

## **A - Modello Organizzativo D.Lgs. 231/01 e Codice Etico**

### **Art. 1. Rilevazione delle Aree di rischio**

La Banca di Legnano (di seguito “BdL”) ha svolto al proprio interno un’analisi al fine di individuare le aree funzionali nelle quali possa riscontrarsi in via astratta un rischio di realizzazione di taluna delle fattispecie criminose o d’illecito amministrativo rilevanti ai sensi del D.Lgs. 231/01.

Per la rilevazione delle aree di rischio si avvale anche di un Repository, istituito dalla Capogruppo BPM e gestito dalla funzione organizzativa di quest’ultima. In esso sono presenti i processi aziendali ed i relativi punti di controllo ai sensi del D.Lgs. 231/01 (per le attività, regolamentate da apposito contratto, eseguite in outsourcing da BPM per conto di BdL, i processi aziendali sono allineati ed il Repository della Capogruppo vale anche per BdL).

Il Repository è monitorato, alimentato ed aggiornato alla luce di nuove normative (o di modifiche e/o integrazioni di quelle esistenti) sia esterne che interne e/o degli sviluppi di attività progettuali connessi ad obiettivi di maggiore efficienza dei processi.

La simbologia utilizzata nel Repository permette di individuare i processi e le attività interessate dal D.Lgs. 231/01 e consente l’esportazione delle informazioni attraverso appositi meccanismi informatici creati ‘ad hoc’.

Le regole di utilizzo del Repository sono documentate in un apposito Manuale operativo. Le aree di rischio sono definite di seguito per categorie di reati ed illeciti amministrativi-presupposto, che vengono elencati rimandando all’Allegato per la puntuale definizione di ciascuna delle fattispecie indicate secondo quanto previsto dalla legge.

#### **Art. 1.1 Aree di rischio concernenti i rapporti con la Pubblica Amministrazione**

Reati:

- Malversazione a danno dello Stato (art. 316-bis cod. pen.)
- Indebita percezione di erogazioni in danno dello Stato (art. 316-ter cod. pen.)
- Concussione (art. 317 cod. pen.)
- Corruzione per un atto d’ufficio (art. 318 cod. pen.)
- Corruzione per un atto contrario ai doveri d’ufficio (art. 319 cod. pen.)
- Corruzione in atti giudiziari (art. 319-ter cod. pen.)
- Istigazione alla corruzione (art. 322 cod. pen.)
- Truffa (art. 640 cod. pen.)
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 cod. pen.)
- Frode informatica (art. 640 ter cod. pen.)

Nella ricerca delle aree funzionali all’interno delle quali possa realizzarsi un contatto con rappresentanti di enti pubblici e, in genere, con la Pubblica Amministrazione, si è fatto riferimento ad un’accezione estensiva di “ente pubblico”, che ricomprende anche

Organismi che, pur non rientrando nella categoria della “Pubblica Amministrazione”, hanno comunque un’indubbia rilevanza pubblicistica (quali l’Unione Europea, la Banca d’Italia, la Consob e le Autorità Garanti).

In relazione ai reati contro la Pubblica Amministrazione, le aree ritenute più a rischio sono:

