle Deleghe;
- People di Capogruppo trasmette:
  - un flusso di rendicontazione con cadenza semestrale:
    - i provvedimenti disciplinari eventualmente comminati al personale dipendente nel periodo di riferimento, con evidenza dei provvedimenti applicati per violazione del Modello;
    - l'attività di formazione e informazione/sensibilizzazione dei Destinatari del Modello (come prevista ai sensi del capitolo *"Informazione e formazione del personale"*) eseguita nel periodo di riferimento e pianificata per il periodo successivo;
    - un'informativa delle principali variazioni intervenute nella struttura organizzativa (comprese eventuali modifiche intervenute a livello di Gruppo aventi impatti sulla struttura della Società), nei processi e nelle procedure;
  - una relazione annuale contenente l'esito delle attività svolte in relazione all'organizzazione e al controllo effettuato sul sistema di gestione aziendale della salute e sicurezza nei luoghi di lavoro;
  - a seguito dell'insorgere o del permanere di emergenze epidemiche/pandemiche (per es: Covid-2019), un'informativa sulle misure organizzative e di controllo adottate per la gestione dell'emergenza e stato della loro attuazione, comprese quelle relative alla informazione/formazione dei dipendenti in materia di salute e sicurezza, eventuali criticità rilevate nella loro osservanza da parte dei dipendenti; numero di contagi nella popolazione aziendale. Tale informativa è da aggiornarsi periodicamente fino alla fine dello stato d'emergenza.
- I Responsabili delle Strutture Organizzative a cui sono attribuite le Funzioni Aziendali, anche diverse da quelle competenti per l'invio dei flussi informativi di cui ai punti precedenti,

trasmettono, con frequenza definita in relazione a ciascun flusso, la Scheda "Reporting informativo per l'Organismo di Vigilanza". In tali Schede attestano, con frequenza annuale, il livello di attuazione del Modello con particolare attenzione al rispetto, nell'ambito dell'operatività di propria competenza, dei principi di controllo e comportamento, evidenziando in particolare: *(i)* le eventuali criticità nei processi gestiti, *(ii)* gli eventuali scostamenti rispetto alle previsioni del Modello e della normativa interna, *(iii)* l'adeguatezza della medesima normativa interna rispetto agli ambiti operativi d'interesse e le eventuali misure risolutive adottate o il piano per la relativa adozione. Le Schede in oggetto sono inviate, a cura dei Responsabili delle Strutture Organizzative, alla U.O. Compliance & DPO di Capogruppo, la quale archivia la documentazione, tenendola a disposizione dei membri degli Organismi di Vigilanza della Società e produce una relazione annuale volta a informare l'Organismo di Vigilanza della Società delle principali evidenze emerse dall'analisi consolidata delle Schede in argomento.

Inoltre, l'OdV definisce una serie di obblighi informativi periodici a carico di individuate Strutture Organizzative della Società, in ragione delle specifiche attribuzioni organizzative di cui esse sono titolari e, di conseguenza, delle attività sensibili nelle quali le stesse sono coinvolte ("flussi informativi specifici"). Al fine di agevolare l'adempimento a tali obblighi informativi da parte dei Destinatari, è prediposto un documento, costituente parte integrante del Modello, in cui sono descritti i flussi informativi specifici verso l'Organismo di Vigilanza in relazione a ciascun Area Sensibile/Protocollo. In tale documento è data altresì evidenza delle informazioni necessarie per l'adeguata e puntuale predisposizione e trasmissione dei flussi in oggetto, i quali ove previsti sono integrati nella Scheda "Reporting informativo per l'Organismo di Vigilanza", già prodotta dai Responsabili delle Strutture Organizzative.

Infine, nel normale svolgimento delle proprie funzioni e in ragione di considerazioni "risk-based", l'Organismo di Vigilanza della Società si riserva di definire flussi informativi (ad evento o periodici) diversi da quelli sopra elencati.

