Parte Generale

Modello di Organizzazione e Gestione

ex D.Lgs. n. 231/2001

Approvato dal Consiglio di Amministrazione

in data 22 / 12 / 2023

Corso di Porta Nuova n. 48, 20121 Milano (MI)

Storico aggiornamenti	
Prima versione	dicembre 2023

INDICE

Parte Prima

1. Introduzione

La Parte Generale si propone di illustrare gli elementi essenziali del D.Lgs. 231/2001, senza pretesa di esaustività.

È necessario fornire, anche al lettore meno esperto, gli strumenti basilari per orientarsi nel tecnicismo giuridico proprio della normativa di riferimento.

2. Il decreto legislativo 8 giugno 2001, n. 231 (D.Lgs. 231/2001)

In data 8 giugno 2001 è stato emanato - in esecuzione della Delega di cui all'art. 11 della legge 29 settembre 2000 n. 300 - il D.Lgs. n. 231/2001 recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica".

Il D.Lgs. n. 231/2001 trova il suo fondamento in convenzioni internazionali e comunitarie ratificate dall'Italia, che impongono di prevedere forme di responsabilità – aggiuntive, a determinate condizioni, rispetto alla responsabilità dell'autore del fatto di reato – degli enti per talune fattispecie delittuose (c.d. reati presupposto).

Il D.Lgs. n. 231/2001 ha introdotto per la prima volta in Italia una responsabilità definita "amministrativa" dal Legislatore, che presenta caratteri propri della responsabilità penale, per alcuni reati commessi o tentati, nell'interesse o a vantaggio delle società stesse, dagli Organi Sociali, dai Soggetti in posizione apicale o dai Soggetti sottoposti (art. 5, comma 1, del D.Lgs. n. 231/2001) se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.

La responsabilità amministrativa delle società è ulteriore e diversa rispetto alla responsabilità penale della persona fisica che ha commesso il reato e permane in capo all'ente anche nel caso in cui la persona fisica, autore del reato, non sia identificata o non risulti punibile.

Ai fini della configurabilità della responsabilità "amministrativa" è necessario che il reato sia commesso nell'interesse o a vantaggio dell'ente. Al contrario, la società non risponde se il reato è stato commesso nell'interesse esclusivo proprio o di terzi (art. 5, comma 2, D.Lgs. 231/2003).

La competenza a conoscere degli illeciti amministrativi dell'ente appartiene al giudice penale. Il D.Lgs. n. 231/2001 provvede a disciplinare puntualmente, al Capo III, l'intero procedimento di accertamento e di applicazione delle sanzioni amministrative.

L'accertamento della responsabilità può comportare l'applicazione di sanzioni gravi e pregiudizievoli per l'ente, quali sanzioni pecuniarie, sanzioni interdittive (es. l'interdizione dall'esercizio dell'attività; la sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; il divieto di contrattare con la Pubblica Amministrazione; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi; il divieto di pubblicizzare beni o servizi), confisca e pubblicazione della sentenza.

Tali sanzioni sono applicabili anche quali misure cautelari, prima dell'accertamento di merito in ordine alla sussistenza del reato e dell'illecito amministrativo che da esso dipende, qualora si ravvisi l'esistenza di gravi indizi tali da far ritenere sussistente la responsabilità dell'ente, nonché il pericolo di reiterazione dell'illecito.

3. Le famiglie di reati presupposto *ex* D.Lgs. 231/2001

I Reati Presupposto sono espressamente enumerati nel D.Lgs. n. 231/2001. L'ente non può essere ritenuto responsabile per un fatto costituente reato se la sua responsabilità amministrativa in relazione a quel reato e le relative sanzioni non sono espressamente previste da una legge entrata in vigore prima della commissione del fatto (art. 2).

Si elencano di seguito le "famiglie di reato" attualmente ricomprese nel D.Lgs. n. 231/2001, rinviando all'Allegato A - "Appendice Normativa" del presente documento il dettaglio delle singole fattispecie incluse in ciascuna famiglia:

1. **Indebita percezione di erogazioni**, **truffa** in danno dello Stato o di un ente pubblico o dell'Unione Europea per il conseguimento di erogazioni pubbliche e **frode informatica** in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture (Art. 24, D.Lgs.n.231/2001-rubrica modificata da D.Lgs.n.75 del 14 luglio 2020 e dalla L. n. 137/2023)
2. **Delitti informatici** e **trattamento illecito di dati** (Art. 24-bis, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 48/2008; modificato dal D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019]
3. Delitti di **criminalità organizzata** (Art. 24-ter, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 94/2009 modificato dalla L. 69/2015 e successivamente dalla L.n.236 /2016]
4. **Peculato**, **concussione**, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio (Art. 25, D.Lgs.n.231/2001-rubrica modificata da D.Lgs.n.75 del 14 luglio 2020)
5. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (Art. 25-bis, D.Lgs. n. 231/2001) [articolo aggiunto dal D.L. n. 350/2001, convertito con modificazioni dalla L. n. 409/2001; modificato dalla L. n. 99/2009; modificato dal D.Lgs. 125/2016]
6. **Delitti contro l'industria e il commercio** (Art. 25-bis.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009]
7. **Reati societari** Art. 25-ter, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 61/2002, modificato dalla L. n. 190/2012, dalla L. 69/2015, dal D.Lgs. n.38/2017 e dal D.Lgs. n. 19/2023]
8. Reati con **finalità di terrorismo** o **di eversione dell'ordine democratico** previsti dal codice penale e dalle leggi speciali (Art. 25-quater, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2003]
9. Pratiche di mutilazione degli organi genitali femminili (Art. 583-bis c.p.) (Art. 25-quater.1, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 7/2006]
10. Delitti **contro la personalità individuale** (Art. 25-quinquies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 228/2003; modificato dalla L. n. 199/2016 e successivamente dalla L.n.236 / 2016 e poi ancora dalla Legge 110 del 14 luglio 2017]
11. Reati di **abuso di mercato** (Art. 25-sexies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 62/2005]
12. Altre fattispecie in materia di abusi di mercato (Art. 187-quinquies TUF) [articolo modificato dal D.Lgs. n. 107/2018]
13. Reati di **omicidio colposo** e **lesioni colpose** gravi o gravissime, commessi **con violazione delle norme antinfortunistiche** e sulla tutela dell'igiene e della salute sul lavoro (Art. 25-septies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 123/2007; modificato L. n. 3/2018]
14. **Ricettazione**, **riciclaggio** e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (Art. 25-octies, D.Lgs. n. 231/2001) [articolo aggiunto dal D. Lgs. n. 231/2007; modificato dalla L. n. 186/2014 e dal D.Lgs.n.195 dell'8 novembre 2021]
15. Delitti in materia di **strumenti di pagamento diversi dai contanti** (Art. 25-octies.1, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. 184/2021 e modificata dalla L. n. 137/2023]
16. Altre fattispecie in materia di strumenti di pagamento diversi dai contanti (Art. 25-octies.1 comma 2, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. 184/2021]
17. Delitti in materia di **violazione del diritto d'autore** (Art. 25-novies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 99/2009; modificato dalla L. n. 93/2023]
18. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25-decies, D.Lgs. n. 231/2001) [articolo aggiunto dalla L. n. 116/2009]

19. **Reati ambientali** (Art. 25-undecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 121/2011, modificato dalla L. n. 68/2015, modificato dal D.Lgs. n. 21/2018 e modificato dalla L. n. 137/2023]
20. **Impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (Art. 25-duodecies, D.Lgs. n. 231/2001) [articolo aggiunto dal D.Lgs. n. 109/2012, modificato dalla legge n.161 del 17 ottobre 2017 e dal D.L. n. 20/2023]
21. **Razzismo** e **xenofobia** (Art. 25-terdecies, D.Lgs. n. 231/2001) – [articolo aggiunto dalla L. 167 del 20 novembre 2017 per la completa attuazione della decisione quadro 2008/913/GAI-Giustizia e affari interni]
22. **Frode** in **competizioni sportive**, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25-quaterdieces, D.Lgs. n. 231/2001) [articolo aggiunto dall' Art. 5 della Legge n. 39 del 03 maggio 2019]
23. **Reati tributari** (Art. 25-quinquiesdecies, D.Lgs.n.231/01) [articolo aggiunto dall'Art. 9 del Decreto Legge n. 124 del 26 ottobre 2019 coordinato con Legge di conversione n. 157 del 19 dicembre 2019 e ampliato dal D.Lgs.n.75 del 14 luglio 2020)
24. **Contrabbando** (Art. 25-sexiesdecies, D.Lgs.n.231/01) (articolo aggiunto dal D.Lgs.n.75 del 14 luglio 2020)
25. Delitti contro il patrimonio culturale (Art.25-septiesdecies, D.Lgs.n.231/01) [articolo aggiunto da L.n.22 del 09 marzo 2022]
26. **Riciclaggio di beni culturali** e devastazione e saccheggio di beni culturali e paesaggistici (Art.25-duodevicies, D.Lgs.n.231/01) [articolo aggiunto da L.n.22 del 09 marzo 2022]
27. Responsabilità degli enti per gli illeciti amministrativi dipendenti da reato (Art. 12, L. n. 9/2013) [Costituiscono presupposto per gli enti che operano nell'ambito della filiera degli oli vergini di oliva
28. **Reati transnazionali** (L. n. 146/2006) [Costituiscono presupposto per la responsabilità amministrativa degli enti i seguenti reati se commessi in modalità transnazionale]

4. I reati commessi all'estero

In considerazione delle attività, anche di natura finanziaria, e comunque connesse al core business aziendale, rivolte all'estero dalla Società e dai propri Dipendenti, risulta opportuno effettuare un richiamo esteso a quanto previsto dall'art. 4 del D.Lgs. n. 231/2001, e ai principi di territorialità previsti dal codice penale.

L'ente può essere considerato responsabile, in Italia, per la commissione, in territorio straniero, di taluni reati. In particolare, l'art. 4 del D.Lgs. n. 231/2001 prevede che gli enti aventi la sede principale nel territorio dello Stato rispondono anche in relazione ai reati commessi all'estero nei casi e alle condizioni previsti dagli articoli da 7 a 10 del codice penale, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto.

Pertanto, l'ente è perseguibile quando:

- in Italia ha la **sede principale**, cioè la sede effettiva ove si svolgono le attività amministrative e di direzione, eventualmente anche diversa da quella in cui si trova l'azienda o la sede legale (enti dotati di personalità giuridica);
- nei confronti dell'ente non stia procedendo lo Stato del luogo in cui è stato commesso il fatto;
- la richiesta del Ministro della Giustizia, cui sia eventualmente subordinata la punibilità, sia riferita anche all'ente medesimo.

