



# Modello di organizzazione, gestione e controllo ex D. Lgs. 231/2001

Aggiornamento del 24 maggio 2019

DATA REVISIONE	24 maggio 2019
----------------	----------------



## Indice

<b>PARTE GENERALE</b> .....	<b>4</b>
<b>DEFINIZIONI</b> .....	<b>4</b>
<b>PREMESSA</b> .....	<b>6</b>
<b>CAPITOLO 1</b> .....	<b>7</b>
IL DECRETO LEGISLATIVO N. 231/2001.....	7
IL SISTEMA DEI CONTROLLI INTERNI E LE AFFINITÀ CON IL D. LGS. N. 231/01 .....	11
<b>CAPITOLO 3</b> .....	<b>15</b>
ADOZIONE DEL MODELLO DA PARTE DELLA SOCIETÀ .....	15
3.1 <i>Obiettivi perseguiti con l'adozione del Modello</i> .....	15
3.3 <i>Struttura del Modello: Parte Generale e Parti Speciali in funzione delle diverse ipotesi di reato</i> .....	16
3.4 <i>Adozione del Modello</i> .....	16
3.5 <i>Modalità di attuazione del Modello e principi comuni</i> .....	16
3.6 <i>Risk assessment – metodologia adottata</i> .....	17
3.7 <i>Destinatari del Modello</i> .....	19
<b>CAPITOLO 4</b> .....	<b>20</b>
ORGANISMO DI VIGILANZA .....	20
4.1 <i>Individuazione dell'Organismo di Vigilanza</i> .....	20
4.2 <i>Funzioni e poteri dell'Organismo di Vigilanza</i> .....	22
4.3 <i>L'operatività dell'Organismo di Vigilanza all'interno della Società</i> .....	23
4.4 <i>L'attività di reporting dell'Organismo di Vigilanza verso altri organi aziendali</i> .....	23
4.5 <i>Flussi informativi</i> .....	23
4.6 <i>Whistleblowing</i> .....	25
<b>CAPITOLO 5</b> .....	<b>26</b>
CODICI DI COMPORTAMENTO .....	26
5.1 <i>Integrità etica</i> .....	26
<b>CAPITOLO 6</b> .....	<b>28</b>
SISTEMA DISCIPLINARE .....	28
6.1 <i>Principi generali</i> .....	28
6.2 <i>Sanzioni previste per i lavoratori dipendenti (aree professionali e quadri direttivi)</i> .....	28
6.3 <i>Sanzioni previste per i dirigenti</i> .....	28
6.4 <i>Sanzioni previste per i componenti del Consiglio di Amministrazione</i> .....	29
6.5 <i>Sanzioni previste per collaboratori, consulenti, procuratori, agenti e terzi</i> .....	29
6.6 <i>Sanzioni previste per chi viola le misure di tutela del segnalante</i> .....	29
6.7 <i>Sanzioni previste per chi effettua con dolo o colpa grave segnalazione che si rivelano infondate.</i> .....	29



*Modello Organizzativo  
Gestione e Controllo  
ex D. Lgs. 231/2001*

*Parte generale*



## Parte Generale

### Definizioni

Le seguenti definizioni si riferiscono a tutte le parti del Modello, fatte salve ulteriori eventuali definizioni contenute nelle singole parti speciali.

**Aree a Rischio:** le aree di attività della Società nel cui ambito risulta profilarsi, in termini più concreti, il rischio di commissione dei Reati.

**Banca:** Banca Finanziaria Internazionale S.p.A., in breve Banca Finint S.p.A.

**Capogruppo:** Banca Finint S.p.A. che esercita attività di direzione e coordinamento sulle società del Gruppo.

**CCNL:** il Contratto Collettivo Nazionale di Lavoro applicato dalla Società.

**Codice Etico:** il codice etico adottato dalla Società, approvato dal Consiglio di Amministrazione e relativi aggiornamenti.

**Collaboratori Esterni:** tutti i collaboratori esterni complessivamente considerati, vale a dire i Consulenti, i Partner e i Fornitori.

**Consulenti:** i soggetti che agiscono in nome e/o per conto della Società in forza di un contratto di mandato o di altro rapporto contrattuale di collaborazione professionale.

**Destinatari:** gli Esponenti Aziendali, i dipendenti ed i Collaboratori Esterni.

**Direzione:** si intendono gli amministratori delegati e i dirigenti aziendali.

**Dipendenti:** i soggetti aventi un rapporto di lavoro subordinato con la Società, ivi compresi i dirigenti.

**D.Lgs. 231/2001 o il Decreto:** il D.Lgs. 8 giugno 2001 n. 231 e successive modifiche e integrazioni.

**Enti:** ai sensi del D. Lgs. 231/2001, qualsiasi società, associazione o fondazione o altro soggetto di diritto, sia esso dotato di personalità giuridica o meno, nonché qualsiasi ente pubblico economico.

**Esponenti Aziendali:** il Presidente e i componenti dell'Organo con Funzione di Supervisione Strategica e dell'Organo con Funzione di Controllo, nonché qualsiasi altro soggetto in posizione apicale, per tale intendendosi qualsiasi persona che rivesta funzioni di rappresentanza, amministrazione o direzione della Società di una sua funzione, ai sensi del Decreto (ivi inclusi i responsabili di unità organizzative della Società).

**Fornitori:** i fornitori di beni e servizi non professionali della Società o del Gruppo che non rientrano nella definizione di Partner.

**Illeciti:** gli illeciti amministrativi di abuso di informazioni privilegiate (art. 187-bis TUF) e di manipolazione del mercato (art. 187-ter TUF).

**Incaricati di un pubblico servizio:** ai sensi dell'art. 358 cod. pen. "sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".



**Modello:** il presente modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001, approvato dal Consiglio di Amministrazione della Società e completo della Parte Speciale e degli Allegati.

**Organi Sociali:** il Consiglio di Amministrazione, il Collegio Sindacale e i loro componenti.

**Organismo di Vigilanza o OdV:** l'organismo interno di controllo, preposto alla vigilanza sul funzionamento e sull'osservanza del Modello nonché al relativo aggiornamento.

**P.A.:** la Pubblica Amministrazione (meglio definita nello specifico regolamento dedicato ai rapporti con la Pubblica Amministrazione), con riferimento ai reati nei confronti della Pubblica Amministrazione, i pubblici ufficiali e gli incaricati di un pubblico servizio.

**Partner:** le controparti contrattuali con le quali la Società addivenga ad una qualche forma di collaborazione contrattualmente regolata, ove destinati a cooperare con la Società o con il Gruppo nell'ambito delle Aree a Rischio.

**Pubblici Ufficiali:** ai sensi dell'art. 357 cod. pen. “sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione o manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi”.

**Reati o Reati Presupposto:** le fattispecie di reato alle quali si applica la disciplina prevista dal D.Lgs. 231/2001 sulla responsabilità amministrativa degli enti.

**Regolamento Interno:** è un documento interno, approvato dal Consiglio di Amministrazione della Società come di volta in volta aggiornato, composto da due sezioni: la prima descrive le procedure interne adottate dalla Società, alle quali i dipendenti della stessa devono rifarsi nello svolgimento dei propri compiti; la seconda è dedicata alla descrizione delle norme interne di comportamento stabilite dalla Società per i propri dipendenti, incluso il cosiddetto “Codice Etico”.

**Regolamenti:** indica il Regolamento Interno e la Relazione sulla Struttura Organizzativa.

**Relazione sulla Struttura Organizzativa:** il documento che illustra l'organizzazione interna nonché il sistema dei controlli interni adottati dalla Società tempo per tempo vigente ed approvato dal Consiglio di Amministrazione.

**Responsabile Interno:** soggetto interno alla Società al quale viene attribuita la responsabilità singola o condivisa con altri per le operazioni nelle Aree a Rischio.

**Società:** Securitisation Services S.p.A..

**Soggetti Apicali:** persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua unità dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione od il controllo della stessa.

**Soggetti Sottoposti:** soggetti sottoposti alla direzione o alla vigilanza di Soggetti Apicali.

**TUB:** il D. Lgs. 1 settembre 1993, n. 385 e successive modifiche e integrazioni (Testo Unico Bancario).

**TUF:** il D.Lgs. 24 febbraio 1998 n. 58 e successive modifiche e integrazioni (Testo Unico della Finanza).



## Premessa

Securitisation Services S.p.A., società facente parte del Gruppo Banca Finanziaria Internazionale S.p.A., sensibile all'esigenza di garantire e promuovere condizioni di correttezza e trasparenza nella conduzione delle attività aziendali. A tal fine ha ritenuto opportuno procedere all'attuazione del proprio Modello di Organizzazione e Gestione ai sensi di quanto previsto dal D. Lgs n. 231/2001.

Al di là di quanto prescritto dal Decreto, che indica il Modello come elemento facoltativo e non obbligatorio, l'iniziativa di adottare il Modello è stata assunta nella convinzione che esso possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano per la Società e per tutte le realtà che collaborano con essa, in modo che seguano, nell'espletamento delle proprie attività, comportamenti corretti e trasparenti tali da prevenire il rischio di commissione dei reati contemplati dal D.Lgs 231/01.

In ultima analisi, la Società ritiene che l'adozione di tale Modello tuteli le aspettative dei propri clienti, il lavoro dei propri dipendenti e collaboratori nonché la posizione e la propria immagine.

Il presente Modello è articolato in una "Parte Generale" e in una "Parte Speciale".

La funzione della Parte Generale è quella di definire, nel complesso, il sistema strutturato e organico finalizzato a prevenire la commissione delle diverse tipologie di reato di cui al Decreto.