5.6 Informativa verso gli Organi della Capogruppo

In considerazione dell'appartenenza della Società al Gruppo doValue, l'Organismo di Vigilanza di doData può ricevere da parte dell'OdV della Capogruppo specifiche richieste di informazioni, qualora le stesse siano necessarie ai fini dello svolgimento delle attività di controllo della Capogruppo stessa. A tal riguardo l'OdV della Società è obbligato ad adempiere alle richieste formulate dall'OdV della Capogruppo.

Inoltre, al fine di garantire la direzione unitaria e il coordinamento della Capogruppo doValue nei confronti delle Società contollate italiane – ivi inclusa doData – sotto il profilo organizzativo, gestionale e di controllo:

- l'OdV di doData comunica all'OdV di doValue l'avvenuta adozione/aggiornamento del Modello approvato dall' Amministratore Unico e lo trasmette allo stesso Organismo. A tal riguardo, l'OdV della Capogruppo può richiedere momenti di confronto con l'OdV di doData per eventuali necessità di approfondimento/coordinamento (e.g. in merito a peculiari profili di rischio);
- nell'ambito dei compiti attribuitigli, l'OdV di doData segnala tempestivamente all'OdV della Capogruppo i seguenti eventi dei quali venga – direttamente o indirettamente – a conoscenza relativamente a:
  - la commissione, la presunta commissione o il ragionevole pericolo di commissione di reati o illeciti previsti dal D.Lgs. 231/2001;
  - le violazioni o le presunte violazioni del Modello o dei protocolli di decisione;
  - ogni fatto/comportamento/situazione con profili di criticità e che potrebbe esporre la Società alle sanzioni di cui al D.Lgs. 231/2001;

- l'OdV delle Società del Gruppo inoltre, in generale, attivano canali informativi e comunicativi volti a favorire lo scambio di informazioni rilevanti ai fini della gestione dei rischi nell'ambito del Gruppo. In particolare:
  - l'OdV di doData trasmette all'OdV della Capogruppo copia della propria relazione annuale, recante le attività svolte nel corso dell'anno;
  - sono organizzati momenti di incontro tra tutti gli OdV delle Società del Gruppo, con frequenza almeno semestrale;
  - inoltre, ciascun OdV può avanzare ulteriori richieste di informazioni agli altri OdV delle Società del Gruppo, nonché di incontri con gli stessi, ove necessario per conseguire una migliore gestione dei rischi a livello di Gruppo.

Eventuali interventi correttivi sul Modello della Società sono di esclusiva competenza della stessa, ferme restando le previsioni di cui al documento "Governance di Gruppo in materia di Modelli 231".

6. IL SISTEMA DISCIPLINARE

Il presente capitolo definisce il sistema disciplinare inerente esclusivamente alle violazioni delle regole e dei principi di controllo e di comportamento definiti nel Modello di organizzazione, gestione e controllo ex D.Lgs. 231/2001, fatte salve le sanzioni previste dalla Società per altre tipologie di infrazioni.

6.1. Principi generali

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

Pertanto, l'adozione di un adeguato sistema disciplinare che sanzioni le violazioni dei principi contenuti nel presente Modello rappresenta un requisito imprescindibile per una piena ed efficace attuazione del Modello stesso.

La definizione di uno specifico sistema di sanzioni, oltre a prevenire la commissione di infrazioni, consente all'OdV di esercitare la funzione di vigilanza con maggiore efficienza e favorisce l'effettiva osservanza del Modello.

Il sistema disciplinare è diretto a sanzionare il mancato rispetto, da parte dei Destinatari, dei principi e delle regole di condotta prescritti nel presente Modello (ivi compresi il Codice Etico e le procedure e norme interne che formano parte integrante del Modello stesso).

Su tale presupposto, doData adotterà nei confronti:

- del proprio personale dipendente, il sistema sanzionatorio stabilito dal Codice disciplinare della Società e dalle leggi che regolano la materia;
- del personale dipendente della Capogruppo e/o di altre Società del Gruppo che eventualmente operi in regime di distacco in nome e per conto della Società o in favore della stessa ("personale distaccato"), il sistema sanzionatorio stabilito dal relativo Codice disciplinare e dalle leggi che regolano la materia e comunque il sistema sanzionatorio vigente nella Società del Gruppo di appartenenza;
- di tutti i soggetti esterni, i provvedimenti stabiliti dalle disposizioni contrattuali e di legge che regolano la materia.