Tali regole riguardano i reati commessi interamente all'estero da Organi sociali, Soggetti apicali o Soggetti sottoposti. Per le condotte criminose che siano avvenute anche solo in parte in Italia, si applica il principio di territorialità ex art. 6 del codice penale, in forza del quale "il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione".

5. L'esimente della responsabilità amministrativa

L'art. 6 del D.Lgs. 231/2001 stabilisce che l'ente, nel caso di reati commessi da Soggetti apicali, non risponda qualora dimostri che:

a) l'organo dirigente abbia adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi;
b) il compito di vigilare sul funzionamento e l'osservanza del Modello nonché di proporne l'aggiornamento sia stato affidato ad un Organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (c.d. "Organismo di Vigilanza, nel seguito anche "Organismo" o "O.d.V.");
c) le persone hanno commesso il reato eludendo fraudolentemente il suddetto Modello;
d) non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Nel caso in cui il reato sia stato commesso da Soggetti sottoposti, l'ente sarà ritenuto responsabile del reato solamente in ipotesi di carenza colpevole negli obblighi di direzione e vigilanza.

Pertanto, l'ente che, prima della commissione del reato, adotti e dia concreta attuazione ad un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi, resta esente da responsabilità se risultano integrate le descritte condizioni di cui all'art. 6 del D.Lgs. 231/2001.

In tal senso, il Decreto fornisce inoltre specifiche indicazioni in merito alle esigenze cui i Modelli di Organizzazione devono rispondere, così come più specificamente dettagliato nel paragrafo 9 con riferimento agli elementi fondamentali del Modello di Organizzazione e Gestione, cui si rinvia.

La mera adozione di un Modello di Organizzazione, tuttavia, non è di per sé sufficiente ad escludere detta responsabilità della Società, risultando necessario che il Modello sia effettivamente ed efficacemente attuato. In particolare, ai fini di un'efficace attuazione del Modello, il D.Lgs. 231/2001 richiede:

- una verifica periodica e l'eventuale modifica dello stesso quando siano emerse significative violazioni delle prescrizioni ovvero quando intervengano mutamenti nell'organizzazione o nell'attività;
- la concreta applicazione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

6. Il sistema sanzionatorio

Il riconoscimento di una responsabilità "personale e colpevole" in capo agli enti, seppure con gli scostamenti dal modello penalistico esaminati in precedenza, trova nella possibile applicazione di sanzioni il proprio effetto concreto. L'ente responsabile per un reato commesso da un soggetto appartenente alla sua struttura organizzativa è condannato da un sistema sanzionatorio che prevede sanzioni amministrative come la sanzione pecuniaria, le sanzioni interdittive, la confisca e la pubblicazione della sentenza di condanna.

Lo scopo delle sanzioni è quello di colpire direttamente o indirettamente il profitto dell'ente, disincentivando la commissione di reati nell'interesse o a vantaggio dell'ente stesso, e di incidere al contempo sulla struttura e sull'organizzazione societaria in modo da favorire attività risarcitorie e/o riparatorie.

6.1. La sanzione pecuniaria

L'art. 10 D.Lgs. 231/2001 stabilisce che per l'illecito amministrativo dipendente da reato la sanzione pecuniaria è sempre applicata come conseguenza dell'accertamento di responsabilità dell'ente; la sua determinazione avviene secondo il meccanismo delle quote che si articola in due fasi:

Nella prima fase il giudice fissa l'ammontare del numero delle quote che non deve essere mai inferiore a cento né superiore a mille; ciò avviene grazie alla valutazione della gravità del fatto, del grado di responsabilità dell'ente (adozione di modelli organizzativi, codici di condotta, sistemi disciplinari), di condotte riparatorie e riorganizzative (sanzioni disciplinari) in seguito alla commissione del reato.

Nella seconda fase l'organo giurisdizionale determina l'importo della quota: l'art. 10 dispone che l'importo di una quota vari da un minimo di 258 euro ad un massimo di 1.549 euro. Il comma 2 dell'art. 11 stabilisce che l'importo della quota sia commisurato in base alle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione.

La somma finale è data dalla moltiplicazione tra l'importo della singola quota e il numero complessivo di quote che quantificano l'illecito amministrativo; la sanzione pecuniaria potrà quindi avere un ammontare che va da un minimo di 25800 euro ad un massimo di 1549000 euro, commisurato alle condizioni dell'ente.

Il comma 3 dell'art. 11 prevede che la quota sia dell'importo fisso di 103 euro nell'ipotesi di cui all'art. 12, comma 1 D.Lgs. 231/2001, ossia quando la sanzione pecuniaria è ridotta perché l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ha ricavato un vantaggio minimo, oppure (ii) il danno cagionato è di particolare tenuità. In tale ipotesi, restano fermi i criteri di cui al comma 1 per la determinazione del numero delle quote e trovano applicazione i limiti massimo (103.291 euro) e minimo (10.329 euro) previsti dallo stesso art. 12.

6.2. Le sanzioni interdittive

L'interdizione è quell'istituto giuridico che comporta una limitazione temporanea dell'esercizio di una facoltà o di un diritto, in tutto o in parte; esso è la base delle sanzioni interdittive elaborate dal legislatore per contrastare più efficacemente le condotte illecite all'interno dell'ente grazie al loro contenuto inibitorio.

Le sanzioni interdittive hanno una durata limitata (non inferiore a tre mesi e non superiore a due anni) e possono essere applicate in via definitiva solo secondo quanto stabilito dall'art. 16 D.Lgs. 231/2001.

L'art. 9 co. 2 D.Lgs. 231/2001 elenca le sanzioni interdittive:

- L'interdizione dall'esercizio dell'attività, che comporta la chiusura dell'intera azienda o di un suo ramo; essa è una sanzione autonoma, ma può anche essere l'effetto dell'applicazione della seconda sanzione interdittiva:
- La sospensione o revoca delle autorizzazioni, licenze, concessioni funzionali all'esercizio dell'attività;
- Il divieto di contrattare con la pubblica amministrazione comporta il blocco delle entrate dell'ente, con l'esclusione dei contratti necessari per ottenere le prestazioni di un servizio pubblico necessario al normale svolgimento dell'impresa;
- L'esclusione da agevolazioni, finanziamenti, contributi e la revoca di quelli già ottenuti o il divieto di pubblicizzare beni o servizi, comportano quasi una totale assenza di occasioni di profitto per l'ente.

I presupposti per l'applicazione delle sanzioni interdittive sono disciplinati dall'art. 13 D.Lgs. 231/2001, ovvero:

Se il reato è commesso da un Soggetto Apicale, l'azienda deve aver tratto dal reato un profitto di rilevante entità.

Se il reato è commesso da un Soggetto Sottoposto, la commissione del reato deve essere stata determinata o agevolata da gravi carenze organizzative.

Infine, ultima condizione alternativa è quella relativa alla reiterazione degli illeciti che si verifica quando la società, già condannata, commette un altro illecito nei cinque anni successivi alla condanna definitiva.

Le sanzioni interdittive si applicano in relazione ai reati per i quali sono espressamente previste, se la società ha tratto dal reato un profitto di un certo rilievo e il reato è stato commesso da un soggetto in posizione apicale o da un soggetto sottoposto alla direzione dei primi, a causa di gravi carenze organizzative; o in caso di reiterazione degli illeciti.

I criteri di scelta delle sanzioni interdittive sono disciplinati dall'art. 14 D.Lgs. 231/2001 e coincidono con i principi di proporzionalità, idoneità e gradualità.

La proporzionalità richiama i criteri previsti per le sanzioni pecuniarie; quindi, il giudice sceglie la sanzione interdittiva a seconda della gravità del fatto, del grado di responsabilità dell'ente, delle condotte riparatorie e riorganizzative dopo la commissione del reato.

L'idoneità evidenzia come la sanzione interdittiva deve essere scelta in modo da prevenire il tipo di illecito commesso, consentendo anche un'applicazione congiunta di più sanzioni.

La gradualità, invece, fissa la sanzione interdittiva massima, l'interdizione dall'esercizio dell'attività, che deve essere applicata dal giudice solo se le altre risultano essere inadeguate.

I casi di non applicazione delle sanzioni interdittive sono disciplinati dall'art. 12 comma 1 D.Lgs. 231/2001, ossia il fatto commesso nel prevalente interesse della persona fisica o la tenuità del danno patrimoniale; rientrano inoltre in questa categoria le condotte riparatorie disciplinate dall'art. 17 D.Lgs. 231/2001 che dice che "ferma l'applicazione delle sanzioni pecuniarie, le sanzioni interdittive non si applicano quando, prima della dichiarazione di apertura del dibattimento di primo grado, si verificano le seguenti condizioni:

- l'ente ha risarcito integralmente il danno e
- ha eliminato le conseguenze dannose del reato, è stato adottato un modello organizzativo idoneo a prevenire i reati della specie di quello verificatosi; l'ente ha messo a disposizione il profitto conseguito ai fini della confisca.

L'art. 16 D.Lgs. 231/2001 definisce quando la sanzione interdittiva va applicata in via definitiva; l'interdizione definitiva dall'esercizio dell'attività può essere applicata se l'ente ha tratto dal reato un profitto di un certo rilievo ed è già stato condannato, almeno tre volte negli ultimi sette anni, all'interdizione temporanea dall'esercizio dell'attività.

Il giudice, inoltre, può applicare all'ente in via definitiva la sanzione del divieto di contrattare con la pubblica amministrazione o del divieto di pubblicizzare beni o servizi, quando è già stato condannato alla stessa sanzione almeno tre volte negli ultimi sette anni.

Infine, in caso di impresa illecita, ossia un'organizzazione con l'unico scopo di consentire o agevolare la commissione di reati, deve essere sempre applicata l'interdizione definitiva dall'esercizio dell'attività.

6.3. L'alternativa alla sanzione interdittiva: il commissario giudiziale

Il legislatore ha elaborato all'art. 15 D.Lgs. 231/2001 un'alternativa alla sanzione interdittiva, rappresentata dal commissario giudiziale; questa soluzione deve essere adottata dal giudice nei confronti dell'ente, per un periodo pari alla durata della sanzione interdittiva che determina l'interruzione dell'attività dello stesso, se sussiste almeno una delle seguenti condizioni:

- L'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione comporterebbe un grave pregiudizio alla collettività.

- L'interruzione dell'attività dell'ente può provocare, a causa delle dimensioni e delle condizioni economiche del territorio, ripercussioni sull'occupazione.

Una volta accertata la sussistenza di uno dei due presupposti, il giudice con sentenza dispone la prosecuzione dell'attività dell'ente da parte di un commissario, indicandone i compiti e i poteri con particolare riferimento alla specifica area in cui è stato commesso l'illecito; il commissario cura quindi l'azione di modelli organizzativi idonei a prevenire la commissione di reati della specie di quello verificatosi e non può compiere atti di straordinaria amministrazione senza autorizzazione del giudice.