- la gestione della tesoreria di enti pubblici e, in genere, di fondi pubblici, sia sotto forma di captazione o erogazione di contributi (in qualsiasi modo denominati) destinati a pubbliche finalità, sia nello svolgimento di attività in regime di concessione (ad esempio, riscossione di tributi);
- il processo per la concessione del credito. Quest’ultimo viene preso in considerazione con riguardo alle fasi di analisi/istruttoria e di delibera, laddove interessino pratiche nascenti da domande di finanziamento avanzate da enti pubblici ovvero da soggetti operanti all’interno di questi e la concessione di finanziamenti agevolati (ovverosia di quei finanziamenti che godono di agevolazioni concesse da parte di enti pubblici al ricorrere di determinate condizioni);
- la partecipazione a procedure pubbliche di gara e, in genere, a procedure competitive per l’aggiudicazione di concessioni da parte di enti pubblici ovvero la partecipazione a trattative private con tali enti al medesimo fine nonché al fine di pervenire al perfezionamento con essi di convenzioni di sponsorizzazione;
- la concessione di condizioni economiche in deroga, laddove si assumano delibere in favore di soggetti rappresentanti di enti pubblici o comunque operanti all’interno dei medesimi;
- l’ottenimento di concessioni o di licenze nel settore edilizio e, in genere, immobiliare ovvero l’ottenimento di contributi pubblici (come quelli connessi alla partecipazione a corsi di formazione organizzati da enti pubblici) o di benefici (quali quelli di natura fiscale connessi ad assunzioni effettuate con contratti di formazione);
- la gestione degli acquisti, con riguardo alle trattative che possono essere instaurate ed agli accordi che possono essere perfezionati con enti pubblici o con soggetti in essi operanti;
- la gestione delle pratiche aventi ad oggetto vicende che generano (o possono generare) contenziosi giudiziari;
- l’attività riferita ai rapporti con gli enti pubblici operanti nei settori tributario e previdenziale;
- le attività che comportano rapporti con Organismi di vigilanza, quali la Banca d’Italia e la Consob;
- le attività aventi ad oggetto la realizzazione e/o la gestione di collegamenti telematici con enti pubblici ovvero la trasmissione a questi ultimi di dati su supporti informatici;
- le attività aventi ad oggetto l’assunzione di personale e/o la gestione di trattamenti previdenziali del personale;
- le attività riguardanti la gestione delle verifiche delle ispezioni;
- le attività di gestione delle consulenze;
- le attività di gestione delle liberalità.

## **Art. 1.2 Aree di rischio concernenti le falsità in monete, carte di pubblico credito e valori di bollo**

Reati:

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 cod. pen.)
- Alterazione di monete (art. 454 cod. pen.)
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 cod. pen.)
- Spendita di monete falsificate ricevute in buona fede (art. 457 cod. pen.)
- Falsificazione dei valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 cod. pen.)
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 cod. pen.)
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 cod. pen.)
- Uso di valori di bollo contraffatti o alterati (art. 464 cod. pen.)

Nell'attività di BdL, come nell'attività di ogni Istituto di credito, rientra tipicamente il maneggio di monete, carte di pubblico credito e valori di bollo e la loro messa in circolazione.

Le aree interessate principalmente sono quelle relative:

- alle operazioni di sportello, in relazione alle operazioni effettuate per cassa;
- alle operazioni connesse all'alimentazione dell'apparecchiatura Bancomat;
- all'attività di custodia e gestione di valori nonché l'attività di recupero crediti, laddove vengano ricevuti pagamenti in denaro contante da parte dei creditori.

### **Art. 1.3 Aree di rischio concernenti i reati societari**

Reati:

- False comunicazioni sociali (art. 2621 cod. civ.)
- False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2621 cod. civ.)
- Falso in prospetto (art. 173 bis TUF)
- Falsità nelle relazioni o nelle comunicazioni della società di revisione (art. 174 bis TUF)
- Indebita restituzione dei conferimenti (art. 2626 cod. civ.)
- Illegale ripartizione degli utili o delle riserve (art. 2627 cod. civ.)
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 cod. civ.)
- Operazioni in pregiudizio dei creditori (art. 2629 cod. civ.)
- Omessa comunicazione del conflitto di interesse (art. 2629 bis cod. civ.)
- Formazione fittizia del capitale (art. 2632 bis cod. civ.)
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 cod. civ.)
- Impedito controllo (art. 2625 cod. civ.)
- Illecita influenza sull'assemblea (art. 2636 cod. civ.)
- Aggiotaggio (art. 2637 cod. civ.)
- Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di Vigilanza (art. 2638 cod. civ.)

Le aree a maggior rischio di commissione dei reati societari sono quelle in cui operano i soggetti in posizione apicale, rivestendo funzioni di rappresentanza, di amministrazione, di controllo (soprattutto contabile) o di direzione, nonché di dirigente preposto alla redazione dei documenti contabili societari.