L'attivazione, sulla base delle segnalazioni pervenute dall'Organismo di Vigilanza, lo svolgimento e la definizione del procedimento disciplinare nei confronti del personale dipendente – a seguito di riscontrate violazioni del presente Modello – sono affidati al Responsabile della Funzione Risorse Umane e all'Amministratore Unico di doData ovvero – in caso di violazioni da parte di eventuale personale distaccato – dall'Organo o dai soggetti della Società distaccante muniti dei necessari poteri, in coordinamento con i competenti Organi e/o soggetti di doData. Questi, sentito il superiore gerarchico dell'autore della condotta ed effettuati gli opportuni approfondimenti, è chiamato a determinare e ad adottare il relativo provvedimento disciplinare.

Gli interventi sanzionatori nei confronti dei soggetti esterni sono affidati alla Funzione che gestisce il contratto o presso cui opera il lavoratore autonomo ovvero il fornitore.

Le sanzioni sono commisurate al livello di responsabilità e autonomia operativa del lavoratore, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità e gravità della condotta, ovvero a tutte le altre particolari circostanze che possono aver caratterizzato la violazione del Modello. Le sanzioni sono applicate in conformità all'art. 7 della Legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori), al CCNL vigente all'interno della Società, nonché al Codice disciplinare della Società, ove presente.

Pertanto, gli Organi e/o i soggetti di cui sopra, nel deliberare sulla sanzione applicabile al caso concreto, devono considerare la tipologia di rapporto di lavoro instaurato con il prestatore

(subordinato dirigenziale e non dirigenziale), la specifica disciplina legislativa e contrattuale, nonché i seguenti criteri:

- gravità della violazione;
- tipologia dell'illecito perpetrato;
- circostanza in cui si sono svolti i comportamenti illeciti;
- eventualità che i comportamenti integrino esclusivamente un tentativo di violazione;
- eventuale recidività del soggetto.

L'Organismo di Vigilanza, nell'ambito dei compiti allo stesso attribuiti, monitora costantemente i procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché gli interventi nei confronti dei soggetti esterni, anche con il supporto dei flussi informativi specificatamente previsti in proposito.

In applicazione dei suddetti criteri, viene stabilito il seguente sistema sanzionatorio.

6.2. Provvedimenti per inosservanza da parte dei dipendenti

6.2.1. Aree professionali e quadri direttivi

Al personale appartenente alle aree professionali e ai quadri direttivi sono applicabili i seguenti provvedimenti:

- rimprovero verbale, in caso di lieve inosservanza dei principi e delle regole di comportamento previsti dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle attività sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello;
- rimprovero scritto, in caso di inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle attività sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello in misura tale da poter essere considerata ancorché non lieve, comunque, non grave;
- sospensione dal servizio e dal trattamento economico fino ad un massimo di 10 giorni, in caso di inosservanza dei principi e delle regole di comportamento previste dal presente Modello ovvero di violazione delle procedure e norme interne previste e/o richiamate ovvero ancora di adozione, nell'ambito delle attività sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello in misura tale da essere considerata di una certa gravità, anche se dipendente da recidiva;
- licenziamento per giustificato motivo, in caso di adozione, nell'espletamento delle attività sensibili, di un comportamento caratterizzato da notevole inadempimento delle prescrizioni e/o delle procedure e/o delle norme interne stabilite dal presente Modello, anche se sia solo suscettibile di configurare uno degli illeciti per i quali è applicabile il Decreto;
- licenziamento per giusta causa, in caso di adozione, nell'espletamento delle attività sensibili, di un comportamento consapevole in contrasto con le prescrizioni e/o le procedure e/o le norme interne del presente Modello, che, ancorché sia solo suscettibile di configurare uno degli illeciti per i quali è applicabile il Decreto, leda l'elemento fiduciario che caratterizza il rapporto di lavoro ovvero risulti talmente grave da non consentirne la prosecuzione, neanche provvisoria.