La funzione della parte Speciale è quella di definire, per ogni fattispecie di reato, comportamenti generali e specifici finalizzati a prevenire la commissione delle diverse tipologie di reato di cui al Decreto.



## Capitolo 1

### Il Decreto Legislativo n. 231/2001

#### Il regime di responsabilità amministrativa previsto a carico delle persone giuridiche, società ed associazioni

Il Decreto Legislativo n. 231, approvato l'8 giugno 2001 in esecuzione della delega contenuta nell'art. 11 della Legge 29 settembre 2000 n. 300 ed entrato in vigore il 4 luglio 2001 (di seguito anche *Decreto*), ha inteso adeguare la normativa nazionale in materia di responsabilità delle persone giuridiche ad alcune Convenzioni internazionali a cui l'Italia aveva già da tempo aderito. Il Decreto, recante "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*", rappresenta un fattore di assoluta innovazione nel quadro normativo italiano in quanto afferma il principio che non solo i singoli individui ma anche gli enti possono essere perseguiti e sanzionati per i reati commessi - purché nell'interesse o a vantaggio dell'organizzazione - dai soggetti che vi operano.

In sintesi, il D. Lgs. 231/2001:

- introduce i principi generali e i criteri di attribuzione della responsabilità amministrativa;
- individua i reati in relazione ai quali può insorgere la responsabilità amministrativa delle società (cd. *reati-presupposto* della suddetta responsabilità amministrativa);
- prevede le sanzioni che possono derivare a carico dell'Ente dalla commissione del reato-presupposto;
- individua gli adempimenti necessari affinché, anche in ipotesi di avvenuta commissione di uno dei reati-presupposto (e ferma la responsabilità penale personale di chi ha agito) l'Ente possa essere esonerato dalla suddetta responsabilità che normalmente consegue alla commissione di uno dei reati-presupposto.

Dal punto di vista **soggettivo**, l'Ente può essere sanzionato per un reato commesso da:

- a) "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 degli stessi" (**Soggetti Apicali**);
- b) "persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera (a)" – vale a dire i Soggetti Apicali (**Soggetti Sottoposti**).

La responsabilità in esame si aggiunge a quella della persona fisica che ha realizzato materialmente il fatto. Elemento qualificante della condotta di tali soggetti è che essi abbiano agito:

- a) nell'**interesse** dell'ente, inteso come convenienza ed utilità che l'ente medesimo potrebbe ottenere dalla commissione del comportamento illecito (ad es. aumento del fatturato, consolidamento del "posizionamento competitivo" o mantenimento di una situazione di "monopolio", risparmio sui tempi operativi, notorietà e referenze, etc.) **oppure**;
- b) a **vantaggio** dell'ente stesso, inteso come effettivo ottenimento di un risultato economico come conseguenza del comportamento illecito (ad es. risparmio sui costi necessari a garantire la sicurezza sui luoghi di lavoro, utile economico, etc.).

I reati da cui può scaturire la responsabilità amministrativa dell'ente (cd. reati-presupposto) sono esclusivamente quelli indicati nel D. Lgs. 231/2001 e successive modifiche ed integrazioni, che hanno via via allargato la portata dell'impianto originario della norma, con l'inserimento di nuove tipologie di reato-presupposto.

Inizialmente, i reati-presupposto (della responsabilità amministrativa dell'ente) previsti dal D. Lgs. 231/2001 erano esclusivamente i seguenti:

- **art. 24:** indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico;



- **art. 25:** concussione e corruzione (ora: Concussione, induzione indebita a dare o promettere utilità e corruzione) come modificato dalla L. 190/2012 e traffico di influenze illecite.

Successivamente sono state incluse, aggiornate e modificate, nel novero dei reati-presupposto, le seguenti ulteriori fattispecie:

- **art. 24 bis:** delitti informatici e trattamento illecito di dati (introdotto dalla L. 48/2008 e modificato dai D.Lgs. n. 7 e 8/2016);
- **art. 24 ter:** delitti di criminalità organizzata (aggiunto dalla L. n. 94/2009 e modificato dalla L. 69/2015);
- **art. 25 bis:** falsità in monete, in carte di pubblico credito, in valori di bollo ed in strumenti o segni di riconoscimento (introdotto dal D.L. 350/2001, convertito nella L. 409/2001 e modificato dapprima dalla L. n. 99/2009 ed in seguito dal D.Lgs. 125/2016);
- **art. 25 bis.1:** delitti contro l'industria e il commercio (introdotto dalla L. 99/2009);
- **art. 25 ter:** reati societari (aggiunto dal D.Lgs. n. 61/2002 come modificato in seguito dalla L. n. 190/2012, dalla L. 69/2015 e dal D.Lgs. 38/2017);
- **art. 25 quater:** delitti con finalità di terrorismo o di eversione dell'ordine democratico (introdotto dalla L. 7/2003);
- **art. 25 quater.1:** pratiche di mutilazione degli organi genitali femminili (introdotto dalla L. 7/2006);
- **art. 25 quinquies:** delitti contro la personalità individuale (aggiunto dalla L. 228/2003 e modificato dalla L. n. 199/2016);
- **art. 25 sexies:** abusi di mercato (introdotto dalla L. 62/2005);
- **art. 25 septies:** omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza del lavoro (introdotto dalla L. 123/2007 e modificato dal D.Lgs. 81/2008);
- **art. 25 octies:** ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (aggiunto dal D.Lgs. 231/2007 ed ampliato dalla L. n. 186/2014);
- **art. 25 novies:** delitti in materia di violazione del diritto d'autore (introdotto dalla L. 99/2009);
- **art. 25 decies:** induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (introdotto dalla L. 116/2009);
- **art. 25-undecies:** reati ambientali (aggiunto dal D.Lgs. 121/2011 e modificato dalla L. 68/2015);
- **art. 25 duodecies:** Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (introdotto dal D.Lgs. 109/2012 e modificato dalla L. 161/2017);
- **art. 25-terdecies:** razzismo e xenofobia (aggiunto dalla L. 167/2017);
- **reati transnazionali** (ex art. 10 L. 146/2006)<sup>1</sup>;
- Con Legge 09/01/2019 è stato modificato l'art. 25 del Decreto, con l'inserimento del delitto di traffico di influenze illecite di cui all'art. 346 - bis.

Il sistema sanzionatorio stabilito dal Decreto, applicabile all'ente, prevede:

### 1. Sanzione pecuniaria

La sanzione pecuniaria:

<sup>1</sup> La Legge 146 del 2006, di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea Generale il 15 novembre 2000 e il 31 maggio 2001, definisce all'art. 3 quale Reato Transazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

- a) sia commesso in più di uno Stato;
- b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in altro Stato;
- c) ovvero sia commesso in uno Stato, ma in esso sia implicate un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.



– viene applicata dal Giudice “per quote” in un numero non inferiore a cento né superiore a mille (tenendo conto della gravità del fatto, del grado di responsabilità dell'ente, nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto illecito);

– l'importo di ogni singola quota è stabilita dal Decreto (art. 10, comma 3) da un minimo di € 258,23 ad un massimo di € 1.549,37, a seconda delle condizioni economiche e patrimoniali della società, allo scopo di assicurare l'efficacia della sanzione (art. 11, comma 2, del Decreto).

## 2. Sanzioni interdittive

Le sanzioni interdittive previste dal Decreto sono:

- a) interdizione dall'esercizio dell'attività;
- b) sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- c) divieto di contrattare con la PA, salvo che per ottenere le prestazioni di un pubblico servizio;
- d) esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- e) divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito commesso dall'Ente e il Giudice ne determina il tipo e la durata tenendo conto dell'idoneità delle singole sanzioni a prevenire gli illeciti del tipo di quello commesso. Se necessario, le sanzioni interdittive possono essere applicate congiuntamente. Le sanzioni interdittive possono essere determinate in via temporanea e, nei casi previsti dall'art. 16, possono essere applicate anche in via definitiva. Le sanzioni interdittive, infine, possono essere applicate anche in via cautelare.

## 3. Confisca

Il Decreto prevede che, con la sentenza di condanna, sia sempre disposta nei confronti dell'ente la confisca del prezzo o del profitto del reato – salvo che per la parte che può essere restituita al danneggiato e salvi i diritti acquisiti dai terzi in buona fede. La confisca può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

## 4. Pubblicazione della sentenza

La pubblicazione della sentenza di condanna può essere disposta quando nei confronti dell'ente viene applicata una sanzione interdittiva.

### 1.1 L'adozione del “Modello di Organizzazione e di Gestione” quale possibile esimente della responsabilità Amministrativa.

Il Decreto prevede espressamente, agli artt. 6 e 7, l'esenzione dalla responsabilità amministrativa qualora l'ente dimostri di essersi dotato e di aver efficacemente attuato, prima della commissione del fatto costituente reato, effettivi ed efficaci modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi. L'adeguata organizzazione rappresenta pertanto il solo strumento in grado di escludere la “colpa organizzativa” dell'ente e, conseguentemente, di evitare o quanto meno attenuare l'applicazione delle sanzioni a carico dello stesso.

Segnatamente, se il reato è stato commesso da soggetti in posizione apicale, l'ente non risponde (art. 6, comma 1, del Decreto) se prova che:

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



Se invece il reato è stato commesso da soggetti sottoposti alla direzione o alla vigilanza dei soggetti apicali, l'Ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza da parte degli organi dirigenti (art. 7 del Decreto).