Nonostante la tutela della collettività, il commissario giudiziale è pur sempre un'alternativa alla sanzione interdittiva ed è per questo che deve possedere un carattere sanzionatorio; ciò avviene mediante la confisca del profitto derivante dalla prosecuzione dell'attività.

Infine, è bene precisare come la soluzione del commissario giudiziale non possa essere adottata in caso di applicazione di una sanzione interdittiva in via definitiva.

6.4. La pubblicazione della sentenza di condanna

L'art. 18 D.Lgs. 231/2001 stabilisce che la pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva; tale sanzione amministrativa ha un carattere accessorio in quanto la sua applicazione può avvenire solo contestualmente ad una sanzione amministrativa ed è discrezionale, in quanto è il giudice a stabilire quando applicarla.

La pubblicazione della sentenza di condanna opera nei casi più gravi come pubblicità denigratoria nei confronti dell'ente; le modalità di pubblicazione sono state oggetto di interventi normativi che le hanno ricondotte all'art. 36 c.p. secondo il quale la sentenza di condanna va pubblicata per estratto o per intero, su richiesta del giudice, sul sito internet del Ministero della Giustizia.

6.5. La confisca

L'art. 19 D.Lgs. 231/2001 stabilisce nei confronti dell'ente è sempre disposta, con sentenza di condanna, la confisca del prezzo o del profitto del reato salvo che per la parte che può essere restituita al danneggiato.

Quando non è possibile eseguire la confisca secondo le condizioni citate, essa può avere ad oggetto denaro, beni di valore equivalente al prezzo o al profitto del reato.

La confisca è una sanzione amministrativa che si distingue dalle altre in quanto non ha limiti di valore (sui generis); essa inoltre viene applicata anche in altre situazioni: la prosecuzione dell'attività dell'ente sotto la gestione del commissario giudiziale, riparazione delle conseguenze del reato da parte dell'ente, irrogazione in seguito all'inosservanza delle sanzioni interdittive (art. 23 D.Lgs. 231/2001), in presenza di un modello organizzativo tale da prevenire la commissione di reati da parte de vertici societari.

La confisca è disposta in tutti i casi di condanna della società, nonché quando, indipendentemente dalla condanna, il reato venga commesso da Soggetti Apicali (art. 6, comma 5).

La confisca ha ad oggetto il prezzo o il profitto del reato, salvo che per la parte restituibile al danneggiato e salvi i diritti dei terzi in buona fede. Laddove non sia possibile eseguire la confisca sul profitto del reato, essa può avere ad oggetto somme di danaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato stesso.

La circostanza che, nel caso di elusione fraudolenta del Modello senza colpa dell'azienda, non sia ravvisabile alcuna responsabilità dello stesso, nulla toglie all'inopportunità che la persona giuridica si giovi dei profitti economici che abbia comunque tratto dall'operato del c.d. amministratore infedele. Per tale ragione, anche in queste ipotesi, è disposta la confisca del profitto del reato.

7. Il delitto tentato

La disciplina codicistica generale in tema di reato tentato è contenuta essenzialmente nell'art. 56 del codice penale, disposizione che, sotto la rubrica intitolata al "delitto tentato" (espressione che chiarisce immediatamente la non configurabilità del tentativo nelle contravvenzioni) definisce al primo comma la struttura del tentativo, articolata sul compimento di atti idonei diretti in modo non equivoco a commettere un delitto e sul mancato compimento (perfezionamento) dell'azione o sulla mancata verificazione (produzione) dell'evento. Il secondo comma traccia la disciplina sanzionatoria della fattispecie tentata, individuando la pena nella reclusione non inferiore a dodici anni, se per la fattispecie consumata è previsto l'ergastolo, e stabilendo negli altri casi una riduzione da un terzo a due terzi della pena prevista per la fattispecie consumata. Il terzo e il quarto comma dell'art. 56 c.p. contengono rispettivamente la disciplina della desistenza volontaria dall'azione (si applica la sola pena per gli atti compiuti, qualora questi costituiscano reato) e del volontario impedimento dell'evento (si applica la pena stabilita per il delitto tentato, diminuita da un terzo alla metà).

Dottrina e giurisprudenza sono da sempre concordi nell'affermare l'autonomia della fattispecie tentata rispetto a quella consumata (della quale conserva lo stesso *nomen iuris*) e nel correlare la prima fattispecie alla combinazione di due previsioni normative, quella che configura la singola incriminazione e, appunto, quella di cui all'art.56 c.p.

La disciplina che il D.Lgs. 231/2001 dedica all'istituto del tentativo richiama, quale presupposto, l'integrazione della fattispecie tentata da parte del soggetto agente e si sostanzia nelle disposizioni di cui all'art. 26, la prima delle quali è intrinsecamente – e necessariamente – collegata alla fattispecie di cui al primo comma dell'art. 56. Questa stabilisce, per il caso in cui il reato da cui discende la responsabilità dell'ente si sia arrestato alla fase del tentativo, la riduzione da un terzo alla metà delle sanzioni pecuniarie o interdittive applicabili all'ente, così mutuando sostanzialmente la disciplina di cui al secondo comma dell'art.56 del codice penale, pur con una riduzione dell'entità massima della sanzione. Anche l'art. 26 fa riferimento ai soli delitti, sulla scorta dell'esclusione, nella disciplina codicistica che costituisce il presupposto di quella di cui al d.lgs. 231/2001, della configurabilità del tentativo nelle contravvenzioni.

Il secondo comma dell'art.26 si ricollega alla disciplina del terzo e quarto comma dell'art. 56 c.p., ma introduce una regolamentazione autonoma nei confronti dell'ente; questo stabilisce una radicale esclusione di responsabilità dell'ente nei casi in cui questo volontariamente impedisca l'azione che integrerebbe il delitto ovvero impedisca la realizzazione dell'evento cui è dalla fattispecie incriminatrice collegata la consumazione del delitto.

8. Le linee guida di Confindustria

L'art. 6, comma 3 del D.Lgs. 231/2001 dispone espressamente che i Modelli di Organizzazione, Gestione e Controllo possano essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti.

Le "Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. 231/2001", anche con riferimento a contesti di gruppi societari, sono state emanate da Confindustria e approvate dal Ministero della Giustizia nel dicembre 2003, in conformità al citato articolo e, da ultimo, aggiornate alla versione di giugno 2021.

Nella definizione del Modello di Organizzazione, Gestione e Controllo, le Linee Guida prevedono, tra l'altro, le seguenti fasi progettuali:

- l'identificazione dei rischi, ossia l'analisi del contesto aziendale per evidenziare in quali aree di attività e secondo quali modalità si possano verificare i reati previsti dal D.Lgs. 231/2001;
- la predisposizione di un sistema di controllo idoneo a prevenire i rischi di reato identificati nella fase precedente, attraverso la valutazione del sistema di controllo esistente all'interno dell'ente ed il suo grado di adeguamento alle esigenze espresse dal D.Lgs. 231/2001.

Le componenti rilevanti del sistema di controllo delineato nelle Linee Guida per garantire l'efficacia del Modello di Organizzazione, Gestione e Controllo sono recepite nel Modello di SevenData così come più specificamente dettagliato nella parte seconda del Codice.

9. Valore ed elementi fondamentali del Modello

Le sanzioni per gli illeciti amministrativi dipendenti da reato si applicano soltanto nel caso in cui l'azienda non abbia provveduto ad adottare e attuare un apposito Modello, che consista, anzitutto, nella definizione e nell'applicazione di regole procedurali interne.

Tali regole procedurali interne devono essere idonee a prevenire i reati e a ridurre i rischi di condotte illecite.

L'approccio seguito da SevenData, è stato di predisporre Protocolli di controllo, eventualmente integrati da procedure aziendali ad essi coerenti. I Protocolli rappresentano, comunque, regole generali cui devono sempre ispirarsi le attività dei singoli, anche nei casi in cui non vi siano specifiche procedure in merito e consistendo in regole già applicabili, costituiscono un presidio di prevenzione dei reati presupposto.

Tale approccio risulta coerente con il percorso seguito dal Legislatore, basato sulla volontà di motivare l'azienda non solo alla semplice adozione di un Modello, bensì alla sua reale, concreta ed effettiva applicazione.

Tale impostazione ha consentito di adottare un Modello orientato a minimizzare il rischio, individuando specifiche misure di prevenzione.

In altre parole, affinché si possa parlare di una corretta prevenzione, occorre che il funzionamento del Modello sia effettivo e che esso sia accompagnato da un'attività di vigilanza strutturata e organizzata.

Il Modello si basa sulla mappatura dei rischi, sulla definizione di ruoli e di competenze e su un'attenta considerazione delle fattispecie di reato presupposto. Il Modello definisce i processi decisionali e tiene conto della separazione tra chi delibera e chi attua le decisioni, tra chi opera e chi controlla e determina le modalità di conservazione delle informazioni.

In particolare, il Modello deve individuare le attività nel cui ambito possono essere commessi reati, prevedere specifici Protocolli diretti a programmare la formazione e l'attuazione delle decisioni di SevenData in relazione ai reati da prevenire, individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati, prevedere obblighi di informazione nei confronti dell'Organismo di Vigilanza, introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello (art. 6, commi 2 e 3, D.Lgs. 231/2001).

Quanto agli elementi fondamentali del Modello, il D.Lgs. 231/2001 attribuisce, unitamente al verificarsi delle altre circostanze previste dagli artt. 6 e 7 del Decreto stesso, un valore esimente all'adozione ed efficace attuazione di Modelli di Organizzazione, Gestione e Controllo, nella misura in cui questi risultino idonei a prevenire, con ragionevole certezza, la commissione, o la tentata commissione, dei reati presupposto.