In particolare, le funzioni maggiormente interessate dalle aree a rischio sono quelle relative a: (i) l'attività di relazione con organi di vigilanza o oltre autorità garanti (incluse le società di revisione); (ii) la gestione della contabilità centrale, della finanza, degli affari societari, (iii) la formazione di documenti, in senso lato, contabili e dei documenti che rappresentino situazioni economiche, finanziarie e patrimoniali della Banca (iv) la rappresentazione e diffusione all'esterno delle informazioni relative alla situazione economica patrimoniale e finanziaria della Banca; (v) i servizi tributari, (vi) l' "internal auditing", (vii) la gestione degli acquisti, (viii) la gestione del patrimonio immobiliare, (ix) l'amministrazione del credito (con riguardo alle determinazioni in tema di dubbi esiti e di passaggio a sofferenza), (x) l'attività legale (sia con riguardo all'attività di recupero di crediti sia a quella di gestione di contenziosi e reclami in genere), (xi) la gestione delle risorse umane (con riguardo alla gestione degli aspetti di natura amministrativa, fiscale e previdenziale nonché relativi alla pianificazione dei costi).

#### **Art. 1.4 Aree di rischio concernenti i reati e gli illeciti amministrativi di market abuse**

Reati:

- Abuso di informazioni privilegiate (art. 184. D. Lgs. n. 58/1998)
- Manipolazione del mercato (art. 185 D. Lgs. n. 58/1998)

Illeciti amministrativi:

- Abuso di informazioni privilegiate (art. 187 bis TUF)
- Manipolazione del mercato (art. 187 ter TUF)

I suddetti reati ed illeciti amministrativi, così come configurati dalla normativa in materia di Market Abuse, coinvolgono quelle funzioni che, all'interno della Banca, hanno la possibilità di accedere ad informazioni privilegiate - con ciò intendendosi (ai sensi dell'art. 181 Testo Unico della Finanza) quelle informazioni concernenti uno o più emittenti strumenti finanziari o uno o più strumenti finanziari che non sono state rese pubbliche e che, se rese pubbliche, potrebbero influire in modo sensibile sui prezzi di tali strumenti finanziari.<sup>(1)</sup>

Le Aree di Rischio interessate dai reati ed illeciti amministrativi di market abuse sono le seguenti:

- a) comunicazioni all'esterno (Borsa Italiana, Consob, analisti finanziari, azionisti, giornalisti, agenzie di rating, etc.);
- b) consulenza all'emissione o al classamento di strumenti finanziari o in generale di distribuzione di strumenti finanziari;
- c) gestione di eventuali conflitti di interesse;

- d) identificazione delle operazioni sospette così come elencate in modo non esaustivo esemplificativo nella Comunicazione Consob DME5078692 del 29 novembre 2005;
- e) negoziazione di strumenti finanziari;
- f) attività nel cui espletamento siano ricompresi rapporti diretti con le Autorità di Vigilanza o con il mercato, ivi compresi gli studi e le ricerche aventi ad oggetto emittenti o strumenti finanziari quotati, le attività di trading (per conto proprio o di terzi, ivi comprese le gestioni di patrimoni) e di advisory per operazioni di corporate finance.

-----

*(1) Talvolta il rischio di commissione di illeciti nell'interesse o a vantaggio dell'ente può sorgere dalla combinazione di ruoli e funzioni (cd. "cumulo di funzioni") che la banca svolge laddove ciò consenta di acquisire (e manipolare) informazioni trasversali su clienti, sull'ente stesso, su terzi.*

## **Art. 1.5 Aree di rischio concernenti delitti aventi finalità di terrorismo o di eversione dell'ordine democratico e delitti contro la personalità individuale**

Reati:

- Associazioni sovversive (art. 270 cod. pen.)
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordinamento democratico (art. 270 bis cod. pen.)
- Assistenza agli associati (art. 270 ter cod. pen.)
- Arruolamento con finalità di terrorismo anche internazionale (art. 270 quater cod. pen.)
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270 quinquies cod. pen.)
- Qualsiasi altro delitto che comporti erogazione o raccolta di fondi allo scopo o nella consapevolezza della loro utilizzazione per la commissione di atti di terrorismo internazionale (art. 25 quater, comma 4 D. Lgs. n. 231/2001)
- Pratiche di mutilazione degli organi genitali femminili (art. 583 bis cod. pen.) solo se commessi in struttura della Banca (art. 25 quater.1 D. Lgs. n. 231/2001)
- Riduzione o mantenimento in schiavitù o in servitù (art. 600 cod. pen.)
- Prostituzione minorile (art. 600 bis cod. pen.)
- Pornografia minorile (art. 600 ter cod. pen.)
- Detenzione di materiale pornografico (art. 600 quater cod. pen.)
- Pornografia virtuale (art. 600 quater.1 cod. pen.)
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600 quinquies cod. pen.)
- Tratta di persone (art. 601 cod. pen.)
- Acquisto e alienazione di schiavi (art. 602 cod. pen.)