**L'adozione e l'efficace attuazione del Modello costituisce**, dunque, la misura della diligenza definita dal legislatore e ha una doppia valenza:

- **scriminante**, se è adottato ed efficacemente attuato prima della commissione del fatto costituente reato;
- **attenuante**, nel caso in cui sia adottato – nel corso di un procedimento giudiziario conseguente alla commissione di un reato-presupposto - prima della dichiarazione di apertura del dibattimento di primo grado, garantendo così una riduzione da un terzo alla metà della pena pecuniaria e l'esenzione dalle sanzioni interdittive.

La mera adozione del Modello da parte dell'organo dirigente non appare dunque misura sufficiente a determinare l'esonero da responsabilità dell'ente, essendo necessario che il modello sia anche efficace ed effettivo (artt. 6 e 7 del Decreto).

Quanto all'**efficacia** del Modello, il legislatore (artt. 6 e 7) prevede che il Modello deve rispondere alle seguenti esigenze:

- a) individuare le attività nel cui ambito possono essere commessi reati (cosiddetta "mappatura" delle attività/processi a rischio);
- b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
- c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- d) definire misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio;
- e) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli.

In merito a quest'ultimo requisito, la Legge 179/2017 ha introdotto, in analogia ai modelli e sistemi anticorruzione, la necessità di definire forme e strumenti di segnalazione idonei a garantire la riservatezza del segnalante, con divieto di atti ritorsivi o discriminatori a carico del segnalante (c.d. whistleblowing).

La caratteristica dell'effettività del Modello è invece legata alla sua efficace attuazione che, a norma dell'art. 7, comma 4, richiede:

- f) una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività (aggiornamento del modello);
- g) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.



## Capitolo 2

### Il sistema dei Controlli Interni e le affinità con il D. Lgs. n. 231/01

Il Decreto legislativo n. 231/01 si è innestato, nell'ambito del settore finanziario, su un terreno particolarmente sensibile alle tematiche ivi affrontate, da un lato per la particolare strutturazione delle banche e degli Intermediari Finanziari, dall'altro per l'evoluzione che la normativa relativa a questo settore ha avuto negli ultimi anni, con particolare riferimento al sistema dei controlli interni.

Negli ultimi anni le Autorità di Vigilanza hanno posto una crescente attenzione alle modalità con le quali gli Intermediari Finanziari organizzano i processi produttivi, amministrativi e distributivi, in quanto l'evoluzione tecnologica e l'accentuata dinamica competitività stanno accrescendo la complessità delle gestioni aziendali.

L'operatività degli Intermediari in mercati integrati e l'ampliamento della gamma dei prodotti e dei servizi offerti alla clientela stanno aumentando le difficoltà di rilevare e governare l'intera classe dei rischi incidenti.

La Vigilanza ha richiesto agli Intermediari Finanziari di dotarsi di sistemi di individuazione, misurazione e monitoraggio dei rischi finanziari ed operativi che consentano loro il governo consapevole della complessità aziendale nell'ottica di una sana e prudente gestione.

La Banca d'Italia, nell'emanare le Istruzioni di Vigilanza, ha ripreso i principi generali concordati a livello internazionale che si muovono secondo tre direttrici:

- Autonomia dell'impresa nella scelta del modello organizzativo;
- Ruoli e responsabilità degli Amministratori e della Direzione nella definizione delle strategie, delle politiche di gestione dei rischi, degli assetti organizzativi e delle procedure di controllo.

La disciplina evidenzia il compito del Collegio Sindacale, che è chiamato a valutare il regolare funzionamento delle principali aree organizzative nonché l'efficacia del Sistema dei Controlli Interni.

Pertanto un efficiente governo dei rischi costituisce l'elemento centrale dell'assetto organizzativo e deve accompagnarsi al necessario rafforzamento della cultura e della politica dei controlli.

Tale opportunità potrà comunque realizzarsi a condizione che gli Organi di Vigilanza accertino la sussistenza di rigorosi standard qualitativi dei processi aziendali deputati alla gestione e al controllo dei rischi.

In esecuzione a quanto prescritto dalle Istruzioni di Vigilanza di Banca d'Italia, il Gruppo Banca Finanziaria Internazionale – e con esso quindi anche la Società - si è dotato di un Sistema dei Controlli Interni (SCI) costituito dall'insieme di regole, procedure e strutture organizzative volte a consentire, attraverso un adeguato processo di identificazione, misurazione, gestione e monitoraggio dei rischi aziendali, una conduzione del Gruppo corretta e coerente con gli obiettivi prefissati di performance, miglioramento, salvaguardia, informazione e conformità.

All'interno della Società è infatti operativo un insieme di regole, di procedure e di strutture organizzative che mirano ad assicurare:

- il rispetto delle strategie aziendali e il conseguimento della efficacia e dell'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 con la legge, con la normativa di vigilanza nonché con le politiche, i piani, i regolamenti e le procedure interne.

Per ottenere quanto sopra, l'azienda deve:



- separare nettamente le funzioni operative e quelle di controllo, prevedendo anzi la presenza (e la collaborazione) di differenti soggetti “controllori”, con competenze e ambiti di attività differenti secondo quanto detto sopra;
- evitare situazioni di conflitto di interesse e di conflitti di attribuzione nell’assegnazione delle competenze, definendo sempre in maniera chiara le missioni delle diverse unità organizzative e le correlate aree di competenza;
- essere in grado di identificare, misurare e monitorare adeguatamente tutti i rischi assunti o assumibili nei diversi segmenti operativi, adottando nel contempo sistemi di reportistica e controllo (ad ogni livello operativo) in grado di portare gli eventi rischiosi o dannosi a conoscenza dei livelli gerarchici competenti;
- disporre di sistemi informativi affidabili e idonei a riferire tempestivamente anomalie riscontrate nell’attività di controllo;
- registrare ogni fatto di gestione con adeguato grado di dettaglio.

I sistemi di controllo, peraltro, oltre al corretto governo dell’azienda, sono chiamati a perseguire una serie di obiettivi anche “tecnicamente” esterni ad essi, quali:

- la protezione e la tutela della clientela;
- il corretto funzionamento dei mercati specifici di operatività, anche in termini di accesso ad informazioni riservate, uso e diffusione delle stesse;
- la prevenzione di specifici reati (ad esempio, il riciclaggio di denaro).

E’ evidente che una simile rete di controlli e verifiche, insieme alla procedura delle attività e dei processi decisionali, costituisce un sistema in grado di per sé di essere utilizzato anche per prevenire la commissione di reati, ivi compresi quelli di cui al Decreto. È immediato notare, infatti, che condotte che attentino ai principi sopra richiamati possano facilmente sfociare in fattispecie rilevanti anche ai sensi del Decreto. Una attenta predisposizione di sistemi di rilevazione e controllo costituisce infatti efficace presidio contro alcuni dei reati di cui all’art. 25 ter del Decreto, così come le norme che regolano la circolazione delle informazioni all’interno della struttura aziendale concorrono alla prevenzione di altri reati di cui allo stesso art. 25 ter, quali l’aggiotaggio (art. 2637 c.c.) e l’ostacolo all’esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, commi 1 e 2, c.c.).

L’approccio imposto dal Decreto, che non ha dettato alle società norme comportamentali immediatamente e direttamente applicabili, bensì ha indicato alle stesse società un obiettivo da raggiungersi mediante una autonoma riflessione sulla propria struttura organizzativa, tale da sfociare nella emanazione di norme interne attagliate alla singola realtà, è un approccio già noto alle realtà bancarie e finanziarie, le quali già da tempo si confrontano con temi di autoregolamentazione.

Lo sviluppo di un sistema di controlli interni ha come punto di partenza l’analisi della Società e del settore all’interno del quale la stessa opera, al fine di identificare e comprendere i rischi ai quali la stessa è potenzialmente soggetta. Per lo sviluppo interno del proprio sistema di controlli, il Consiglio di Amministrazione si è avvalso principalmente delle analisi effettuate dalle funzioni di Internal Audit, di Compliance e di Risk Management, ma anche dei responsabili delle diverse funzioni aziendali nell’ambito delle riunioni dedicate allo sviluppo del modello.

Alla base del sistema dei controlli interni vi è l’individuazione dei principali processi che regolano la *core business* dell’azienda, al fine di identificarne i potenziali rischi ed i relativi presidi. Fin dai primi anni della propria attività, la Società ha attribuito forte rilevanza alla gestione ed al controllo del rischio e tale mentalità trova riscontro in un modello aziendale che prevede:

- la chiara individuazione delle responsabilità nella loro assunzione;
- la separatezza tra le unità organizzative deputate alla gestione e le funzioni addette al controllo;
- una mappatura completa e approfondita delle procedure e dei rischi aziendali, dalla quale emergono chiaramente ruoli e responsabilità per ogni singola fase dei processi decisionali/operativi;
- un Regolamento Interno che approfondisce ed illustra le linee guida, stabilendo dei vincoli condivisi e rivisti periodicamente per le fasi più critiche di ogni processo.



La Società, in coerenza con le indicazioni degli Organi di Vigilanza, ha individuato le seguenti quattro macro tipologie di controllo:

- **controlli di linea**, diretti ad assicurare il corretto svolgimento dell'operatività quotidiana e delle singole transazioni. Di norma tali controlli sono effettuati dalle strutture produttive o incorporati nelle procedure informatiche;
- **controlli sulla gestione dei rischi**, che hanno l'obiettivo di concorrere alla definizione delle metodologie di misurazione del rischio, di verificare il rispetto dei limiti assegnati alle varie funzioni operative e di controllare la coerenza dell'operatività delle singole strutture produttive con gli obiettivi di rischio-rendimento assegnati. Essi sono di norma affidati a strutture diverse da quelle produttive;
- **controlli di conformità**, costituiti da politiche e procedure in grado di individuare, valutare, controllare e gestire il rischio conseguente al mancato rispetto di leggi, provvedimenti delle autorità di vigilanza e norme di autoregolamentazione, nonché di qualsiasi altra norma applicabile alla Società;
- **revisione interna**, volta ad individuare andamenti anomali, violazioni delle procedure e della regolamentazione, nonché a valutare la funzionalità del complessivo sistema dei controlli interni. Essa è condotta da strutture diverse ed indipendenti rispetto a quelle produttive.