In particolare, gli elementi costitutivi del Modello di SevenData, in conformità al comma 2 dell'art. 6 del D.Lgs. 231/2001, e sulla base delle indicazioni fornite dalle Linee Guida di Confindustria, possono essere così declinati:

- adozione dei principi etici e delle regole comportamentali, sancite anche nel Codice di Comportamento, volte alla prevenzione di condotte che possano integrare le fattispecie di reato;

- modello organizzativo sufficientemente formalizzato e chiaro, con particolare riguardo all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e descrizione dei compiti con specifica previsione di principi di controllo;
- procedure che regolino lo svolgimento delle attività, prevedendo opportuni controlli;
- poteri autorizzativi e di firma coerenti con le responsabilità organizzative e gestionali attribuite, prevedendo, laddove opportuno, corrispondenti limiti di spesa;
- sistemi di controllo e di gestione, idonei a segnalare tempestivamente possibili criticità;
- individuazione delle "Aree Sensibili", svolta attraverso l'analisi dei processi aziendali e delle possibili modalità realizzative delle fattispecie di reato rilevanti;
- predisposizione e aggiornamento di specifici principi di comportamento, protocolli e strumenti normativi, proporzionati alla dimensione e alla complessità della Società, diretti a programmare la formazione e l'attuazione dei processi decisionali, relativi alle Attività Sensibili di cui al punto precedente;
- previsione di standard di controllo in relazione alle Attività Sensibili individuate di cui al successivo paragrafo "Individuazione degli ambiti aziendali esposti al rischio e relativi presidi";
- programma di verifiche sulle Aree Sensibili e relativi standard di controllo;
- nomina dell'Organismo di Vigilanza, con attribuzione di specifici compiti di vigilanza su l'efficace attuazione ed effettiva applicazione del Modello, cui competono e nei cui confronti sussistono specifici obblighi di informazione;
- piano di formazione e comunicazione al personale dipendente;
- sistema sanzionatorio idoneo a garantire l'efficacia del Modello, contenente le misure applicabili in caso di violazione delle prescrizioni ivi contenute;

In particolare, il Modello di Organizzazione e Gestione contiene:

nella Parte Generale, una descrizione relativa:

- al quadro normativo di riferimento (con elenco dei reati e normativa richiamata, dettagliatamente riportati nell'Appendice Normativa - Allegato A);
- all'assetto istituzionale e organizzativo, agli strumenti di governance e di regolamentazione interna, al Sistema di Controllo Interno e di Gestione dei Rischi aziendali;
- agli elementi fondamentali del Modello stesso;
- alla individuazione e nomina dell'OdV, con specificazione di poteri, compiti e flussi informativi che lo riguardano;
- al piano di formazione e comunicazione da adottare al fine di garantire la conoscenza delle misure e delle disposizioni del Modello;
- alla funzione del sistema disciplinare e al relativo apparato sanzionatorio;
- ai criteri di aggiornamento e adeguamento del Modello;
-

nella Parte Speciale, una descrizione relativa:

- alle fattispecie di Reato richiamate dal D.Lgs. 231/2001 e rilevanti per la Società;
- alle Attività Sensibili e relativi standard di controllo generali e specifici;
- ai principi di comportamento e di attuazione dei processi decisionali con riferimento ai reati e alle Attività Sensibili.

Parte Seconda

Il Modello di Organizzazione, Gestione e Controllo di SevenData

1. La Società

SevenData è una martech company, nata nel 2017 dall'iniziativa di un team di imprenditori e senior manager con storia di successi nel data marketing e nella business information ed è il partner indispensabile per aziende, manager, imprenditori e per tutti coloro che desiderano creare valore nella loro "customer value chain".

SevenData offre ai propri clienti strumenti e soluzioni data-driven, per aiutarli a conoscere i loro mercati e le loro customer base al fine di identificare e profilare al meglio i target e le audience specifiche, per ingaggiarli attraverso strumenti personalizzati e con la sicurezza dell'affidabilità creditizia. Il tutto integrato nei sistemi informatici e di CRM del cliente.

2. Organizzazione

Con riferimento all'organizzazione, l'ente deve essere dotato di un sistema organizzativo formalizzato, chiaro e aggiornato, con specifica attribuzione di responsabilità, chiare linee di dipendenza gerarchica e descrizione dei compiti, previsione di principi di controllo e tracciatura della copertura temporale degli incarichi. Inoltre, è necessario assicurare che i sistemi premianti aziendali, diretti a indirizzare i dipendenti verso il conseguimento degli obiettivi dell'azienda, non si fondino su obiettivi di prestazione e risultato inaccessibili, tali da incentivare la commissione di reati-presupposto .

La Società adotta un sistema di gestione tradizionale i cui organi sociali sono rappresentati dal Consiglio di Amministrazione, che svolge funzione amministrativa, ovvero si occupa di gestire la società in maniera conforme all'oggetto sociale, ed annovera tra i suoi compiti anche quello di rappresentare la società nei confronti di terzi, e dal Collegio Sindacale, ovvero l'organo di controllo delle società quotate che ha il compito di vigilare sull'attività degli amministratori e controllare che la gestione e l'amministrazione della società si svolgono nel rispetto della legge e dell'atto costitutivo.

Il Consiglio di Amministrazione, cui spetta la gestione dell'impresa, ha delegato parte delle proprie competenze all'Amministratore Delegato. La rappresentanza legale della Società spetta al Presidente del Consiglio di Amministrazione nonché all'Amministratore Delegato nei limiti dei poteri conferiti.

3. Modello di governance

La corporate governance di SevenData indica l'insieme di regole finalizzate a individuare competenze e responsabilità degli Organi Sociali, del management e di tutti i soggetti che operano all'interno dell'organizzazione.

La corporate governance è diretta a garantire una sana e corretta gestione dell'impresa, assicurando, attraverso un adeguato sistema di controllo interno, un costante monitoraggio ed un'accorta gestione del rischio.

Essa costituisce un ulteriore presidio in grado di garantire la protezione degli interessi sottesi al Decreto.

La corporate governance di SevenData è delineata tenendo conto delle previsioni di legge e Statuto, nonché delle best practice in materia di governo societario.

Nello specifico, SevenData ha sviluppato un insieme di strumenti di governance che vengono sottoposti ad una continua verifica da parte del Consiglio di Amministrazione ed adeguati all'evolversi del contesto normativo, delle prassi operative e dei mercati. Tali strumenti sono periodicamente monitorati, al fine di verificarne la corretta applicazione all'interno dell'organizzazione aziendale. Per il dettaglio si rinvia a:

- Statuto di SevenData.
- Regolamento aziendale.
- Policy Aziendali.
- Sistema di deleghe e procure.
- Organigrammi.
- Mansionari.
- Procedure interne ed Istruzioni operative.
- Processi.
- Manuali interni.
- Documento Programmatico sulla Sicurezza (DPS).
- Documento di Valutazione dei Rischi (DVR).
- Altra normativa interna.

4. Individuazione degli ambiti aziendali esposti al rischio e relativi presidi

I presidi di controllo sono stati costruiti nell'ottica di garantire una più efficace copertura contro il rischio di colpa organizzativa.

A tal fine, sono stati predisposti Protocolli il cui rispetto contribuisce a prevenire il rischio che vengano commessi reati presupposto.

I Protocolli, elaborati in relazione ai singoli processi aziendali esaminati, costituiscono parte integrante del Modello. Nella loro formulazione è stato privilegiato un metodo di analisi che ha valorizzato ognuna delle seguenti fasi:

- La rilevazione delle singole aree a rischio, in base alle fattispecie di reato considerate dal D.Lgs. 231/2001 e all'identificazione, al loro interno, delle sole attività e processi sensibili per i quali si è accertata l'esistenza di rischi concreti di comportamenti illeciti.
- La selezione delle fattispecie di reato presupposto per le quali si è riscontrata una propensione al rischio di commissione nell'ambito dell'attività di SevenData, ordinate e classificate in base a una matrice di probabilità dell'evento (alto, medio, basso).
- L'associazione dei processi organizzativi e operativi - per i quali si è avuto modo di verificare la sussistenza di un rischio di esposizione all'evento illegale in base a una valutazione preventiva - a ciascuna tipologia di reato presupposto.
- La predisposizione di regole e linee applicative (strumenti e presidi), secondo le tecniche riconducibili alla better regulation, dirette a programmare la formazione e l'attuazione delle decisioni di SevenData in relazione ai reati da prevenire.

I Protocolli sono stati predisposti in modo da:

- Integrarsi con i processi aziendali e le procedure interne.
- Definire criteri, regole e strumenti atti a prevenire la commissione dei reati presupposto.
- Indicare presidi organizzativi e comportamentali di diffusa applicabilità, in grado di prevenire irregolarità nei processi decisori e illiceità nella gestione, quali fonte di responsabilità ai sensi del D.Lgs. 231/2001.

I Protocolli contengono accorgimenti specifici, fatti di regole interne anche etiche, nonché di strumenti informatici, operativi e di controllo, che sono adottati come rafforzativo delle procedure e dei processi ordinari in vigore.

Parte terza

1. Finalità

SevenData si dota di un proprio Modello, nella consapevolezza che il medesimo, seppur costituendo una facoltà e non un obbligo, rappresenta un'opportunità per rafforzare la propria governance, cogliendo al contempo l'occasione per sensibilizzare tutte le strutture interne rispetto ai temi del controllo dei processi aziendali, ai fini di una prevenzione idonea ed efficace dei rischi-reato, adottando comportamenti improntati a legalità, correttezza e trasparenza.

Il Modello è costituito dalla presente Parte Generale, composta da sei sezioni ("parti"), e da una Parte Speciale contenente le diverse fattispecie di reato-presupposto concretamente e potenzialmente rilevanti per la Società, in ragione della attività svolta, delle attività a rischio reato, nonché dei principi comportamentali e di controllo generali e specifici a presidio delle attività a rischio.

I principi espressi nel Modello sono coerenti con il Codice di Comportamento, parte integrante del Modello stesso.

Con l'adozione del Modello, elaborato, sulla base delle indicazioni previste dalle Linee Guida di Confindustria e con specifico riferimento alla concreta realtà aziendale, affinché sia possibile prevenire efficacemente i Reati Presupposto, la Società intende dunque perseguire le seguenti finalità:

- diffondere la consapevolezza che, dalla violazione delle prescrizioni contenute nel Modello e dei principi del Codice Etico, possa derivare l'applicazione di misure sanzionatorie (pecuniarie e interdittive) anche a carico della Società;
- consentire alla Società, grazie ad un sistema strutturato di regole, procedure e sanzioni e ad una costante azione di monitoraggio sulla corretta attuazione di tale sistema, di prevenire e/o contrastare tempestivamente la commissione di reati rilevanti ai sensi del Decreto.

2. Destinatari

I Destinatari devono osservare le regole contenute nel Modello. In genere, sono Destinatari del Modello:

- Soci;
- Componenti gli Organi Sociali;
- Dirigenti, quadri, impiegati;
- Partner, consulenti, professionisti esterni e fornitori di beni e servizi;
- Ogni altra controparte che intrattenga con SevenData rapporti contrattualmente regolati.

Ogni Destinatario è tenuto a:

1. acquisire consapevolezza dei principi e contenuti del Modello;
2. conoscere le modalità operative con le quali deve essere realizzata la propria attività;
3. contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del Modello, segnalando eventuali carenze riscontrate nello stesso ai soggetti a ciò deputati, anche attraverso i sistemi di Whistleblowing.

3. Comunicazione

Al fine di garantire un'efficace e razionale attività di comunicazione, SevenData intende promuovere ed agevolare la conoscenza dei contenuti e dei principi del Modello da parte dei dipendenti, con grado di approfondimento diversificato a seconda della posizione e del ruolo dagli stessi ricoperto.

Al personale di lavoro è garantita la possibilità di accedere e consultare la documentazione che costituisce il Modello di SevenData, anche tramite Intranet aziendale.