Sia i delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, sia quelli riconducibili al crimine organizzato transnazionale e previsti dall'art. 10 della legge n. 146/2006, sia quelli contro la personalità individuale (fatta eccezione per quello relativo alla mutilazione degli organi genitali femminili, che si richiede sia commesso in struttura dell'ente e perciò, nella specie, della Banca) coinvolgono, ai fini del D.Lgs. n. 231/01, quelle funzioni che, all'interno della Banca, hanno la possibilità, sulla base del contatto diretto che instaurano con la clientela e/o sulla base dell'esame di documentazione ad

essa relativa ovvero dell'operatività da essa realizzata, di venire a conoscenza di circostanze anche solo tali da far insorgere dubbi in merito al possibile collegamento della clientela medesima con i delitti qui in considerazione .

Pertanto, le aree funzionali interessate sono quelle che operano attraverso il contatto diretto con i clienti o, comunque, che hanno la possibilità di accedere all'esame dell'operatività da loro posta in essere e/o di documenti concernenti quest'ultima o, in genere, contenenti informazioni concernenti lo svolgimento della loro attività. <sup>(1)</sup> Conseguentemente le funzioni principalmente coinvolte possono essere individuate in quella commerciale, in quelle relative al processo di erogazione del credito, nonché in quella finanziaria.

Per il delitto relativo alla mutilazione degli organi genitali femminili, invece, l'area funzionale interessata è quella della vigilanza sugli accessi alle unità operative della Banca e la funzione interessata è quella che si occupa della sicurezza fisica dei dipendenti e di terzi.

-----

<sup>(1)</sup> *La banca, infatti, per il tramite di propri operatori (che agiscano con finalità illecite o con la consapevolezza delle altrui finalità illecite), nella fisiologica attività di raccolta del risparmio ed erogazione del credito, si potrebbe trovare ad instaurare rapporti con clienti che perseguono, direttamente o quali prestanome, finalità di terrorismo od eversione dell'ordine costituzionale o, più in generale, con organizzazioni operanti sul piano internazionale, così da agevolarli mettendo a loro disposizione risorse finanziarie o comunque incrementandone le disponibilità economiche, che risultino poi strumentali nel perseguimento dei loro criminali obiettivi.*

## **Art. 1.6 Aree di rischio concernenti i reati transnazionali**

Reati, se a carattere transnazionale:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416 bis c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291 quater del Testo Unico di cui al Presidente della Repubblica del 23 gennaio 1973 n. 43);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del Testo Unico del Presidente della Repubblica del 9 ottobre 1990, n. 309);
- Riciclaggio (art. 648 bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter c.p.);
- Disposizioni contro le immigrazioni clandestine (art. 12, co. 3, 3 bis, 3 ter e 5, del Testo Unico di cui al d.lgs. 25 luglio 1998, n. 286);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377 bis c.p.)
- Favoreggiamento personale (art. 378 c.p.).

A tal fine, si definisce “reato transnazionale”, a norma dell’art. 3 della medesima legge 16 marzo 2006 n. 146, «il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonchè:

- 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 un altro Stato;
- c. ovvero sia commesso in uno Stato ma in esso sia implicato 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.»

Le funzioni interessate appaiono tendenzialmente coincidenti con quelle di cui al precedente punto 1.5, quali quelle che operano attraverso il contatto diretto con la clientela, o che hanno comunque la possibilità di accedere ai contenuti di tale attività. Anche per questi reati, pertanto, le aree principalmente coinvolte possono essere individuate in quella commerciale, in quelle relative al processo di erogazione del credito, nonché in quella finanziaria.

### **Art. 1.7 Aree di rischio concernenti la tutela della salute e della sicurezza sul lavoro**

Reati, se commessi con violazione delle norme antinfortunistiche e sulla tutela dell’igiene e della salute sul lavoro:

- omicidio colposo (art. 589 cod. pen.)
- lesioni personali colpose gravi o gravissime (art. 590, comma 3 cod. pen.)