La Società ha già elaborato e approvato i Regolamenti sui principali processi aziendali che disciplinano e definiscono i ruoli, i doveri, le responsabilità e i controlli di organi e strutture aziendali. I Regolamenti sono eventualmente completati da comunicazioni interne che regolamentano nel dettaglio le singole attività significative.

Alla luce delle considerazioni sopra esposte, tenuto conto anche del lavoro già in parte svolto con il Sistema dei Controlli Interni, il Modello qui descritto rappresenta un passo necessario per completare un programma di protezione e controllo aziendale già da tempo avviato, che consente alla Società di essere riconosciuta nel mercato come un'impresa responsabile, trasparente e soprattutto affidabile.

La cultura del controllo assume una posizione di rilievo nella scala dei valori del Gruppo e, di conseguenza, non riguarda solo le Funzioni Aziendali di Controllo, ma coinvolge tutta l'organizzazione nella definizione, applicazione ed evoluzione di meccanismi, metodologie e strumenti in grado di identificare, misurare/valutare, gestire/mitigare i rischi, secondo i criteri di:

- proporzionalità, intesa come applicazione del quadro normativo in funzione della natura dell'attività svolta, della tipologia dei servizi prestati, della complessità operativa e delle caratteristiche dimensionali delle Società del Gruppo;
- integrazione, intesa come ricerca di meccanismi di coordinamento e armonizzazione tra i diversi attori dello SCI con utilizzo di metodologie che consentano di fornire informazioni complete, fruibili, e frutto di un processo integrato di valutazione che consentano di pervenire ad una visione unitaria per l'assunzione consapevole delle decisioni;
- economicità, intesa come ricerca di un adeguato trade off tra costo complessivo del controllo e corretto presidio dei rischi;
- evoluzione, intesa come ricerca nel continuo di meccanismi finalizzati al miglioramento dell'assetto del Sistema dei Controlli Interni e della sua efficacia ed efficienza.

I profili strutturali del complessivo Sistema dei Controlli Interni del Gruppo Banca Finanziaria Internazionale, concernenti il modello dei controlli adottato, i meccanismi di raccordo e coordinamento delle funzioni componenti lo SCI, i principi e le linee guida ai quali lo stesso si ispira, i ruoli e responsabilità, i flussi informativi tra i soggetti coinvolti sono contenuti in uno specifico documento denominato "Sistema dei Controlli Interni Integrato" approvato dall'Organo con Funzione di Supervisione Strategica della Capogruppo e recepito dai rispettivi organi delle Controllate. In coerenza con quanto previsto dal Sistema dei Controlli Interni Integrato, ciascuna Controllata si dota di un Sistema dei Controlli Interni che sia coerente con le strategie e le politiche del Gruppo in materia di controlli, fermo restando il rispetto della disciplina eventualmente applicabile su base individuale. Le Controllate hanno piena responsabilità del governo della propria realtà e, ferme restando le esigenze di Gruppo, adottano autonomamente le misure rispondenti a



specifiche esigenze di presidio dei rischi, sottoponendo le stesse al preventivo esame della Capogruppo per consentire a quest'ultima di svolgere al meglio il proprio ruolo di direzione e coordinamento del Gruppo.



## Capitolo 3

### Adozione del modello da parte della Società

#### 3.1 Obiettivi perseguiti con l'adozione del Modello

La decisione della Società di adottare il Modello, accompagnata dall'emanazione di uno specifico Codice Etico, è stata assunta in primo luogo nella convinzione che il Modello possa costituire un valido strumento di sensibilizzazione nei confronti di tutti coloro che operano in nome e per conto della Società, affinché seguano, nell'espletamento delle proprie attività, dei comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati dal Decreto.

In particolare, attraverso l'adozione ed il costante aggiornamento del Modello, la Società si propone di perseguire le seguenti principali finalità:

- determinare, in tutti coloro che operano per conto della Società nell'ambito di "attività sensibili", la consapevolezza di poter incorrere, in caso di violazione delle disposizioni impartite in materia, in conseguenze disciplinari e/o contrattuali, oltre che in sanzioni penali e amministrative irrogabili nei loro stessi confronti;
- ribadire che tali forme di comportamento illecito sono fortemente condannate, in quanto le stesse sono comunque contrarie, oltre che alle disposizioni di legge, anche ai principi etici ai quali la Società intende attenersi nell'esercizio dell'attività aziendale;
- consentire alla Società, grazie ad un'azione di monitoraggio sulle aree di rischio, di intervenire tempestivamente al fine di prevenire o contrastare la commissione dei reati stessi e sanzionare i comportamenti contrari al proprio Modello;
- costruire un sistema strutturato ed organico di procedure nonché di attività di controllo, da svolgersi anche in via preventiva (controllo *ex ante*), volto a prevenire la commissione delle diverse tipologie di reato contemplate dal Decreto.

Inoltre, considerato il notevole impatto negativo che potrebbe avere un coinvolgimento, seppur inconsapevole, della Società in reati rilevanti ai fini 231/01, con l'adozione del Modello la Securitisation Services S.p.A. si propone anche l'obiettivo di tutelare la reputazione aziendale.

Pertanto punti cardine del Modello sono, oltre ai principi già indicati:

- l'attività di sensibilizzazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- la mappa delle Aree a Rischio dell'azienda, vale a dire delle attività nel cui ambito si ritiene più alta la possibilità che siano commessi i reati;
- la prevenzione del rischio, attraverso l'adozione di principi procedurali dotati di specificità e volti a programmare la formazione e l'attuazione delle decisioni della Società in relazione ai reati da prevenire;
- la verifica e documentazione delle operazioni a rischio;
- l'individuazione, anche attraverso il richiamo a procedure aziendali adottate dalla Società, di modalità di gestione delle risorse finanziarie che consentano la tracciabilità di ogni singola operazione;
- il rispetto del principio della separazione delle funzioni;
- la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
- la verifica dei comportamenti aziendali, nonché del funzionamento del Modello con conseguente aggiornamento periodico (controllo *ex post*);
- l'adozione di un sistema disciplinare specifico ed idoneo a perseguire e sanzionare l'inosservanza delle misure organizzative adottate;
- l'attribuzione all'OdV di specifici compiti di vigilanza sull'efficace e corretto funzionamento del Modello.



### 3.3 Struttura del Modello: Parte Generale e Parti Speciali in funzione delle diverse ipotesi di reato

Il presente Modello è composto da:

1. una “**Parte Generale**” che illustra la struttura del Modello adottato da Securitisation Services S.p.A. ai sensi del Decreto Legislativo 231/01;
2. una “**Parte Speciale**” che illustra le diverse tipologie di reato contemplate nel Decreto, individua le aree di rischio ed i principi di comportamento per la prevenzione dei singoli reati.

Costituisce altresì parte integrante del modello il Codice Etico.

Nella redazione del Modello si è tenuto conto che la Securitisation Services S.p.A. volontariamente intende porre particolare attenzione ai rapporti da instaurarsi, in particolare con i propri clienti e fornitori, ferma restando la natura e l'attività svolta dalla Società e nella convinzione, già sopra espressa, che l'adozione del Modello, sebbene facoltativa e non obbligatoria ai sensi del Decreto, possa costituire un valido strumento di sensibilizzazione di tutti coloro che operano in nome e per conto della stessa a tenere condotte conformi alla normativa vigente, nonché in un'ottica di perseguimento della *best practice* nello svolgimento dell'attività aziendale.

### 3.4 Adozione del Modello

In conformità alle prescrizioni dell'articolo 6 del Decreto per il quale il Modello è un “...atto di emanazione dell'organo dirigente...”, il Consiglio di Amministrazione in data odierna ha approvato la presente revisione del “Modello di organizzazione, Gestione e Controllo ex D. Lgs. 231/2001”. Il Modello sarà oggetto di aggiornamento, qualora necessario, e sottoposto all'approvazione del Consiglio di Amministrazione.

Eventuali modifiche o integrazioni di carattere formale del Modello Organizzativo potranno essere apportate dal Consiglio di Amministrazione, anche su proposta dell'Organismo di Vigilanza. La Società comunicherà tempestivamente a tutto il personale ogni modifica apportata al Modello.

### 3.5 Modalità di attuazione del Modello e principi comuni

Per la realizzazione di un Modello efficace ed efficiente e pertanto idoneo a prevenire la realizzazione dei reati di cui al Decreto, è fondamentale che la Società indichi le azioni da intraprendere per migliorare il Sistema dei Controlli Interni esistente, alla luce delle fattispecie di rischio di cui al Decreto.