Al momento dell'instaurazione del rapporto, la Società consegna ai neoassunti nota informativa, indicante l'indirizzo ove reperire copia del Modello di SevenData. Il neoassunto ne prende contezza, dandone atto mediante sottoscrizione di apposita dichiarazione, impegnandosi, con la medesima, ad osservare il Modello. SevenData documenta e conserva la consegna della suddetta informativa, nonché la dichiarazione sottoscritta dallo stesso.

Ai componenti degli Organi Sociali di SevenData vengono applicate le medesime modalità di diffusione del Modello previste per il personale di lavoro. Idonei strumenti di comunicazione sono adottati per aggiornare il personale di lavoro circa le modifiche apportate al Modello e ogni rilevante cambiamento procedurale o organizzativo.

L'attività di comunicazione e diffusione è indirizzata a tutti i Destinatari, con specifico riferimento ai soggetti che intrattengono con SevenData particolari rapporti contrattualmente regolati.

4. Formazione

L'attività di formazione, finalizzata a diffondere i contenuti delle prescrizioni del D.Lgs. 231/2001 e del Modello di SevenData, è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, delle responsabilità assegnate e del livello di rischio dell'area in cui operano.

L'attività formativa può essere erogata attraverso diverse modalità alternative:

- Sessioni in aula: con incontri dedicati oppure mediante l'introduzione di moduli specifici nell'ambito di altre sessioni formative, a seconda dei contenuti e dei Destinatari, con questionari di verifica del grado di apprendimento.
- E-learning: attraverso un modulo relativo alla parte generale per tutto il personale di lavoro, con esercitazioni intermedie e test di verifica di apprendimento.

I contenuti degli interventi formativi vengono adeguati in relazione ad interventi di aggiornamento del Modello.

La partecipazione agli interventi formativi è obbligatoria.

L'Organismo di Vigilanza, tramite le competenti Funzioni, registra ed archivia la partecipazione dei Destinatari alle attività formative programmate.

Parte quarta

1. Il sistema sanzionatorio

Un aspetto essenziale nella costruzione di un modello organizzativo è rappresentato dalla previsione di un adeguato sistema disciplinare/sanzionatorio per le violazioni del modello, delle procedure previste dallo stesso e del Codice di Comportamento. Per poter beneficiare dell'efficacia esimente del modello, infatti, la Società deve assicurarsi non solo che il modello sia adottato, ma anche che esso sia efficacemente attuato. E tale efficace attuazione richiede, tra le altre cose, l'adozione e implementazione di un “sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello”.

Il sistema disciplinare è previsto dal D.Lgs. 231/2001 come elemento indispensabile del modello e condizione per garantire l'efficace attuazione di esso. In particolare:

- in relazione ai soggetti in posizione apicale, l'art. 6, comma 2, del D.Lgs. 231/2001 prevede che: "In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli (...) devono rispondere alle seguenti esigenze: (...) e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello";
- con riferimento ai soggetti sottoposti all'altrui direzione, l'art. 7, comma 4, del D.Lgs. 231/2001 stabilisce che: "L'efficace attuazione del modello richiede: (...) b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".

Inoltre, ai sensi del comma 2-bis dell'art. 6 del D.Lgs. 231/2001, il sistema disciplinare adottato ai sensi del comma 2, lettera e), di tale articolo deve altresì prevedere sanzioni nei confronti di coloro che violino le misure di tutela del segnalante, nonché di coloro che effettuino, con dolo o colpa grave, segnalazioni che si rivelino infondate.

È quindi fondamentale che il sistema disciplinare/sanzionatorio sia formalizzato e sia parte integrante del modello organizzativo. Occorre inoltre che esso sia adeguatamente divulgato in modo che ne sia data conoscenza generalizzata, con riferimento sia ai lavoratori dipendenti, secondo le norme che si riferiscono a tale rapporto di lavoro (e quindi con applicazione delle disposizioni di cui all'art. 7 dello Statuto dei Lavoratori), sia a tutte le forme di collaborazione esterna, assicurando in questo caso le comunicazioni informative più idonee allo scopo.

1.1. Violazioni del Modello

Il sistema sanzionatorio di SevenData trova applicazione ogniqualvolta il Destinatario violi il Modello. A titolo meramente esemplificativo, ma non esaustivo, integra violazione del Modello:

- Qualsiasi atto o comportamento, commissivo od omissivo, doloso o colposo, non conforme alle prescrizioni contenute nel Modello.
- La commissione, dolosa o colposa, di un reato presupposto, tentato o consumato.
- Ogni altra violazione delle disposizioni contenute nel D.Lgs. 231/2001.

1.2. Criteri generali di irrogazione delle sanzioni

Il sistema sanzionatorio prevede diverse tipologie di sanzioni. La sanzione applicabile, proporzionata ed adeguata alla violazione, è individuata tenuto conto, altresì, dei seguenti criteri:

- Natura della prescrizione violata.
- Gravità dell'infrazione.
- Mansioni, livello di responsabilità gerarchica e funzionale.
- Elemento soggettivo della condotta (dolo o colpa).
- Comportamento complessivo, accertando eventuali precedenti disciplinari.
- Gravità potenziale del danno alla Società, anche derivante dall'applicazione delle sanzioni previste dal D.Lgs. 231/2001.

In ogni caso, per dirigenti, quadri, impiegati, trovano applicazione le disposizioni contenute nello Statuto dei Lavoratori e nel Contratto Collettivo Nazionale applicato.

Fermo restando i poteri e i doveri facenti capo alla funzione Risorse Umane, il procedimento sanzionatorio relativo alle violazioni del Modello di SevenData è attivato a seguito dell'accertamento di presunte violazioni da parte dell'Organismo di Vigilanza nell'esercizio delle proprie funzioni, ovvero a seguito di segnalazione eseguita anche tramite strumenti di Whistleblowing (per il dettaglio si veda Capitolo 3).

Il procedimento sanzionatorio è attivato a prescindere dall'instaurazione di un procedimento penale a carico del Destinatario, diretto ad accertare l'eventuale violazione delle disposizioni contenute nel D.Lgs. 231/2001.

Nessun procedimento sanzionatorio può essere archiviato, né alcuna sanzione può essere irrogata per violazione del Modello di SevenData, senza avere preventivamente notiziato l'Organismo di Vigilanza, che esprime un parere.

1.3. Quadri, impiegati

SevenData aggiorna il proprio codice disciplinare ed estende le sanzioni ivi indicate alle violazioni del Modello.

Le sanzioni applicabili sono quelle previste dall'art. 7 dello Statuto dei Lavoratori e dal Contratto Collettivo Nazionale applicato.

Il procedimento sanzionatorio è regolato dall'art. 7 dello Statuto dei Lavoratori.

1.4. Dirigenti

SevenData aggiorna il proprio codice disciplinare ed estende le sanzioni ivi indicate alle violazioni del Modello.

SevenData introduce nei contratti di lavoro conclusi con i propri dirigenti un'apposita clausola diretta a sanzionare la violazione del Modello di SevenData e del D.Lgs. 231/2001.

In ogni caso, SevenData si riserva di adottare i provvedimenti più opportuni, ivi comprese le sanzioni previste dall'art. 7 dello Statuto dei Lavoratori e dal Contratto Collettivo Nazionale applicato.

Il procedimento sanzionatorio è regolato dall'art. 7 dello Statuto dei Lavoratori.

1.5. Consiglieri di Amministrazione

SevenData introduce nei contratti conclusi con i propri Consiglieri di Amministrazione un'apposita clausola diretta a sanzionare la violazione del Modello di SevenData e del D.Lgs. 231/2001.

Nel caso in cui il Consigliere di Amministrazione commetta una violazione del Modello, SevenData si riserva di adottare i provvedimenti più opportuni, in conformità alla normativa vigente, tra i quali:

- Revoca totale o parziale delle deleghe.
- Revoca della carica.
- Convocazione dell'Assemblea dei Soci per l'adozione delle iniziative previste dalla legge.

Per i Consiglieri di Amministrazione che appartengono alle categorie dei prestatori di lavoro indicate nell'art. 2095 c.c., SevenData si riserva di adottare i provvedimenti più opportuni, ivi comprese le sanzioni previste dall'art. 7 dello Statuto dei Lavoratori e dal Contratto Collettivo Nazionale applicato. In tal caso, il procedimento sanzionatorio è regolato dall'art. 7 dello Statuto dei Lavoratori. In ogni caso, sono salve le ulteriori disposizioni sanzionatorie previste dalla legge per la carica di Consigliere di Amministrazione (esemplificativamente, azione di responsabilità).

Per i Consiglieri di Amministrazione che non appartengono alle categorie dei prestatori di lavoro indicate nell'art. 2095 c.c. (ad esempio, lavoratori autonomi e liberi professionisti), il Consiglio di Amministrazione contesta per iscritto l'asserita violazione del Modello al Consigliere, assegnandogli un termine di 10 giorni dalla ricezione della contestazione per presentare difese scritte al Consiglio di Amministrazione. Entro 10 giorni dalla ricezione delle difese scritte, il Consiglio di Amministrazione convoca l'interessato per un'audizione orale, alla quale partecipano anche i componenti dell'Organismo di Vigilanza. Decorsi almeno 10 giorni dall'Adunanza, il Consiglio di Amministrazione adotta i provvedimenti più opportuni con l'astensione del Consigliere sottoposto al procedimento sanzionatorio, sentito il parere dell'Organismo di Vigilanza.

1.6. Componenti dell'Organismo di Vigilanza

SevenData introduce nel sistema sanzionatorio un'apposita clausola diretta a sanzionare la violazione del Modello di SevenData e del D.Lgs. 231/2001 da parte dei componenti del proprio Organismo di Vigilanza.

Per i componenti dell'Organismo di Vigilanza che appartengono alle categorie dei prestatori di lavoro indicate nell'art. 2095 c.c., oltre alla revoca dell'incarico, SevenData si riserva di adottare i provvedimenti più opportuni, ivi comprese le sanzioni previste dall'art. 7 dello Statuto dei Lavoratori e dal Contratto Collettivo Nazionale applicato. In tal caso, il procedimento sanzionatorio è regolato dall'art. 7 dello Statuto dei Lavoratori.

Per i componenti dell'Organismo di Vigilanza che non appartengono alle categorie dei prestatori di lavoro indicate nell'art. 2095 c.c. (ad esempio, lavoratori autonomi e liberi professionisti), il Consiglio di Amministrazione, di concerto con i componenti non coinvolti dell'Organismo di Vigilanza, contesta per iscritto l'asserita violazione del Modello al componente, assegnandogli un termine di 10 giorni dalla ricezione della contestazione per presentare difese scritte all'Organismo di Vigilanza e al Consiglio di Amministrazione. Entro 10 giorni dalla ricezione delle difese scritte, il Consiglio di Amministrazione convoca l'interessato per un'audizione orale, alla quale partecipano anche i componenti non coinvolti dell'Organismo di Vigilanza. Decorsi almeno 10 giorni dall'Adunanza, il Consiglio di Amministrazione adotta i provvedimenti più opportuni, sentito il parere dei componenti non coinvolti dell'Organismo di Vigilanza.