6.2.2. Personale dirigente

Il rapporto dirigenziale si caratterizza per la natura eminentemente fiduciaria. Il comportamento del dirigente oltre a riflettersi all'interno della Società, costituendo modello ed esempio per tutti

coloro che vi operano, si ripercuote anche sull'immagine esterna della medesima. Pertanto, il rispetto da parte dei dirigenti della Società delle prescrizioni del Modello, del Codice Etico, e delle relative procedure di attuazione costituisce elemento essenziale del rapporto di lavoro dirigenziale.

Nei confronti dei dirigenti che abbiano commesso una violazione del Modello, la Funzione Risorse Umane avvia i procedimenti di competenza per effettuare le relative contestazioni e applicare le misure sanzionatorie più idonee, in conformità con quanto previsto dal CCNL applicabile ai dirigenti vigente e, ove necessario, con l'osservanza delle procedure di cui all'art. 7 della Legge 30 maggio 1970, n. 300.

Le sanzioni devono essere applicate nel rispetto dei principi di gradualità e proporzionalità rispetto alla gravità del fatto e della colpa o dell'eventuale dolo. Tra l'altro, con la contestazione può essere disposta cautelativamente la revoca delle eventuali procure affidate al soggetto interessato, fino alla eventuale risoluzione del rapporto in presenza di violazioni così gravi da far venir meno il rapporto fiduciario con la Società.

6.3. Provvedimenti per inosservanza da parte degli amministratori della Società

Nel caso in cui la violazione del Modello sia posta in essere dall'Amministratore Unico, l'OdV deve darne immediata comunicazione all'Assemblea dei Soci, mediante relazione scritta.

L'Assemblea dei Soci procede agli accertamenti necessari e assume i provvedimenti opportuni, in coerenza con le disposizioni normative e statutarie relative alle materie riservate alla competenza dell'Assemblea stessa.

6.4. Provvedimenti per inosservanza da parte dei soggetti esterni destinatari del Modello

Ogni comportamento in violazione del Modello o che sia suscettibile di comportare il rischio di commissione di uno degli illeciti per i quali è applicabile il Decreto, posto in essere dai soggetti esterni, come definiti nel presente Modello, determinerà, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico o negli accordi di convenzione, la risoluzione anticipata del rapporto contrattuale per giusta causa, fatta ovviamente salva l'ulteriore riserva di risarcimento qualora da tali comportamenti derivino danni concreti alla Società.

7. INFORMAZIONE E FORMAZIONE DEL PERSONALE

7.1. Diffusione del Modello

Le modalità di comunicazione del Modello devono essere tali da garantirne la piena pubblicità, al fine di assicurare che i Destinatari siano a conoscenza delle procedure che devono seguire per adempiere correttamente alle proprie mansioni.

L'informazione deve essere completa, tempestiva, accurata, accessibile e continua.

Obiettivo di doData è quello di comunicare i contenuti e i principi del Modello anche ai soggetti che, pur non rivestendo la qualifica formale di dipendente, operano – anche occasionalmente – per il conseguimento degli obiettivi di doData in forza di rapporti contrattuali.

A tal fine è previsto l'accesso diretto ad una sezione apposita della intranet aziendale, nella quale è disponibile e costantemente aggiornata tutta la documentazione di riferimento in materia di D.Lgs. 231/2001.

L'attività di comunicazione e formazione è supervisionata dall'OdV, avvalendosi delle strutture competenti, alle quali è assegnato il compito di promuovere le iniziative per la diffusione della conoscenza e della comprensione del Modello, dei contenuti del D.Lgs. 231/2001, degli impatti della normativa sull'attività di doData, nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello e di promuovere e coordinare le iniziative volte ad agevolare la conoscenza e la comprensione del Modello da parte di tutti coloro che operano per conto di doData.