Costituiscono principi comuni a tutti i sistemi di controllo implementati nonché del presente modello 231/01:

- **regolamentazione delle attività e attribuzione di poteri e responsabilità:** le diverse attività devono essere regolamentate attraverso documenti gestionali (regolamenti, procedure) che definiscano in modo chiaro ed esaustivo ruoli, responsabilità, principi di comportamento, modalità operative, di gestione e di controllo. In relazione al sistema di deleghe e procure definito, devono esistere regole formalizzate per l'esercizio di poteri di firma e poteri autorizzativi interni. In particolare, essi devono essere: coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; essere chiaramente definiti e conosciuti all'interno dell'organizzazione;
- **segregazione delle funzioni:** non dovrebbe esserci identità soggettiva tra coloro che assumono le decisioni, coloro che le attuano e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge o dalle procedure contemplate dal sistema di controllo interno;
- **tracciabilità delle informazioni e del processo decisionale:** ogni operazione deve essere adeguatamente formalizzata. Il processo di decisione e le relative fasi di autorizzazione, svolgimento e controllo delle diverse attività devono essere verificabili ex post, tramite appositi supporti informatici e/o documentali che devono essere archiviati e conservati, a cura della funzione competente, con modalità tali da non permettere la modificazione successiva, se non con apposita evidenza;
- **formazione continua:** deve essere implementato un processo di formazione continua di tutti i soggetti coinvolti; le attività formative devono essere efficaci e documentate;



- **monitoraggio, verifica e revisione:** in ottica di miglioramento gestionale e di gestione del rischio, deve essere strutturato un processo di verifica, audit, riesame e follow up delle decisioni, delle attività e connesse responsabilità; in caso di emersione di comportamenti “devianti”, deve essere predisposto, diffuso ed applicato un idoneo **sistema disciplinare**.

### 3.6 Risk assessment – metodologia adottata

Si premette che la Società non è mai stata indagata per reati di alcun genere e pertanto nemmeno per reati rilevanti 231. Inoltre, al fine di monitorare internamente i rischi cui è esposta, la Società si è dotata di un database per la raccolta di segnalazioni da parte dei dipendenti che evidenzino delle non conformità nell’operato della Società rispetto a norme di etero regolamentazione (normativa applicabile e contratti) o di autoregolamentazione.

Dall’analisi di tali segnalazioni non è mai emerso alcun coinvolgimento, neanche indiretto, della Società in fatti criminosi, né tantomeno rilevanti ai fini dell’applicazione del D.Lgs. 231/2001. Tutto ciò premesso, l’attività di risk assessment è stata necessariamente effettuata in primo luogo attraverso l’esame della documentazione aziendale rilevante (organigramma della Società, deleghe e procure, job description, ecc) e in secondo luogo tramite una serie di interviste con i responsabili di funzione/divisione, al fine di formalizzare una autovalutazione dei rischi e dei controlli in essere nella Società.

Tali interviste hanno permesso di individuare:

- le caratteristiche delle diverse aree aziendali e delle rispettive attività sensibili ai fini del Decreto;
- le procedure e i controlli attualmente presenti in azienda;
- le potenziali modalità attuative dei reati.

In particolare l’intervista ha permesso di effettuare una valutazione generale del sistema di controllo interno della Società in relazione gli aspetti del D. Lgs. 231/2001. La tabella seguente illustra il processo di risk assessment seguito durante la fase di mappatura.

Fase	Soggetti coinvolti
Analisi della documentazione della Società ed in particolare del modello già esistente	Funzioni di <i>internal audit</i> e di <i>compliance</i>
Interviste con i responsabili aziendali	Funzione di <i>internal audit</i> , di <i>compliance</i> e di <i>risk management</i>
Revisione dei rischi aziendali sensibili ai reati di cui al D.Lgs 231/2001, dei relativi presidi e dei processi aziendali connessi	Funzione di <i>internal audit</i> , di <i>compliance</i> e di <i>risk management</i>
Aggiornamento del modello	Funzioni di <i>affari societari</i> con il supporto di <i>internal audit</i> e di <i>compliance</i>

La valutazione dei rischi e dei presidi è avvenuta su base soggettiva da parte dei responsabili aziendali. A tale proposito si evidenzia come le metodologie di misurazione si basano prevalentemente sull’analisi dei dati storici della Società (ove disponibili) e sull’esperienza dei Responsabili di Funzione/Divisione.

Le interviste hanno avuto ad oggetto una preliminare descrizione delle aree di attività e la valutazione dei singoli reati 231 al fine di individuare le aree sensibili in cui possono essere commessi i reati. Successivamente sono stati valutati i presidi già in essere che riducono la possibilità di commettere reati rilevanti ai sensi del D.Lgs. 231/2001; tale analisi ha permesso di individuare:

- le caratteristiche delle diverse aree aziendali e delle rispettive attività sensibili ai fini del Decreto;



- le procedure e i controlli attualmente presenti in azienda;
- potenziali modalità attuative dei reati.

Si rende noto che la Società effettua annualmente anche una valutazione dei rischi complessivi a cui è esposta, in ottemperanza alle disposizioni di vigilanza prudenziale ad essa applicabili (processo ICAAP) e che nell'ambito di tale analisi essa effettua una valutazione di tipo qualitativo (assegnazione di un giudizio qualitativo come di seguito descritto e successiva individuazione degli interventi correttivi da intraprendere) in particolare sui rischi di natura operativa a cui è soggetta.

Si informa, inoltre, che nel corso degli ultimi anni la mappatura dei rischi cui la Società è esposta è stata rivista, con il coordinamento della Funzione di *Risk Management*, al fine di:

- i. estendere la valutazione anche ai rischi di alcune importanti aree operative della Società
- ii. uniformare i criteri di valutazione utilizzati nell'analisi in modo da ridurre il più possibile l'elemento soggettivo nelle considerazioni da parte di ogni singolo *risk owner*.

A seguito di tale attività di razionalizzazione la numerosità dei rischi si è ridotta e le formulazioni dei rischi stessi è stata resa il più possibile omogenea, senza che la mappatura generale ne sia risultata sostanzialmente modificata.

Alla luce di ciò, al fine di uniformare la valutazione dei rischi cui la Società è esposta è stato deciso di adeguare le valutazioni specifiche svolte ai fini del presente Modello a quelle effettuate nell'ambito della valutazione complessiva nell'ambito della redazione del Resoconto ICAAP.

Tale attività di *Risk Assessment* mira ad individuare situazioni potenzialmente critiche e, basandosi sull'analisi dei dati storici della Società e sull'esperienza dei responsabili di funzione/divisione, stima per i singoli rischi associati a uno o più processi aziendali i seguenti elementi:

- “frequenza” degli eventi di rischio, ovvero il numero atteso di eventi di perdita nell'arco temporale di riferimento;
- “impatto” degli eventi di rischio, ovvero la quantificazione della perdita attesa per singolo evento.

La frequenza e l'impatto, così come definiti e valutati, vengono combinati in una matrice, come nell'esempio riportato di seguito. A ciascun incrocio corrisponde, quindi, uno specifico punteggio, funzionale ad esprimere il grado di rischio intrinseco stimato per la specifica anomalia.

Heatmap		Impatto				
		Basso	Medio-Basso	Medio	Medio-Alto	Alto
Frequenza	Bassa					
	Medio-Bassa					
	Media					
	Medio-Alta					
	Alta					

Successivamente si procede con l'individuazione dei relativi presidi esistenti, la valutazione della loro capacità mitigante e l'eventuale individuazione, nel caso in cui il livello di rischio residuo sia elevato, delle opportune *remediation*. La valutazione del controllo infatti consente di pervenire ad un concetto di rischio residuo, che rappresenta gli effetti prodotti dal rischio potenziale, o intrinseco, che non sono neutralizzati dall'esecuzione dei controlli.



Come detto l'indice di rischio residuo ottenuto, classificato di norma in 4 classi secondo la logica semaforica indicata in precedenza, guida il tipo di azione di gestionale che la Società decide di attuare.

Di norma per i rischi con giudizio "Alto" e "Medio Alto" viene valutata *in primis* la possibilità di migliorare l'efficacia dei presidi in essere, anche eventualmente tramite la stipula di specifiche polizze assicurative, e, quando ciò non fosse ritenuto possibile o sufficiente, vengono prese in considerazione soluzioni quali la cessazione di alcune delle attività prestate.

Indubbiamente il processo di autovalutazione dei rischi e dei presidi, essendo effettuato su base soggettiva, presenta dei limiti legati alla maggiore o minore propensione al rischio del responsabile aziendale. Ai fini della precedente analisi, tuttavia, non è possibile procedere sulla base di elementi oggettivi, come ad esempio dei *track record*, essendo stata la Società finora totalmente estranea a coinvolgimenti in indagini amministrative o penali da parte dell'autorità giudiziaria. Il coordinamento dell'attività di valutazione dei rischi da parte della Funzione di *Risk Management*, ha, *inter alia*, lo scopo di uniformare il più possibile le valutazioni, in modo da ridurre la soggettiva propensione al rischio di ciascun *risk owner*.

Sulla base di quanto osservato nel processo di mappatura delle attività sensibili e alla luce dei controlli attualmente esistenti presso la Società, sono stati individuati i principi generali di comportamento e le regole generali per l'organizzazione, lo svolgimento e il controllo delle operazioni svolte nell'ambito delle attività sensibili, nonché le procedure di prevenzione ed i criteri a cui le stesse debbono uniformarsi.

A tal fine è stato predisposto il Codice Etico della Società che risulta pubblicato sul sito web della Società stessa.

Considerato l'ampissimo novero dei reati sottoposti alla disciplina del Decreto, al continuo inserimento di nuovi reati da parte del legislatore ed alle evidenze che emergeranno nell'ambito dell'attività di svolta dall'Organo di Vigilanza appositamente istituito, il presente modello dovrà necessariamente essere sottoposto a periodiche revisioni o integrazioni.

### 3.7 Destinatari del Modello

L'intero modello è indirizzato a tutto il personale operante all'interno della Società ovvero Esponenti Aziendali e dipendenti, nonché ai Collaboratori Esterni, tra cui Consulenti, Partner e Fornitori.