Le aree funzionali a rischio principalmente interessate sono:

- la gestione delle risorse umane (con particolare riferimento agli aspetti contrattuali e di legge in tema di salute e sicurezza nei luoghi di lavoro, nonché alla formazione del personale sulla materia specifica);
- la gestione del patrimonio immobiliare (lavori immobiliari concernenti sia i cespiti di proprietà che in affitto, installazione dell’impiantistica, conduzione e manutenzione ordinaria e straordinaria degli stabili e degli impianti), con particolare riferimento alla contrattualistica relativa alle prestazioni commissionate in appalto;
- la gestione degli interventi in tema di sicurezza ambientale;
- l’applicazione del D.Lgs. 626 del 1994;
- la definizione ed il mantenimento degli standard aziendali di sicurezza presso la totalità delle unità organizzative;
- la congruità dei sistemi e delle soluzioni attivate per il rispetto delle normative concernenti la sicurezza e la tutela delle persone;
- la gestione del parco automezzi (manutenzione, revisione ecc.).

### **Art. 1.8 Aree di rischio concernenti l'utilizzo del sistema finanziario a scopo di riciclaggio**

Reati :

- ricettazione (art. 648 cod. pen.)
- riciclaggio (art. 648-bis cod. pen.)
- impiego di danaro, beni o utilità di provenienza illecita (art. 648-ter cod. pen.).

La Banca, per il tramite di propri operatori (che agiscano con finalità illecite o con la consapevolezza delle altrui finalità illecite), nello svolgimento della propria attività fisiologica si potrebbe trovare ad instaurare rapporti con clienti che perseguono, direttamente o quali prestanome, le finalità delittuose in argomento, così da agevolarli mettendo a loro disposizione risorse finanziarie o comunque incrementandone le disponibilità economiche, che risultino poi strumentali nel perseguimento dei loro criminosi obiettivi.

Le aree funzionali a rischio interessate sono quindi assimilabili a quelle indicate per i delitti di terrorismo (punto 1.5) e crimine transnazionale (punto 1.6), ovvero quelle funzioni che, all'interno della Banca, hanno la possibilità, sulla base del contatto diretto che instaurano con la clientela e/o sulla base dell'esame di documentazione ad essa relativa o dell'operatività da essa realizzata, di venire a conoscenza di circostanze tali da far insorgere dubbi relativi al possibile collegamento della clientela medesima con i delitti qui considerati.

Pertanto, sono coinvolte :

- le funzioni che operano attraverso il contatto diretto con la clientela (area commerciale in genere, principalmente per quanto concerne le attività di acquisizione/sviluppo e gestione dei rapporti, anche sotto il profilo strettamente operativo);
- le funzioni che operano nell'ambito dell'attività finanziaria (servizi di investimento);
- le funzioni che esercitano il processo di analisi, valutazione, concessione ed erogazione del credito (sia a livello periferico che a livello centrale);
- le funzioni che esercitano l'attività di recupero dei crediti (area legale e contenzioso);
- le funzioni che esercitano l'attività di monitoraggio, sorveglianza e gestione dei rischi, ivi compresa la Funzione di Compliance, per quanto concerne la valutazione del cosiddetto "rischio di non conformità", ovvero il rischio di incorrere in sanzioni giudiziarie o amministrative in conseguenza di violazione delle specifiche norme imperative (di legge o di regolamento), attraverso la verifica in via preventiva dell'idoneità delle procedure interne ad assicurare il rispetto della normativa di riferimento;
- le funzioni che esercitano, ai vari livelli, l'attività di controllo;
- le funzioni preposte all'attività di valutazione e gestione delle segnalazioni di operazioni sospette;
- le funzioni preposte alle comunicazioni delle informazioni richieste dall'Autorità Giudiziaria.

Per quanto riguarda infine il reato di ricettazione, la funzione coinvolta è, in particolare, quella che si occupa degli acquisti.

### **Art. 1.9 Aree di rischio concernenti i reati informatici**

Reati (nuove fattispecie di illecito amministrativo commesse in dipendenza di delitti informatici e trattamento illecito di dati) :

- falsità in documenti informatici (art. 491-bis cod. pen.)

- accesso abusivo ad un sistema informatico o telematico (art. 615-ter cod. pen.)
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater cod. pen.)
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. pen.)
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater cod. pen.)
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies cod. pen.)
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. pen.)
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter cod. pen.)
- danneggiamento di sistemi informatici o telematici (art. 635-quater cod. pen.)
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies cod. pen.)
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies cod. pen.)