7.2. Formazione del personale

Ai fini dell'efficace attuazione del Modello, è obiettivo generale della Società garantire a tutti i Destinatari del Modello la conoscenza dei principi e delle disposizioni in esso contenuti.

doData persegue, attraverso un adeguato programma di formazione aggiornato periodicamente e rivolto a tutto il personale dipendente – incluso il personale eventualmente distaccato dalla Capogruppo e/o da altre Società del Gruppo – una loro sensibilizzazione continua sulle problematiche attinenti al Modello, al fine di raggiungere la piena consapevolezza delle direttive aziendali e di essere posti in condizioni di rispettarle in pieno.

Al fine di garantire un'efficace attività di formazione, la Società promuove e agevola la conoscenza dei contenuti del Modello da parte del personale dipendente, con grado di approfondimento diversificato a seconda del loro coinvolgimento nelle attività individuate come sensibili ai sensi del Decreto.

Gli interventi formativi, che potranno essere erogati in modalità e-learning o in aula hanno ad oggetto:

- una parte generale, indirizzata a tutti i dipendenti, volta a illustrare il quadro normativo di riferimento della responsabilità amministrativa degli Enti e i contenuti generali del Modello;
- una parte specifica, differenziata per aree di attività del personale dipendente, diretta a illustrare le attività individuate come sensibili ai sensi del Decreto e i relativi protocolli contenuti nella Parte Speciale del Modello;
- una verifica del grado di apprendimento della formazione ricevuta.

I contenuti formativi sono opportunamente aggiornati in relazione all'evoluzione del contesto normativo e del Modello.

La partecipazione ai corsi formativi è obbligatoria e deve essere documentata attraverso la richiesta della firma di presenza. L'OdV, per il tramite delle preposte Funzioni Aziendali, raccoglie e archivia le evidenze relative all'effettiva partecipazione ai suddetti interventi formativi.

Periodicamente, in coerenza con l'evoluzione della normativa di riferimento e con le modifiche della struttura organizzativa aziendale, si procede alla reiterazione dei corsi, al fine di verificare

l'effettiva applicazione del Modello da parte dei Destinatari nonché la loro sensibilizzazione alle prescrizioni dello stesso, secondo modalità indicate dall'Organismo di Vigilanza all'Amministratore Unico, in coordinamento con le Funzioni Aziendali competenti.

A ogni modo, è compito dell'OdV valutare l'efficacia del piano formativo con riferimento al contenuto dei corsi, alle modalità di erogazione, alla loro reiterazione, ai controlli sull'obbligatorietà della frequenza e alle misure adottate nei confronti di quanti non li frequentino senza giustificato motivo.

8. AGGIORNAMENTO DEL MODELLO

L'adozione e l'efficace attuazione del Modello costituiscono per espressa previsione legislativa una responsabilità dell'Amministratore Unico della Società. L'efficacia del Modello è garantita dalla costante attività di aggiornamento, intesa sia come integrazione sia come modifica delle parti che costituiscono lo stesso.

A titolo esemplificativo, l'aggiornamento del Modello può rendersi necessario in presenza delle seguenti circostanze:

- aggiornamento o modifica del catalogo dei reati presupposto;
- evoluzioni normative e giurisprudenziali;
- modifiche relative alla struttura organizzativa e alle aree di business;
- variazioni della struttura e/o dei contenuti del Modello di Capogruppo aventi impatto sul Modello della Società.

Il potere di aggiornare il Modello compete all'Amministratore Unico, in relazione a:

- modifiche sostanziali, quali a titolo esemplificativo: *(i)* l'aggiornamento o la modifica della struttura e/o dei contenuti delle Aree sensibili e/o dei Protocolli in considerazione di evoluzioni della normativa rilevante ai sensi del Decreto (attinenti per esempio alla variazione del perimetro dei reati rilevanti) o di mutamenti del business (aventi a oggetto, per esempio, l'introduzione di nuovi ambiti di operatività); *(ii)* la modifica della composizione dell'Organismo di Vigilanza;
- modifiche non sostanziali del Modello, quali a titolo esemplificativo quelle dovute a riorganizzazioni aziendali e conseguente riassegnazione a nuove Strutture Organizzative di attività a rischio-reato già individuate e considerate nel Modello, oppure variazioni di carattere formale (per esempio, ridenominazione di attività e/o Strutture Organizzative).