In particolare, il Modello si rivolge a quanti si trovino a svolgere le attività classificate quali "attività sensibili/strumentali", ovvero a rischio di commissione dei reati. Le disposizioni contenute nel Modello devono, dunque, essere rispettate dai citati destinatari, opportunamente formati ed informati dei contenuti del Modello medesimo. A tal fine, ogni volta che la Società entra in contatto con Collaboratori Esterni, viene inserita nel documento che ne disciplina i reciproci rapporti una clausola che informi circa l'esistenza del Modello e del Codice Etico adottato dalla Società -- e che indichi l'adeguamento del Collaboratore Esterno ai principi contenuti nel Modello e nel Codice Etico necessari a prevenire i reati ipotizzati ed ivi indicati.



## Capitolo 4

### Organismo di Vigilanza

#### 4.1 Individuazione dell'Organismo di Vigilanza

##### *Composizione dell'Organo di Vigilanza*

L'art. 6 del D.Lgs. 231/2001 indica, quale condizione per l'esenzione dalla responsabilità amministrativa dell'ente, l'affidamento del compito di vigilare sul funzionamento e sull'osservanza del Modello nonché di curarne l'aggiornamento, ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

Tale organismo, con riguardo a quanto previsto dal D.Lgs.231/01, è preposto a:

- **assicurare** una costante ed indipendente **azione di sorveglianza** sul regolare andamento dell'operatività e sulla conformità dei processi della Società relativamente al dettato del D.Lgs. 231/2001 al fine di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose;
- **curare l'aggiornamento del Modello e delle regole e dei principi organizzativi** in esso contenuti o richiamati, in termini di proposta per il Consiglio di Amministrazione, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative, anche attraverso l'intervento dei competenti organi e funzioni societarie.

In ottemperanza ai requisiti di legge ed a quanto sopra definito, la Società ha individuato come soggetto idoneo ad assumere tale responsabilità un organo collegiale composto da 3 membri. Possono far parte dell'Organismo (i) dipendenti della Società o del Gruppo dotati di adeguata professionalità e indipendenza; (ii) persone esterne alla Società ed al Gruppo, dotate di riconosciuta esperienza in campo legale, contabile, di auditing, consulenziale, purché nel loro insieme garantiscano al medesimo organo carattere di autonomia, indipendenza e continuità d'azione.

Ai sensi dell'art. 6, comma 4 *bis* del Decreto, il Collegio Sindacale può svolgere anche le funzioni dell'Organismo di Vigilanza (OdV); la Società ha optato per incaricare il Collegio Sindacale per le funzioni di OdV.

A tal riguardo si precisa che:

- l'**autonomia** va intesa in senso non meramente formale: è necessario cioè che l'OdV sia dotato di effettivi poteri di ispezione e controllo, che abbia possibilità di accesso alle informazioni aziendali rilevanti, che sia dotato di risorse adeguate e possa avvalersi di strumentazioni, supporti ed esperti nell'espletamento della sua attività di monitoraggio;
- quanto al requisito dell'**indipendenza**, i componenti dell'Organismo di Vigilanza non devono trovarsi in una posizione, neppure potenziale, di conflitto di interessi con la Società né essere titolari all'interno della stessa di funzioni di tipo esecutivo; in caso di soggetti interni alla struttura aziendale, essi devono altresì godere di una posizione organizzativa adeguatamente elevata ed indipendente dalle strutture operative;
- infine, con riferimento al requisito della **professionalità**, è necessario che all'interno dell'OdV siano presenti soggetti con professionalità adeguate in materia di controllo e gestione dei rischi aziendali. L'OdV potrà, inoltre, anche avvalendosi di professionisti esterni, dotarsi di risorse competenti in materia di organizzazione aziendale, revisione, contabilità e finanza.

L'Assemblea dei Soci della Società ha provveduto ad affidare al Collegio Sindacale le funzioni di Organismo di Vigilanza ex D.Lgs 231/2001 (OdV).



L'Organismo di Vigilanza si riunisce con periodicità almeno trimestrale in base ad un approccio basato sul rischio e come di volta in volta concordato dai membri nominati. È possibile la partecipazione di uno o più membri in audio conferenza.

#### *Cessazione, decadenza e revoca dei membri dell'Organo di Vigilanza*

L'Organismo di Vigilanza e i suoi componenti rimangono in carica, fatti salvi i casi di cessazione, revoca e decadenza di seguito illustrati, per tre esercizi dalla data dell'Assemblea convocata per l'approvazione del bilancio relativo all'ultimo esercizio della sua carica.

1. La **cessazione** dell'incarico dell'Organismo di Vigilanza o dei suoi componenti può avvenire per una delle seguenti ipotesi:
  - scadenza dell'incarico;
  - revoca da parte del Consiglio di Amministrazione;
  - rinuncia di ciascun componente dell'Organismo di Vigilanza, formalizzata mediante apposita comunicazione scritta, inviata al Consiglio di Amministrazione;
  - sopraggiungimento di una delle cause di ineleggibilità e/o di decadenza del componente dell'Organismo di Vigilanza, di seguito elencate.
2. La **revoca** dell'Organismo di Vigilanza o dei suoi componenti può essere disposta solo per giusta causa e tali devono intendersi, a titolo esemplificativo, le seguenti ipotesi:
  - il caso in cui il componente sia coinvolto in un processo penale avente ad oggetto la commissione di un reato;
  - una grave negligenza nell'espletamento dei compiti connessi all'incarico;
  - il possibile coinvolgimento della Società in un procedimento, penale o civile, che sia connesso ad un'omessa o insufficiente vigilanza, anche colposa;
  - la violazione da parte del componente degli obblighi di riservatezza;

La revoca è disposta con delibera del Consiglio di Amministrazione, previo parere non vincolante del Collegio Sindacale, qualora allo stesso non siano già attribuite le funzioni di OdV.

3. Costituiscono cause di **ineleggibilità e/o di decadenza** del componente dell'Organismo di Vigilanza:
  - l'interdizione, l'inabilitazione, la dichiarazione di fallito o, comunque, la condanna penale, anche non passata in giudicato, per uno dei reati previsti dal Decreto o, comunque, ad una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici o l'incapacità di esercitare uffici direttivi;
  - l'esistenza di relazioni di parentela, coniugio o affinità entro il quarto grado con i membri del Consiglio di Amministrazione o del Collegio Sindacale della Società (salva l'ipotesi in cui allo stesso non siano già attribuite le funzioni di OdV), o con i soggetti esterni incaricati della revisione (a livello manageriale);
  - l'esistenza di rapporti di natura patrimoniale tra il componente e la Società tali da compromettere l'indipendenza del componente stesso.

Qualora, nel corso dell'incarico, dovesse sopraggiungere una causa di ineleggibilità/decadenza, il componente dell'Organismo di Vigilanza è tenuto ad informare immediatamente il Consiglio di Amministrazione affinché, nella prima riunione utile, proceda alla dichiarazione di decadenza dell'interessato dalla carica di componente dell'Organismo di Vigilanza ed alla sua sostituzione.

In caso di cessazione, revoca o rinuncia, il Consiglio di Amministrazione nomina senza indugio il nuovo componente dell'Organismo di Vigilanza, mentre il componente uscente rimane in carica fino alla sua sostituzione.

#### *Autonomia di spesa dell'Organo di Vigilanza e obbligo di rendiconto*



L'Organismo di Vigilanza ha un potere di spesa adeguato a consentirne l'appropriata operatività. Tale potere di spesa dovrà essere impiegato esclusivamente per esborsi che questo dovrà sostenere nell'esercizio delle sue funzioni quali, a titolo esemplificativo, assistenza consulenziale, spese di funzionamento e di aggiornamento. L'autonomia di spesa risponde all'esigenza di ottemperare alle disposizioni normative in materia di obblighi dell'OdV di individuare le modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati.

Il budget di spesa deve essere approvato con apposita delibera del Consiglio di Amministrazione sulla base di una stima effettuata dall'Organismo di Vigilanza stesso.

L'Organismo di Vigilanza relaziona con cadenza almeno annuale al Consiglio di Amministrazione in merito all'utilizzo del budget assegnato.

#### 4.2 Funzioni e poteri dell'Organismo di Vigilanza

All'OdV è affidato sul piano generale il compito di vigilare:

- sull'osservanza delle prescrizioni del Modello da parte dei Destinatari, in relazione alle diverse tipologie di reato contemplate dal Decreto;
- sulla reale efficacia ed effettiva capacità del Modello, in relazione alla struttura aziendale, di prevenire la commissione dei reati di cui al Decreto;
- sull'opportunità di aggiornamento del Modello, in relazione alle mutate condizioni aziendali e alle novità legislative e regolamentari.

Su di un piano più operativo è affidato all'OdV il compito di:

- Attivare le procedure di controllo, tenendo presente che una responsabilità primaria sul controllo delle attività, anche per quelle relative alle Aree a Rischio, resta comunque demandata al management operativo e forma parte integrante dei processi aziendali ("controlli di linea"); il che conferma l'importanza di un processo formativo del personale.
- Condurre ricognizioni dell'attività aziendale ai fini della mappatura aggiornata delle Aree a rischio ed effettuare verifiche mirate su determinate operazioni o atti posti in essere nell'ambito delle Aree a Rischio.
- Promuovere idonee iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione organizzativa contenente le istruzioni, chiarimenti o aggiornamenti per il funzionamento del Modello stesso.
- Raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione richiesta in conformità a quanto previsto nelle singole Parti Speciali del Modello per le diverse tipologie di reati. Inoltre, aggiornare la lista di informazioni che devono essere allo stesso OdV obbligatoriamente trasmesse o tenute a sua.
- Coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il migliore monitoraggio delle attività nelle Aree a Rischio. A tal fine, l'OdV viene tenuto costantemente informato sull'evoluzione delle attività nelle Aree a Rischio ed ha libero accesso a tutta la documentazione aziendale rilevante, compresi i relativi dati di aggiornamento. All'OdV devono essere inoltre segnalate da parte del management eventuali situazioni dell'attività aziendale che possano esporre l'azienda al rischio di reato.
- Condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello.
- Verificare che gli elementi previsti dalle singole Parti Speciali del Modello per le diverse tipologie di reati (adozione di clausole standard, espletamento di procedure, ecc.) siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, ad un aggiornamento degli elementi stessi.
- Coordinarsi con i Responsabili delle diverse Funzioni aziendali per i diversi aspetti attinenti all'attuazione del Modello (definizione delle clausole standard, formazione del personale, provvedimenti disciplinari, ecc.).