Si premette che la gestione dei sistemi informatici è accentrata presso la Capogruppo Banca Popolare di Milano, sulla base di specifico contratto di servizio di conduzione.

Le aree di rischio principalmente interessate sono pertanto individuabili presso la Capogruppo stessa, nell'ambito delle strutture facenti capo alla Divisione Organizzazione I.T. e Operations, in particolare la D.I.C.T.O. (Direzione Information Communication Technology e Operations) alla quale rispondono :

- l'Area Pianificazione e Governance, che supporta la Direzione nell'attività di governo della struttura, attraverso i Settori ad essa facenti capo, con particolare riferimento al Settore Pianificazione e Controllo IT che supporta la Direzione nella gestione delle relazioni con i vertici aziendali e con enti esterni (tra i quali la Banca d'Italia, la Consob e l'ABI);
- il Comitato Sicurezza IT, che supporta la Direzione nella definizione delle linee guida delle politiche di sicurezza delle infrastrutture tecnologiche, applicative e del patrimonio informativo gestito prevalentemente con soluzioni automatizzate garantendo, attraverso attività di coordinamento, che la politica di sicurezza sia adeguatamente conosciuta e implementata all'interno della stessa Direzione;
- il Servizio Sviluppo Informatico (con i diversi Settori ed Aree ad esso facenti capo);
- il Servizio Infrastrutture Informatiche (al quale risponde, in particolare, l'Area Telecomunicazioni e Sicurezza all'interno della quale il Settore Sicurezza IT è responsabile del processo che garantisce la sicurezza logica dei dati ed il suo aggiornamento, verificandone costantemente l'efficacia ed assicurando azioni tempestive in caso di violazioni; detto Settore è inoltre responsabile dello sviluppo, gestione e manutenzione delle applicazioni di sicurezza).

Altre aree di rischio presso la Capogruppo sono costituite da :

- la Divisione Risorse e Politiche Contrattuali che, tramite l'Area Sistemi del Personale e Controlli ad essa facente capo, provvede all'amministrazione della Sicurezza Informatica su Host, gestendo operativamente la definizione delle risorse e il rilascio delle autorizzazioni all'accesso al sistema informatico in

- generale, intrattenendo inoltre, in merito agli aspetti di sicurezza, i rapporti con gli EDP auditors;
- il Settore Segreteria Fidi dell'Area Amministrazione Credito, all'interno del Servizio Back Office, che coordina l'attività di controllo e rettifica dei dati anagrafici e contabili per le segnalazioni mensili alla Centrale Rischi Banca d'Italia ed alla Centrale Rischi di Importo Contenuto (C.R.I.C.).

Per quanto riguarda i servizi prestati attraverso Reti Telematiche un'area di rischio si configura nell'ambito della società di servizi del Gruppo alla quale i servizi stessi sono stati affidati ([We@Service](#) Spa che ha il compito di sviluppare la piattaforma informatica Internet della divisione [We@Bank](#)).

All'interno di BdL le funzioni potenzialmente coinvolte possono essere individuate nell'ambito della Direzione Amministrativa che, tramite l'Ufficio Contabilità Generale, presiede al rispetto ed all'aggiornamento degli obblighi di Vigilanza verso la Banca d'Italia relativamente alle segnalazioni di carattere contabile, provvedendo inoltre alla verifica ed all'effettuazione dei pagamenti dei vari tributi, fatta eccezione per quelli di competenza di altri settori della Banca (quali ad esempio i contributi da versare agli enti previdenziali, la cui gestione è affidata all'Ufficio Relazioni Normative e Amministrazione della Direzione Personale, altra area funzionale potenzialmente interessata ai reati in argomento).

## **Art. 2 Regole (o "standard") di controllo**

Nella realizzazione delle attività che hanno condotto alla formulazione del presente Modello, BdL, dopo avere effettuato un attento esame dei reati ed illeciti amministrativi cui si applica il D.Lgs. 231/01, ha proceduto ad individuare i principali controlli (definiti "standard di controllo") volti a presidiare il rischio di commissione dei reati medesimi.