PARTE SPECIALE

9. METODOLOGIA DI INDIVIDUAZIONE DELLE AREE SENSIBILI

L'art. 6, comma 2, del D.Lgs. 231/2001 prevede che il Modello debba "individuare le attività nel cui ambito possono essere commessi reati".

Pertanto, sono state identificate le attività a rischio di commissione dei reati rilevanti ai sensi del D.Lgs. 231/2001 e quelle strumentali, intendendosi rispettivamente le attività il cui svolgimento può dare direttamente adito alla commissione di una delle fattispecie di reato contemplate dal D.Lgs. 231/2001 e le attività in cui, in linea di principio, potrebbero configurarsi le condizioni, le occasioni o i mezzi per la commissione dei reati (in generale "Attività sensibili").

Nella Parte Speciale del Modello, le attività sensibili individuate in fase di *risk assessment* (attività a rischio-reato) sono distribuite in "Aree Sensibili", ciascuna delle quali concerne una o più "famiglie di reato" e/o fattispecie di reato, individuate per comunanza di attività sensibili e "principi di controllo" e "principi di comportamento" aventi efficacia ai fini del presidio dei rischi di commissione dei reati presupposto del D.Lgs. 231/2001.

Le Aree Sensibili identificate nell'ambito del Modello sono le seguenti:

- Area Sensibile I - Reati contro la Pubblica Amministrazione e reato di corruzione tra privati;
- Area Sensibile II - Reati societari;
- Area Sensibile III - Reati di criminalità organizzata e transnazionali;
- Area Sensibile IV - Reati con finalità di terrorismo ed eversione dell'ordine democratico e di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio;
- Area Sensibile V - Reati e illeciti amministrativi di abuso di informazioni privilegiate e manipolazione del mercato;
- Area Sensibile VI - Reati in materia di salute e sicurezza sul lavoro;
- Area Sensibile VII - Reati informatici e relativi al trattamento illecito di dati, nonchè delitti in materia di strumenti di pagamento diversi dal contante;
- Area Sensibile VIII - Reati contro l'industria e il commercio e in materia di violazione del diritto d'autore
- Area Sensibile IX - Reati ambientali e delitti contro il patrimonio culturale;
- Area Sensibile X - Reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
- Area Sensibile XI - Reati tributari.

Nel seguito del documento, per ciascuna di tali Aree Sensibili sono:

- elencati i reati ritenuti rilevanti in relazione all'operatività di doData e che, pertanto, si intendono presidiare (*paragrafo "Fattispecie di reato"*). È previsto il rimando all'Allegato "Reati presupposto del D. Lgs. 231/2001" per un'illustrazione delle fattispecie delittuose;
- indicate le attività a rischio-reato (*paragrafo "Attività sensibili"*);
- definiti i principi di controllo e i principi di comportamento a cui devono attenersi i Destinatari nell'ambito di tutte le attività sensibili identificate (paragrafo *"Principi di controllo e comportamento applicabili a tutte le attività sensibili"*);
- definiti, per ciascuna attività sensibile identificata, i "Protocolli" contenenti principi di controllo e principi di comportamento a cui devono attenersi i Destinatari nell'ambito della specifica attività sensibile (paragrafi *"Principi di controllo"* e *"Principi di comportamento"*).

Si evidenzia che il Modello trova piena attuazione nella realtà della Società attraverso il collegamento di ciascuna Area Sensibile e attività sensibile/ Protocollo con la normativa interna nella quale sono formalizzati anche i presidi di controllo posti in essere dalle Struttura

Organizzative aventi efficacia per la prevenzione della commissione dei reati presupposto. Ciò è consentito mediante apposite matrici di collegamento tra i Protocolli del Modello e i documenti di normativa interna contenenti presidi di controllo, nonché tra i Protocolli stessi e le attività a rischio-reato individuate nelle schede di *risk assessment & gap analysis*, ove per ciascuna di tali attività è indicata la normativa interna ove sono formalizzati i presidi.

Quanto definito dalle Aree Sensibili e in particolare dai Protocolli di seguito rappresentati è volto a garantire il rispetto, da parte della Società, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.