### 4.3 L'operatività dell'Organismo di Vigilanza all'interno della Società

L'Organismo di Vigilanza per le sue verifiche si avvale delle strutture dell'azienda (e, in tale ambito, in particolare delle Funzioni di Internal Audit e di Compliance, le quali operano nel rispetto di quanto previsto dai Regolamenti). L'Organismo di Vigilanza effettua le proprie valutazioni in piena autonomia e può richiedere autonomamente qualunque informazione che ritenga necessaria per l'espletamento del proprio ruolo.

Ai fini della rispondenza a quanto prescritto dal Decreto, l'Organismo di Vigilanza richiede alle funzioni di *Internal Audit* e di *Compliance* di inserire nei propri piani delle verifiche controlli specifici volti, in particolare per le aree sensibili, a valutare l'adeguatezza delle procedure operative e di controllo al fine di prevenire comportamenti illeciti, ferma restando la possibilità di richiedere, sempre da parte dell'Organismo di Vigilanza, qualora ravvisi esigenze di carattere di urgenza, interventi straordinari. Si intende che le modifiche del piano di audit 231, in seguito alle verifiche straordinarie disposte, incidono prioritariamente sulla pianificazione degli interventi di verifica nel medesimo ambito.

L'Organismo di Vigilanza porta periodicamente a conoscenza del Consiglio di Amministrazione e del Collegio Sindacale - qualora ad esso non siano affidate anche le funzioni di OdV - le valutazioni sul Sistema dei Controlli Interni che derivano dagli accertamenti richiesti ai fini del D.Lgs.231/2001.

### 4.4 L'attività di reporting dell'Organismo di Vigilanza verso altri organi aziendali

L'Organismo di Vigilanza relaziona, su base annuale ovvero ogni qual volta sia necessario, al Consiglio di Amministrazione della Società. L'Organismo di Vigilanza:

- predispone con cadenza almeno annuale, e ogni qual volta risulti necessario, una relazione descrittiva per il Consiglio di Amministrazione contenente, in particolare, una sintesi di tutte le attività svolte, dei controlli e delle verifiche eseguite, nonché l'eventuale aggiornamento del Modello e gli altri temi di maggior rilevanza. Nella relazione annuale l'Organismo di Vigilanza predispone altresì un piano, su base annua, delle attività previste per l'esercizio successivo e prende visione, per gli ambiti di competenza, del piano annuale delle verifiche delle funzioni di Internal Audit e di Compliance.

L'attività di *reporting* ha in ogni caso sempre ad oggetto:

- l'attività svolta dall'Organismo di Vigilanza;
- le eventuali criticità emerse sia in termini di comportamenti o eventi interni alla Società sia in termini di efficacia del Modello.

Il Consiglio di Amministrazione e il Collegio Sindacale – qualora ad esso non siano attribuite le funzioni di Organismo di Vigilanza - hanno la facoltà di convocare in qualsiasi momento l'Organismo di Vigilanza il quale, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

Gli incontri con gli organi cui l'Organismo di Vigilanza riferisce devono essere verbalizzati e copie dei verbali devono essere custodite dall'Organismo di Vigilanza o dagli organismi di volta in volta coinvolti.

Nell'adempimento delle proprie funzioni, l'Organismo accede o delega, per proprio conto, l'accesso, a tutte le attività svolte dalla Società ed alla relativa documentazione.

In caso di attribuzione a soggetti terzi di attività rilevanti, o potenzialmente rilevanti, per il funzionamento del Sistema dei Controlli Interni ai fini del D.Lgs.231/2001, l'Organismo di Vigilanza deve poter accedere anche alle attività svolte da tali soggetti.

### 4.5 Flussi informativi

Come già ricordato, è stabilito che l'Organismo di Vigilanza riferisca almeno annualmente al Consiglio di Amministrazione circa l'attività svolta e l'adeguatezza del Modello organizzativo adottato.

Vengono, di seguito, definiti i flussi informativi interni attraverso i quali i dipendenti sono in grado di riferire direttamente all'Organismo di Vigilanza sui comportamenti illeciti eventualmente riscontrati.



Chiunque venga a conoscenza di situazioni illegali o eticamente scorrette ovvero di situazioni che potrebbero essere anche solo potenzialmente foriere di attività illegali o scorrette, deve informare tempestivamente, preferibilmente per iscritto, l'Organismo di Vigilanza. L'Organismo di Vigilanza stabilisce, caso per caso, la documentazione che deve essere sottoposta alla sua attenzione, anche con riferimento ad un semplice visto di conformità.

L'Organismo di Vigilanza stabilisce altresì le modalità con cui le informazioni e le notizie relative all'attuazione del Modello devono essere fatte pervenire all'Organo stesso, predisponendo, laddove necessario, anche appositi "canali informativi". Le segnalazioni potranno, ad esempio, essere indirizzate ad una casella di posta elettronica il cui accesso sarà consentito solo ed esclusivamente ai membri dell'Organismo di Vigilanza.

Come detto, dovranno essere portate a conoscenza dell'Organismo di Vigilanza tutte le informazioni, di qualsiasi tipo, provenienti anche da terzi e attinenti all'attuazione del Modello nelle aree di attività a rischio che potrebbero ingenerare responsabilità della Società ai sensi del D.Lgs. n. 231/01. Valgono al riguardo le seguenti prescrizioni di carattere generale:

- devono essere raccolte eventuali segnalazioni relative alla commissione di reati, o al ragionevole pericolo di commissione dei reati, previsti dal Decreto in relazione all'attività della Società o comunque comportamenti non in linea con le regole di condotta adottate dalla Società stessa;
- l'afflusso di segnalazioni, incluse quelle di natura officiosa, deve essere canalizzato verso l'Organismo di Vigilanza;
- l'Organismo di Vigilanza valuterà le segnalazioni ricevute e 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 a una indagine interna;
- l'Organismo di Vigilanza agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente o in mala fede.

Le **segnalazioni** o eventuali richieste fatte dai Dipendenti o da terzi possono essere rivolte direttamente all'Organismo di Vigilanza a mano, mediante consegna di busta chiusa indirizzata a:

Organismo di Vigilanza di Securitisation Services S.p.A. – Via Vittorio Alfieri n. 1, 31015 Conegliano (TV), con l'apposizione sulla busta della dicitura "riservata".

L'inoltro della comunicazione può avvenire anche a mezzo posta elettronica indirizzata a:

[odv231.secservices@finint.com](mailto:odv231.secservices@finint.com).

Oltre alle segnalazioni anche officiose di cui sopra devono essere obbligatoriamente trasmesse all'Organismo di Vigilanza tutte le informazioni concernenti:

- i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al Decreto;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti in caso di avvio di provvedimento giudiziario per i reati previsti dal Decreto;
- i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello Organizzativo con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate (ivi compresi i provvedimenti contro i Dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

In occasione dell'attuazione di nuovi prodotti o servizi l'Organismo di Vigilanza deve essere preventivamente informato dalle competenti strutture aziendali in merito alla valutazione di eventuali rischi riconducibili al D.Lgs n. 231/01.



L'Organismo di Vigilanza valuta le segnalazioni ricevute 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.

#### 4.6 Whistleblowing

A seguito delle novità introdotte con legge 179 del 2017, l'art. 6 del Decreto è stato integrato con i commi 2 – bis, 2 – ter e 2 – quater.

In particolare il comma 2 – bis, alla lett. b), dispone che il Modello adottato debba prevedere almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante.

A tal riguardo, si precisa che il CdA della Capogruppo ha approvato, in data 13/9/2016, la “Politica di Gruppo per la gestione delle segnalazioni di violazioni”, che norma e disciplina la possibilità per tutto il personale del Gruppo di procedere con la segnalazione di violazioni, intese come comunicazioni che pongono in rilievo una violazione perpetrata.

Al fine di favorire l'emersione di ogni fattispecie di illecito, le Società del Gruppo hanno, pertanto, messo a disposizione di dipendenti, membri di Organi Sociali e soggetti terzi aventi rapporti e relazioni d'affari con la Società e le Società del Gruppo, canali di comunicazione idonei a garantire la ricezione e gestione delle segnalazioni e l'anonimato del segnalante.

Si precisa che in seno al CdA del 28/9/2016 Securitisation Services S.p.A. ha recepito la suddetta Policy di gruppo.

In ossequio alle disposizioni normative sopra citate, la Società ha costituito i seguenti canali:

- casella posta elettronica: segnalazioneviolazione@bancafinint.com;
- cassetta delle lettere affissa nel corridoio in cui possono essere inserite segnalazioni in forma cartacea.



## Capitolo 5

### Codici di comportamento

#### 5.1 Integrità etica

Per garantire un efficace ed efficiente governo della Società ed una consapevole gestione della stessa, oltre alla formalizzazione di procedure in grado di garantire la corretta conduzione dei fatti aziendali, è necessario anzitutto la presenza di un ambiente caratterizzato da un'integrità etica tale da permettere la realizzazione degli obiettivi nella massima lealtà e trasparenza.