1.7. Destinatari terzi

SevenData introduce nei contratti conclusi con Destinatari terzi un'apposita clausola diretta a sanzionare l'osservanza del Modello di SevenData e del D.Lgs. 231/2001.

In caso di violazioni del Modello di SevenData e si riserva di adottare i provvedimenti più opportuni, ivi inclusa la risoluzione del rapporto ed il risarcimento dei danni (vedi Parte Speciale, documento Clausola Contrattuale 231).

Il Responsabile della Funzione che gestisce il rapporto con il Destinatario terzo ne dà notizia all'Organismo di Vigilanza, all'Amministratore Delegato e ad altri soggetti eventualmente indicati dal Consiglio di Amministrazione che, di concerto, adottano i provvedimenti più opportuni.

Parte quinta

1. Organismo di Vigilanza

Ai sensi dell'art. 6, comma 1, del D. Lgs. 231/2001 si richiede, quale condizione per beneficiare dell'esimente dalla responsabilità amministrativa, che il compito di vigilare sull'osservanza e funzionamento del Modello, curandone il relativo aggiornamento, sia affidato ad un Organismo di Vigilanza interno all'ente che, dotato di autonomi poteri di iniziativa e di controllo, eserciti in via continuativa i compiti ad esso affidati. Pertanto, l'Organismo di Vigilanza svolge le sue funzioni al di fuori dei processi operativi della Società, riferendo periodicamente al Consiglio di Amministrazione, svincolato da ogni rapporto gerarchico con il Consiglio stesso e con i singoli responsabili delle Direzioni.

Il Consiglio di Amministrazione è chiamato a deliberare sulla formale adozione del Modello, ai sensi degli artt. 6 e 7, D.Lgs. n. 231/2001, e a nominare i componenti dell'Organismo di Vigilanza.

L'istituzione dell'Organismo di Vigilanza, la cessazione dalla carica di componente dell'Organismo di Vigilanza, il rinnovo e la sostituzione dei componenti, è comunicata dal Consiglio di Amministrazione al personale della Società e all'Assemblea dei Soci.

1.1. Requisiti dei componenti

I componenti dell'Organismo di Vigilanza non devono:

- Essere congiunti di Soggetti Apicali.
- Essere legati a SevenData da interessi di qualsiasi natura che possano, in atto o potenza, generare conflitto di interesse, ad esclusione del rapporto di lavoro.
- Trovarsi nelle condizioni indicate dall'art. 2382 del Codice Civile.
- Avere riportato sentenza di condanna passata in giudicato, decreto penale di condanna divenuto irrevocabile, sentenza di applicazione della pena su richiesta ai sensi dell'art. 444 c.p.p., né essere attualmente sottoposti a procedimento per reati in danno dello Stato, reati di partecipazione ad un'organizzazione criminale, di corruzione, riciclaggio, reati commessi in violazione delle norme in materia di sicurezza sul lavoro e tutela dell'ambiente, altre violazioni comunque sanzionate dal D.Lgs. n. 231/2001.

Il Regolamento dell'Organismo di Vigilanza disciplina ulteriori cause di ineleggibilità, incompatibilità e revoca.

L'interessato attesta con formale autodichiarazione resa ai sensi del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, l'assenza delle già menzionate cause.

Laddove ricorrano le situazioni ostative suindicate, il Consiglio di Amministrazione effettua gli opportuni accertamenti notiziandone l'Organismo di Vigilanza. Sentito l'interessato, assegna un congruo per rimuovere perentoriamente la

causa ostativa. Decorso invano il termine perentorio, il Consiglio di Amministrazione dichiara decaduto il componente e procede alla sua sostituzione, informandone l'Organismo di Vigilanza.

1.2. Requisiti dell'Organismo di Vigilanza

L'Organismo di Vigilanza risponde ai seguenti requisiti:

- Indipendenza e autonomia, anche finanziaria. L'Organismo di Vigilanza, per poter esercitare in piena autonomia ed indipendenza le proprie funzioni, dispone di un budget di spesa annuale adeguato a queste ultime e a fare fronte all'acquisizione di consulenze.
- Professionalità. I componenti devono essere dotati di competenze tecniche che permettano di svolgere efficacemente la funzione assegnata.
- Continuità di azione. Per garantire un costante ed effettivo monitoraggio sul Modello di SevenData.
- In relazione alla composizione dell'Organismo di Vigilanza, il D.Lgs. n. 231/2001 consente di optare per una composizione monocratica o collegiale. La scelta deve essere, in ogni caso, idonea ad assicurare l'effettività e l'efficienza dei controlli, in relazione alla dimensione e complessità organizzativa dell'ente nonché garantire i requisiti di autonomia, indipendenza, professionalità e continuità di azione dell'Organismo di Vigilanza.
- Per questi motivi, il Consiglio di Amministrazione di SevenData ha ritenuto di istituire un Organismo di Vigilanza monocratico, connotato da competenze e professionalità trasversali.

In particolare, i componenti, nel loro complesso, devono essere in possesso dei seguenti requisiti:

- Competenza in materia giuridica.
- Conoscenza dei processi aziendali.
- Competenza amministrative e di controllo di gestione.
- Competenza in materia di sicurezza e ambiente.

Il Consiglio di Amministrazione valuta periodicamente l'adeguatezza dell'Organismo di Vigilanza in termini di struttura organizzativa e di poteri conferiti, apportando, se del caso, modifiche alla composizione.

1.3. Funzionamento dell'Organismo di Vigilanza

L'Organismo di Vigilanza si dota autonomamente di un proprio Regolamento, con il quale disciplina il proprio funzionamento: esemplificativamente, modalità di riunione, cadenze temporali dei controlli, individuazione dei criteri e delle procedure di analisi, calendarizzazione delle attività, verbalizzazione delle riunioni.

1.4. Cessazione dell'Organismo di Vigilanza

L'Organismo di Vigilanza rimane in carica per tre anni.

L'Organismo di Vigilanza cessa dalle proprie funzioni se viene a mancare, per qualunque causa, la maggioranza dei componenti.

I componenti dell'Organismo di Vigilanza possono rinunciare alla propria carica, mediante preavviso di almeno tre mesi, a mezzo raccomandata con avviso di ricevimento o posta elettronica certificata: in tal caso, il Consiglio di Amministrazione provvede alla nomina di un nuovo componente.

La revoca dell'Organismo di Vigilanza e di ciascun componente compete esclusivamente al Consiglio di Amministrazione. Ciascun membro può essere revocato con un preavviso di almeno tre mesi.

I poteri dell'Organismo di Vigilanza sono prorogati sino alla nomina del nuovo Organismo di Vigilanza. I componenti dell'Organismo di Vigilanza sono rieleggibili.

1.5. Funzioni e poteri e dell'Organismo di Vigilanza

L'Organismo di Vigilanza vigila su:

- L'efficacia del Modello, in relazione alla struttura aziendale e alla effettiva idoneità dello stesso a prevenire la commissione dei reati presupposto.
- L'osservanza delle prescrizioni del Modello da parte dei Destinatari. Il controllo si sostanzia nella verifica della coerenza tra i comportamenti concreti e le disposizioni del Modello.
- L'aggiornamento del Modello.
- Il sistema sanzionatorio applicabile alle violazioni del Modello, con l'ausilio della Funzione aziendale competente.

In ogni caso, il Consiglio di Amministrazione è responsabile dell'adozione e dell'aggiornamento del Modello.

A fronte degli obblighi di vigilanza sopra indicati, l'Organismo di Vigilanza dovrà, a livello operativo, svolgere i seguenti specifici compiti:

Con riferimento alla verifica dell'efficacia del Modello, l'Organismo di Vigilanza:

- Conduce ricognizioni dell'attività aziendale, al fine di mantenere aggiornata la mappatura delle aree a rischio.
- Aggiorna le attività relative alle aree a rischio, avvalendosi delle Funzioni aziendali competenti. Pertanto, l'Organismo di Vigilanza viene tenuto costantemente informato dell'evoluzione delle attività svolte nelle aree a rischio.
- Verifica, avvalendosi delle Funzioni aziendali competenti, che le soluzioni organizzative adottate siano adeguate a consentire un'efficace attuazione del Modello.

Con riferimento alla verifica dell'osservanza del Modello, l'Organismo di Vigilanza:

- Promuove idonee iniziative per la diffusione, la conoscenza e la comprensione dei principi contenuti del Modello.
- Raccoglie, elaborare, conservare ed aggiornare le informazioni rilevanti in ordine al rispetto del Modello.
- Conduce indagini interne per accertare eventuali violazioni del Modello.

Con riferimento all'effettuazione di proposte di aggiornamento del Modello e di monitoraggio, l'Organismo di Vigilanza:

- Valuta periodicamente, sulla base dei risultati delle attività di verifica e controllo, l'adeguatezza del Modello rispetto alle prescrizioni contenute nel D.Lgs. n. 231/2001.

- Propone periodicamente al Consiglio di Amministrazione, sulla base dei risultati delle attività di verifica e controllo: i) l'adeguamento del Modello. ii) l'implementazione del Modello (predisposizione di procedure, adozione di clausole contrattuali standard, e così via).
- Verifica periodicamente l'attuazione e l'effettiva funzionalità delle azioni correttive proposte.

Inoltre, ogni variazione dell'organigramma di SevenData, dei mansionari, del sistema delle deleghe e procure è oggetto di valutazione da parte dell'Organismo di Vigilanza di SevenData, al fine di definire se incidano o meno sul Modello. Se del caso, l'Organismo di Vigilanza propone al Consiglio di Amministrazione gli opportuni aggiornamenti.

1.6. Operatività e verifiche dell'Organismo di Vigilanza

SevenData prevede apposite forme di raccordo tra l'Organismo di Vigilanza e le Funzioni aziendali.

L'Organismo di Vigilanza può avvalersi dell'ausilio delle competenti Funzioni aziendali e di consulenti esterni.

1.7. Obblighi di informazione da parte dell'Organismo di Vigilanza

L'Organismo di Vigilanza informa il Consiglio di Amministrazione in merito alla propria attività. In particolare, riferisce per iscritto:

- Con cadenza periodica, in merito alla propria attività di vigilanza.
- Tempestivamente, gravi criticità del Modello.
- Immediatamente, ogni violazione del Modello.