L'integrità etica contribuisce in modo rilevante all'efficacia delle politiche e dei sistemi di controllo ed influisce sui comportamenti che potrebbero sfuggire ai sistemi di controllo medesimi, per quanto gli stessi siano sofisticati. Si è ritenuto necessario diffondere i valori posti alla base dei giusti comportamenti, al fine di stimolare la condivisione degli stessi da parte di tutti i soggetti della struttura aziendale.

Partendo da questa premessa Securitisation Services S.p.A. ha adottato un proprio Codice Etico, che è stato sottoscritto per accettazione da tutti i Dipendenti, il quale sintetizza l'essenza del comportamento della Società, attraverso un insieme di valori e di regole il cui rispetto e la cui osservanza rappresentano elementi fondamentali dell'attività aziendale.

In un contesto economico caratterizzato da una forte e sempre maggiore competitività, esso ha l'obiettivo di improntare a trasparenza, correttezza, lealtà, integrità e credibilità i rapporti tra la Securitisation Services S.p.A. ed i suoi "portatori di interesse", intesi internamente quali Amministratori, soci, dipendenti ed esternamente quali Pubblica Amministrazione, clienti, mercato e l'intero contesto economico nel quale la Società opera.

Il Codice Etico è teso ad evitare comportamenti ambigui o scorretti mediante l'individuazione chiara delle principali regole da rispettare.

Tutte le azioni, operazioni e transazioni compiute o poste in essere a vantaggio dell'azienda o nel suo interesse devono essere ispirate alla massima correttezza, alla completezza e alla trasparenza delle informazioni, alla legittimità sotto l'aspetto formale e sostanziale, alla chiarezza e verità nei riscontri contabili, secondo le norme vigenti e le procedure stabilite. In particolare, la convinzione di agire in qualche modo a vantaggio della Società non giustifica l'adozione di comportamenti in contrasto con i suddetti principi.

Il Codice Etico è finalizzato a garantire l'esplicita posizione assunta dall'azienda in merito ai comportamenti da tenere da parte del personale (comprese le funzioni apicali), i propri collaboratori e consulenti, con particolare riferimento alle circostanze nelle quali sussistono i rischi collegati ai reati previsti dal Decreto.

Tale Codice Etico è soggetto a revisione periodica, attraverso una specifica valutazione cui sovrintende l'Organismo di Vigilanza. Quest'ultimo procede alla revisione di tale documento quando lo ritiene necessario ovvero, a titolo esemplificativo e non esaustivo, nelle circostanze, o sulla base, delle seguenti risultanze:

- inclusione di nuove fattispecie di reato nell'ambito del regime del Decreto in oggetto;
- esiti delle verifiche condotte sui rischi, sull'applicazione del Modello e circa i riscontri effettuati anche in merito alla piena conoscenza e comprensione da parte delle funzioni aziendali.

Ogni aggiornamento del Codice Etico viene portato a conoscenza delle funzioni interessate attraverso modalità analoghe a quelle previste per la sua diffusione ovvero con altre modalità, tempo per tempo verificate dall'Organismo di Vigilanza, atte ad assicurarne la sua massima diffusione e conoscenza.

Il Codice Etico rientra nella documentazione fornita ai dipendenti (in formato elettronico alternativamente a quello cartaceo) all'atto dell'instaurazione del rapporto di lavoro, ovvero all'atto dell'incarico ad Amministratori e Sindaci, e ad esso viene dedicata particolare attenzione all'interno dei piani di formazione alle strutture aziendali.

Tutto il personale di Securitisation Services S.p.A. (i Dipendenti anche a livello direttivo, gli Amministratori, i Sindaci e i collaboratori) è tenuto alla scrupolosa osservanza delle disposizioni contenute nel Codice Etico: la mancata



osservanza è valutata sotto il profilo disciplinare e potrà comportare l'adozione delle sanzioni contrattualmente previste. A fronte di ciò, la Società promuove la più ampia diffusione del Codice Etico presso tutti i soggetti interessati, la corretta interpretazione dei suoi contenuti e fornisce gli strumenti più adeguati per favorirne l'applicazione.

La Società mette in atto, inoltre, le necessarie misure al fine di svolgere attività di verifica e di monitoraggio dell'applicazione del Codice stesso e tale compito è stato affidato all'Organismo di Vigilanza.



## Capitolo 6

### Sistema disciplinare

#### 6.1 Principi generali

Aspetto essenziale per l'effettività del Modello è costituito dalla predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta imposte ai fini della prevenzione dei Reati di cui al Decreto, e, in generale, delle procedure interne previste dal Modello stesso.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dall'azienda in piena autonomia indipendentemente dall'illecito che eventuali condotte possano determinare.

La verifica dell'adeguatezza del sistema sanzionatorio, il costante monitoraggio dei procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché degli interventi nei confronti dei soggetti esterni sono affidati all'Organismo di Vigilanza, il quale procede anche alla segnalazione delle infrazioni di cui venisse a conoscenza nello svolgimento delle funzioni che gli sono proprie.

#### 6.2 Sanzioni previste per i lavoratori dipendenti (aree professionali e quadri direttivi)

I lavoratori/lavoratrici che incorrono nella violazione degli obblighi previsti nel Modello di organizzazione e di gestione e nel Codice Etico adottati dalla Società sono soggetti a sanzioni disciplinari – oggettivamente e soggettivamente correlate alla gravità delle infrazioni – nel rispetto dei criteri di proporzionalità stabiliti dal vigente CCNL e nel rispetto delle procedure previste dall'art. 7 Legge 20 maggio 1970, n. 300 nonché di eventuali normative speciali, di legge o di contratto applicabili. Tali violazioni devono essere in ogni caso comunicate tempestivamente, e comunque preventivamente all'irrogazione della sanzione, all'Organismo di Vigilanza, istituito dalla Società ai sensi dell'art. 6, comma 1, lett. b) del D.Lgs. n. 231/2001.

#### 6.3 Sanzioni previste per i dirigenti

Le violazioni commesse singolarmente dai dirigenti della Società, saranno tempestivamente, e comunque preventivamente all'irrogazione della sanzione, formalmente comunicate per iscritto dall'Organismo di Vigilanza alla Direzione del Personale e al Consiglio di Amministrazione, per la valutazione e l'adozione, da parte di quest'ultimo, degli opportuni provvedimenti sanzionatori compatibili con la vigente normativa. Stante la non opportunità dell'applicazione del sistema disciplinare in senso stretto, in ragione dell'elevato grado di fiducia che connota il relativo rapporto di lavoro, tali violazioni tuttavia, in relazione alla loro gravità, potranno comportare, nei casi di maggior rilievo, la risoluzione del rapporto di lavoro. Di tale conseguenza sanzionatoria verranno portati a conoscenza i singoli dirigenti o all'atto dell'assunzione o in corso di rapporto, mediante specifica, individuale comunicazione.

Detta comunicazione dovrà far riferimento alla natura fiduciaria del rapporto ed alla estrema gravità delle violazioni in questione, fermo restando sul piano applicativo, il rispetto delle garanzie procedurali di cui ai commi 2 e 3 dell'art. 7 della legge n. 300/1970, che secondo un consolidato orientamento giurisprudenziale, trovano applicazione anche nei confronti dei dirigenti.



#### **6.4 Sanzioni previste per i componenti del Consiglio di Amministrazione**

Le infrazioni commesse singolarmente dagli Amministratori della Società saranno tempestivamente, e comunque preventivamente all'irrogazione della sanzione, formalmente comunicate per iscritto dall'Organismo di Vigilanza al Consiglio di Amministrazione, per la valutazione e l'adozione degli opportuni provvedimenti sanzionatori compatibili con la vigente normativa. La commissione delle violazioni da parte degli Amministratori e gli eventuali provvedimenti sanzionatori irrogati dal Consiglio di Amministrazione dovranno essere comunicati, a cura dell'Organismo di Vigilanza (che esercita anche le funzioni di Collegio Sindacale) ed all'Assemblea dei soci.

#### **6.5 Sanzioni previste per collaboratori, consulenti, procuratori, agenti e terzi**

La violazione dei principi e delle regole di comportamento contenute nel Modello e ove inserite in specifiche clausole all'interno dei contratti, delle lettere di incarico e degli accordi stipulati dalla Società con consulenti, collaboratori, procuratori, agenti e terzi (ad esempio fornitori) potrà comportare le conseguenze espresse previste dalle medesime clausole, ivi compresi nei casi più gravi, la risoluzione del rapporto, il recesso ed il risarcimento dei danni. Tali violazioni devono essere in ogni caso comunicate, preventivamente all'irrogazione della sanzione, all'Organismo di Vigilanza.

#### **6.6 Sanzioni previste per chi viola le misure di tutela del segnalante**

La violazione del divieto di porre in essere atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante una violazione per motivi legati direttamente o indirettamente alla segnalazione saranno tempestivamente, e comunque preventivamente all'irrogazione della sanzione, formalmente comunicate per iscritto dall'Organismo di Vigilanza al Consiglio di Amministrazione, per la valutazione e l'adozione degli opportuni provvedimenti sanzionatori compatibili con la vigente normativa

#### **6.7 Sanzioni previste per chi effettua con dolo o colpa grave segnalazione che si rivelano infondate.**

Le segnalazioni che si rivelano infondate, effettuate dal personale con dolo o colpa grave, saranno tempestivamente, e comunque preventivamente all'irrogazione della sanzione, formalmente comunicate per iscritto dall'Organismo di Vigilanza al Consiglio di Amministrazione, per la valutazione e l'adozione degli opportuni provvedimenti sanzionatori compatibili con la vigente normativa.



*[omissis]*