L'Organismo di Vigilanza riferisce, altresì, al Consiglio di Amministrazione in merito a:

- Azioni correttive, ritenute idonee ad assicurare l'efficacia e l'effettività del Modello.
- Carenze organizzative o procedurali tali da esporre SevenData al pericolo che siano commessi reati presupposto.
- Mancata o carente collaborazione da parte delle Funzioni aziendali di volta in volta interessate.

Gli incontri dell'Organismo di Vigilanza con le Funzioni aziendali e con gli Organi Sociali risultano da processo verbale.

1.8. Obblighi di informazione dell'Organismo di Vigilanza

La vigilanza sul funzionamento del Modello, e l'accertamento di eventuali violazioni dello stesso, è assicurata da una regolare informativa dell'Organismo di Vigilanza proveniente dalle singole Funzioni aziendali, come previsto dall'art. 6, comma 2, lett. d, D.Lgs. n. 231/2001.

Tale obbligo, rivolto alle Funzioni aziendali che operano nelle aree a rischio reato, riguarda le risultanze periodiche delle attività poste in essere e le atipicità o anomalie riscontrate nell'ambito delle informazioni disponibili.

Devono, inoltre, essere trasmesse all'Organismo di Vigilanza tutte le informative che presentino elementi rilevanti in relazione all'attività di vigilanza, quali a titolo esemplificativo:

- Informazioni provenienti da organi di polizia giudiziaria, da Autorità Pubbliche di Vigilanza o altre Autorità, dalle quali risulti lo svolgimento di indagini relative a reati presupposto.
- Relazioni interne che evidenziano la commissione di reati presupposto.

- Report predisposti dai Responsabili di Funzione, dai quali emergano atti o fatti con profili di criticità rispetto alle previsioni del D.Lgs. n. 231/2001.
- Copia della reportistica periodica in materia di salute e sicurezza sul lavoro (ad esempio, copia del Documento di Valutazione dei Rischi), nonché di incidenti, infortuni e visite ispettive.
- Notizie relative a commesse da parte di soggetti pubblici.
- Ogni eventuale modifica e/o integrazione al sistema di deleghe e procure.
- Cambiamenti organizzativi o di business.
- Adozione di nuove procedure o la modifica delle procedure esistenti.
- Notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello, con evidenza degli eventuali procedimenti disciplinari svolti e delle sanzioni irrogate, ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.
- Bilancio annuale, corredato della nota integrativa, nonché la situazione patrimoniale semestrale.
- Incarichi conferiti alla società di revisione.
- Comunicazioni della società di revisione, relative ad ogni criticità emersa, anche se risolta.
- *Mala gestio* aziendale.
- Ogni violazione del Modello.

In aggiunta a tali informazioni, i Responsabili delle Funzioni aziendali comunicano periodicamente all'Organismo di Vigilanza le seguenti informazioni:

- Elenco nominativo dei soggetti legittimati a intrattenere relazioni con soggetti pubblici, con indicazione dettagliata dei contatti intrattenuti da altri soggetti vicari per motivi di urgenza e necessità.
- Elenco nominativo dei soggetti aziendali che ricoprono il ruolo di pubblico ufficiale o incaricato di pubblico servizio.
- Atti emanati dal soggetto pubblico che incidono sulla gestione di SevenData
- Atti di rendicontazione destinati al socio pubblico o ad altri soggetti pubblici.
- Istanze di concessione di finanziamenti pubblici.

L'Organismo di Vigilanza può sempre richiedere integrazioni e approfondimenti in merito alle informazioni trasmesse dalle Funzioni aziendali.

1.9. Obblighi generali di informazione nei confronti dell'Organismo di Vigilanza

Per dare attuazione al disposto ex art. 6 comma 2 lett. d) del Decreto "prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli", la Società contempla due categorie di flussi informativi:

a. Flussi informativi generali e informazioni non strutturate consistenti:
   - nell'obbligo generale in capo ai responsabili delle funzioni aziendali o i referenti individuati da costoro, di comunicare all'Organismo di Vigilanza ogni informazione utile per agevolare lo svolgimento delle verifiche sulla corretta attuazione del Modello. Inoltre, qualora riscontrino ambiti di miglioramento nella definizione e/o

nell'applicazione dei protocolli di prevenzione definiti nel Modello, trasmettono all'Organismo di Vigilanza una relazione contenente: i) una descrizione sullo stato di attuazione dei protocolli di prevenzione delle attività a rischio di propria competenza; ii) una descrizione delle attività di verifica effettuate per quanto all'attuazione dei protocolli di prevenzione e/o delle azioni di miglioramento intraprese; iii) le eventuali proposte di modifiche ai protocolli/procedure di prevenzione;

- nell'obbligo in capo a tutti i responsabili delle funzioni aziendali di comunicare all'OdV: i) l'emissione e/o l'aggiornamento di disposizioni, comunicati organizzativi o linee guida e procedure aziendali; ii) l'eventuale aggiornamento del sistema delle deleghe e procure aziendali;
- nell'obbligo da parte di tutti i dipendenti di segnalare direttamente all'Organismo di Vigilanza nell'apposito indirizzo di posta elettronica (odv@sevendata.it), qualunque violazione parte dei Dipendenti, degli Organi Sociali, degli Agenti, dei Consulenti, Partner commerciali e finanziari di norme o qualunque evento che potrebbe rappresentare una violazione al Codice Etico, ai principi di cui al d.lgs. 231/01 o comportare rischi di responsabilità ai sensi del Decreto. Qualunque responsabile di Funzione che abbia ricevuto segnalazione di tali circostanze da un proprio sottoposto o da un consulente o fornitore, inoltra la segnalazione all'Organismo di Vigilanza conservando copia della mail inoltrata. Gli agenti, i consulenti, i collaboratori e i partner commerciali e/o finanziari devono effettuare ogni segnalazione direttamente all'Organismo di Vigilanza o alle Direzioni aziendali preposte.

b. informazioni strutturate, ad evento o periodiche

Si tratta di informazioni da inviare all'OdV a cura di ciascuna funzione aziendale e riferite ai processi sensibili. È compito dell'Organismo di Vigilanza definire e rivedere periodicamente, per ciascun processo sensibile o area di rischio le informazioni necessarie per esercitare i propri compiti. Tali informazioni possono essere:

- ad evento: nel senso che al verificarsi di un dato evento l'informazione deve essere resa all'OdV (es. avvio di ispezioni da parte di Autorità Esterne, infortunio grave sul lavoro etc.…);
- periodiche: nel senso che con cadenza periodica (mensile, trimestrale, semestrale, annuale) vengono trasmessi dati aggregati all'OdV relativi a determinati eventi o operazioni (es. mancati infortuni sul lavoro, nuovi fornitori inseriti in anagrafica, acquisti fuori procedura per importi superiori ad un ammontare prestabilito). Per taluni eventi o operazioni la ciclica valutazione del rischio consentirà di definire se un informazione dovrà essere fornita immediatamente o su base periodica.
-

L'Organismo di Vigilanza valuta le segnalazioni ricevute definendo i provvedimenti conseguenti in conformità con quanto previsto al successivo paragrafo.

L'Organismo di Vigilanza può decidere di richiedere alle funzioni aziendali una dichiarazione attestante – con riferimento ad un dato periodo – l'assenza di eventi che richiedevano l'invio di informazioni.

c. Le operazioni in deroga o fuori procedura.

Le operazioni o le scelte aziendali sono da considerarsi in deroga o fuori procedura o fuori sistema, quando sono assunte al di fuori delle procedure aziendali standard o quando non sono tracciate nei sistemi di gestione.

Tuttavia, pur rendendosi a volte necessario procedere in difformità rispetto alle procedure standard per non ingessare l'operatività aziendale, anche in questi casi, è necessario rispettare le seguenti regole di controllo:

a. Presupposti il ricorso alle deroghe è ammesso in presenza di presupposti connessi ad esigenze aziendali quali a titolo esemplificativo ma non esaustivo:
   - Necessità e urgenza (es. acquisti a fronte di un evento straordinario o di un incidente non compatibili con tempi di selezione di un fornitore)
   - Iperspecializzazione, quando cioè quel fornitore è riconosciuto come altamente specializzato in quella tipologia di fornitura o servizio;
   - Rapporto fiduciario: riferito a legali, consulenti o, nella selezione del personale alla fiducia nei confronti di chi segnala il candidato (es. altro dipendente)
   - Esistenza di contratti quadro

b. Tracciabilità
   - Ogni operazione in deroga deve essere rigorosamente tracciata mediante conservazione di tutta la documentazione formale e informale che ne comprovi la correttezza (es. mail scambiate con il fornitore);
   - il rigore nella conservazione della documentazione informale è commisurato all'entità dell'operazione ed è rimandato ai protocolli riferiti ai singoli processi sensibili. L'OdV potrà richiedere alle singole funzioni aziendali un maggior livello di tracciabilità ed un aggiornamento continuo, in relazione a singole operazioni.

c. Informativa all'OdV

Le operazioni in deroga vengono comunicate all'OdV dalle singole funzioni responsabili, ad evento o con periodicità a seconda dell'entità dell'operazione.

1.10. Whistleblowing Scheme

SevenData predispone un sistema di whistleblowing, inteso come procedura che consente ai Destinatari di segnalare riservatamente all'Organismo di Vigilanza le violazioni del Modello.

I Destinatari segnalano le violazioni del Modello all'Organismo di Vigilanza, delle quali siano venuti a conoscenza in ragione del loro rapporto con SevenData, attraverso il sistema di Whistleblowing. Le segnalazioni possono essere effettuate solo agendo in buona fede.

L'Organismo di Vigilanza istituisce una casella di posta elettronica dedicata, cui inoltrare le predette segnalazioni: odv@sevendata.it

A seguito della segnalazione, l'Organismo di Vigilanza svolge le investigazioni necessarie e valuta le eventuali ed opportune misure da adottare.

L'Organismo di Vigilanza:
- Garantisce la conservazione dei dati ricevuti.
- Informa il segnalante ed il segnalato degli sviluppi delle investigazioni.

1.11. Contenuto della comunicazione

SevenData individua il contenuto minimo della segnalazione. In ogni caso, la segnalazione contiene l'indicazione:

- Del soggetto segnalante. Il soggetto segnalante dichiara se ha un interesse collegato alla comunicazione.
- Del soggetto al quale il Destinatario ritenga imputabile la violazione del Modello. SevenData individua i soggetti che possono essere segnalati, garantendo la riservatezza sulla loro identità.
- Degli elementi utili alla ricostruzione della violazione del Modello e alla sua verifica.

1.12. Tutela del whistleblower

SevenData predispone forme di whistleblowing conformi alla legislazione in materia di protezione e trattamento dei dati personali.

L'identità del segnalante è riservata. Non può essere rivelata senza il suo consenso, salvo le eccezioni previste dalla legge.

Nello specifico, il prestatore di lavoro che abbia segnalato violazioni del Modello all'Organismo di Vigilanza non può essere sanzionato, licenziato o sottoposto a misure discriminatorie, dirette o indirette, incidenti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla predetta segnalazione.

1.13. Verifiche

Il Modello è soggetto, peraltro, a specifiche verifiche congiunte da parte dell'Organismo di Vigilanza di SevenData e delle Funzioni aziendali di volta in volta competenti. Nello specifico, trattasi di:

- Verifiche di atti: semestralmente verifica i principali atti societari (delibere, modifiche allo Statuto, bilanci e relative relazioni) ed i contratti di maggior rilevanza conclusi da SevenData nell'ambito di aree a rischio.
- Verifica delle procedure: verifica costantemente l'efficace attuazione di procedure, regolamenti ed istruzioni operative.

Delle verifiche è redatto processo verbale.

Parte Sesta

1. Adozione, aggiornamento e miglioramento continuo del modello

L'adozione e l'efficace attuazione del Modello sono, per espressa previsione legislativa, una responsabilità rimessa al Consiglio di Amministrazione. Ne deriva che il potere di adottare eventuali aggiornamenti del Modello compete altresì al Consiglio di Amministrazione, che lo esercita mediante delibera con le modalità previste per la sua adozione.

L'attività di aggiornamento, intesa sia come integrazione sia come modifica, è volta a garantire l'adeguatezza e l'idoneità del Modello, valutate rispetto alla funzione preventiva di commissione dei reati previsti dal D. Lgs. 231/2001.

Compete, invece, all'Organismo di Vigilanza la concreta verifica circa la necessità od opportunità di procedere all'aggiornamento del Modello, facendosi promotore di tale esigenza nei confronti del Consiglio. L'Organismo di Vigilanza, nell'ambito dei poteri ad esso conferiti conformemente agli art. 6, comma 1 lett. b) e art. 7, comma 4 lett. a) del Decreto, ha la responsabilità di formulare al Consiglio di Amministrazione proposte in ordine all'aggiornamento e all'adeguamento del presente Modello.

In ogni caso il Modello deve essere tempestivamente modificato ed integrato dal Consiglio di Amministrazione, anche su proposta e previa consultazione dell'Organismo di Vigilanza, quando siano intervenute:

- variazioni ed elusioni delle prescrizioni in esso contenute che ne abbiano evidenziato l'inefficacia o l'incoerenza ai fini della prevenzione dei reati;
- significative modificazioni all'assetto interno della Società e/o delle modalità di svolgimento delle attività di impresa;
- modifiche normative.

Restano in capo all'Organismo di Vigilanza i seguenti compiti:

- condurre ricognizioni periodiche volte ad identificare eventuali aggiornamenti al novero dell'attività aziendale ai fini dell'aggiornamento della mappatura delle attività sensibili;
- coordinarsi con il responsabile di Direzione per i programmi di formazione per il personale;
- interpretare la normativa rilevante in materia di reati presupposti, nonché le Linee Guida eventualmente predisposte, anche in aggiornamento a quelle esistenti, e verificare l'adeguatezza del sistema di controllo interno in relazione alle prescrizioni normative o relative alle Linee Guida;
- verificare le esigenze di aggiornamento del Modello.

I Responsabili delle Direzioni interessate elaborano e apportano le modifiche delle procedure operative di loro competenza, quando tali modifiche appaiano necessarie per l'efficace attuazione del Modello, ovvero qualora si dimostrino inefficaci ai fini di una corretta attuazione delle disposizioni del Modello. Le funzioni aziendali competenti curano altresì le modifiche o integrazioni alle procedure necessarie per dare attuazione alle eventuali revisioni del presente Modello.

Le modifiche, gli aggiornamenti e le integrazioni del Modello devono essere sempre comunicati all'Organismo di Vigilanza.

GLOSSARIO

Nel Documento, nella Parte Speciale e nella Mappatura dei Rischi di Dettaglio, le espressioni utilizzate assumono il significato di seguito indicato:

Attività aziendali a rischio reato (o Attività a rischio o Aree a rischio): atti, fatti od operazioni che, anche potenzialmente, potrebbero esporre SevenData S.p.A. al rischio derivante dall'eventuale commissione di reati presupposto.

CCNL: Contratto/i Collettivo/i Nazionale/i di Lavoro.

Codice Disciplinare: insieme di regole che il personale di lavoro deve osservare in costanza di rapporto, previsto dall'art. 7, comma 1, Statuto dei Lavoratori ("*Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti*").

Codice di Comportamento: documento attraverso il quale SevenData esplicita valori, principi di comportamento, impegni e responsabilità che essa assume verso l'interno e l'esterno.

D.Lgs. 231/2001: Decreto Legislativo 8 giugno 2001, n. 231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni ed integrazioni.

Destinatari del Modello (o Destinatari): soggetti tenuti all'osservanza del Modello. A titolo meramente esemplificativo, ma non esaustivo, rientrano in tale categoria i Soggetti Apicali ed i Soggetti Sottoposti.

Talora, si fa riferimento ai Destinatari terzi cioè coloro che, pur essendo esterni alla struttura societaria di SevenData S.p.A., intrattengono con essa rapporti di qualsiasi natura e durata. A titolo meramente esemplificativo sono Destinatari terzi, le imprese assicuratrici, gli istituti di credito, i partner, i fornitori di beni e servizi, i consulenti, le agenzie di comunicazione e pubblicità, le società di somministrazione di lavoro, i mass media, gli organismi certificatori, le associazioni di categoria.

Personale (o prestatore o dipendente): tutti coloro che intrattengono con SevenData S.p.A. un rapporto di lavoro, di qualunque tipo.

Modello (o Modello 231): Modello di organizzazione, gestione e controllo, così come previsto e disciplinato dal D.Lgs. 231/2001, adottato dal Consiglio di Amministrazione di SevenData S.p.A. Il Modello di SevenData è composto da Parte Generale, Parte Speciale (Schede Reato, Protocolli di Controllo 231, Sintesi Mappatura dei Rischi, Clausola Contrattuale 231), Mappatura dei Rischi di Dettaglio.

Organi Sociali: Assemblea dei Soci e Consiglio di Amministrazione.

Organismo di Vigilanza (o O.d.V.): Organismo previsto dall'art. 6 del D.Lgs. 231/2001, con il compito di vigilare sul funzionamento, sull'osservanza e sull'aggiornamento del Modello.

Protocollo di Controllo 231 (o Protocolloi231): insieme di regole comportamentali e di presidi di controllo che i Destinatari sono tenuti ad osservare, in Italia ed all'estero, il cui rispetto contribuisce a prevenire la commissione dei reati presupposto.

I Protocolli si articolano in: Protocolli Generali, ossia principi e regole di carattere generale che i Destinatari sono tenuti ad osservare in tutte le attività a rischio; Protocolli Speciali, ossia disposizioni particolari disciplinanti aspetti peculiari delle attività a rischio, ovvero costituenti declinazione di Protocolli Generali.

Procedura interna (o procedura aziendale o procedura o normativa interna): insieme di regole, emanate dalla Funzione aziendale competente, disciplinanti nel dettaglio lo svolgimento di un determinato processo, sottoprocesso ed attività. Le procedure attuano i Protocolli ed individuando, tra l'altro, le responsabilità delle singole entità aziendali, il soggetto responsabile dello svolgimento di una certa fase dell'attività, i controlli previsti ed i flussi informativi nei confronti dell'Organismo di Vigilanza.

Reati presupposto: reati previsti dal D.Lgs. 231/2001, la cui commissione, oltre alla responsabilità personale dell'autore materiale, determina, altresì, il sorgere della responsabilità amministrativa da reato a carico della Società. L'elenco dei reati presupposto è contenuto nella Parte Speciale, documento denominato Schede Reato.

Sistema Disciplinare: insieme delle misure sanzionatorie applicabili in caso di violazione del Modello.

SevenData (o Società): SevenData S.p.A.

Soggetti Apicali: persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché le persone che esercitano, anche di fatto, la gestione e il controllo. Esemplificativamente, rientrano nella definizione di Soggetto Apicale, i Componenti del Consiglio di Amministrazione - e, quindi, anche il Presidente e l'Amministratore Delegato - i Dirigenti e, più in generale, i soggetti deputati a ruoli di vertice.

Soggetti Sottoposti: persone sottoposte alla direzione o alla vigilanza dei Soggetti Apicali. Esemplificativamente, rientrano nella definizione di Soggetto Sottoposto, tutti coloro i quali operano nella Società in posizione di subordinazione, anche se non formalmente inquadrabili in un rapporto di lavoro dipendente, purché sottoposti a direzione e vigilanza di Soggetti Apicali. Peraltro, non possono essere escluse a priori dalla categoria di Soggetto Sottoposto, i liberi professionisti o i lavoratori autonomi (Partita IVA) o legati da altro tipo di rapporto (come il c.d. Stage o lavoratori in somministrazione).

Soggetti pubblici: Pubbliche Amministrazioni centrali e locali, anche estere e sovrannazionali, con particolare riferimento a Ministero dell'Ambiente e della Tutela del Territorio e del Mare, Istituto Superiore di Sanità, Regioni, Comune di Milano, Autorità Giudiziaria, Guardia di Finanza, INPS, INAIL, Direzione Territoriale del Lavoro (DTL), ASL, ISPRA, ARPA, Vigili del Fuoco, Agenzia delle Entrate, Camere di Commercio, Capitaneria di Porto, Questura, Ufficio Territoriale del Governo, Autorità Amministrative Indipendenti, Autorità Pubbliche di Vigilanza in genere ed ogni Stazione Appaltante. Ogni altra Pubblica Amministrazione ed ogni altro pubblico ufficiale, incaricato di pubblico servizio ed esercente un servizio di pubblica necessità, italiano, straniero o sovrannazionale.

Statuto dei Lavoratori: legge 20 maggio 1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento". Concretamente, lo Statuto dei Lavoratori rappresenta la disciplina di riferimento per i rapporti tra personale di lavoro e Società.

Violazione del Modello: a titolo meramente esemplificativo integra violazione del Modello: qualsiasi atto o comportamento, commissivo od omissivo, doloso o colposo, non conforme alle prescrizioni contenute nel Modello; la commissione, dolosa o colposa, di un reato presupposto, tentato o consumato; ogni altra violazione delle disposizioni contenute nel D.Lgs. 231/2001.

Whistleblowing: istituto che consente al Destinatario di segnalare riservatamente all'Organismo di Vigilanza eventuali violazioni del Modello, di cui venga a conoscenza in ragione dei propri rapporti con SevenData S.p.A. Il *whistleblower* è il Destinatario che segnala all'Organismo di Vigilanza le eventuali violazioni del Modello. Il *Sistema di Whistleblowing* è la procedura che consente ai Destinatari di segnalare all'Organismo di Vigilanza le violazioni del Modello.