Tali regole, peraltro, si affiancano ai principi etici (di carattere, ovviamente, più generale) cui devono conformarsi l'attività ed il comportamento di tutto il personale, nonché di tutti coloro che collaborano a qualsivoglia titolo con la Banca stessa: principi che sono contenuti in un apposito "CODICE ETICO" diffuso presso i dipendenti di BdL.

Gli approfondimenti di cui sopra sono stati svolti con riguardo alle diverse categorie di illeciti cui si applica il decreto legislativo.

Gli "standard" di controllo così individuati vengono a costituire il complesso di regole che costituisce il contenuto del modello di organizzazione, gestione e controllo adottato da BdL.

Peraltro tali regole, nella loro generalità, risultano già da tempo adottate da BdL, essendo presenti nell'Ordinamento Generale d'Istituto allo stato vigente all'interno di quest'ultima, e formano, comunque, oggetto, laddove necessario, di costanti interventi d'implementazione.

L'Ordinamento Generale d'Istituto costituisce il documento in cui sono definiti l'assetto organizzativo, l'ordinamento funzionale e i regolamenti della Banca di Legnano.

Per la pratica attuazione delle norme contenute in tale Ordinamento e per il corretto svolgimento delle attività valgono le istruzioni generali o particolari impartite nel tempo mediante regolamenti, circolari normative, disposizioni operative e comunicazioni di servizio non in contrasto con le seguenti disposizioni.

L'Ordinamento è sottoposto a regolare aggiornamento e revisione al fine di garantire un corretto adeguamento alle normative emanate dal Legislatore in materia di Banca.

Attraverso l'Ordinamento Generale d'Istituto la Banca assicura il regolare svolgimento delle attività aziendali, orientando le proprie azioni e comportamenti ai principi di onestà, integrità, correttezza e trasparenza sui quali si fonda l'Ordinamento medesimo per un corretto perseguimento degli obiettivi aziendali.

Ciascun dipendente è tenuto a conoscere e rispettare il predetto Ordinamento.

Il Direttore Generale e i Responsabili di Funzione hanno l'obbligo di segnalare agli organi preposti ad attività di controllo eventuali anomalie e situazioni che possono determinare rischi rilevanti per la Società.

Il Consiglio di Amministrazione, sentito il Collegio Sindacale, modifica l'Ordinamento su proposta del Direttore Generale.

## **Art. 2.1 Controlli preventivi di tutte le tipologie di reati ex D.Lgs. 231/01**

Con riguardo ai diversi reati previsti dal D.Lgs. 231/01, BdL si è dotata di regole preventive ("standard" di controllo) così riassumibili:

- Normativa aziendale.

BdL si è da tempo dotata di un sistema di disposizioni aziendali (norme, circolari, regolamenti e tutti quei documenti costituenti il sopra menzionato Ordinamento Generale dell'Istituto) idoneo a fornire a coloro che operano per conto della stessa i principi di riferimento sia generali sia specifici, per la regolamentazione delle attività svolte e al rispetto delle quali gli operatori medesimi sono tenuti: un sistema che, peraltro, è soggetto a continui aggiornamenti da parte di Funzioni all'uopo specificamente dedicate (Ordinamento Generale d'Istituto: Ordinamento Funzionale, Regolamento dei Comitati, Regolamento Fidi, Regolamento Registro degli "Insider", Regolamento di Cassa e Custodia Valori, Regolamento di Sicurezza, Regolamento Acquisti).

Tutta la normativa aziendale costituisce parte integrante del presente modello.

Le normative interne contengono altresì le specifiche degli "standard" di controllo di seguito elencati.

- Regole per l'esercizio dei poteri di firma e dei poteri autorizzativi.

L'esercizio dei poteri di firma e dei poteri autorizzativi è rigidamente regolamentato da disposizioni che, in modo specifico e dettagliato, individuano i soggetti ai quali, con riguardo ai diversi atti e alle diverse operatività, sono riconosciuti tali poteri nonché le modalità e le limitazioni con le quali essi devono essere esercitati (limiti d'importo riferiti all'operazione, diversi a seconda del grado ricoperto, e/o modalità di abbinamento di firme di diversi soggetti). Si vedano, in Ordinamento Generale d'Istituto: Poteri delegati (Poteri di Firma e Poteri di Pricing) e Regolamento Fidi.

- Segregazione delle attività.

Lo svolgimento delle diverse attività all'interno di BdL è regolamentato sulla base di una rigorosa separazione tra l'attività di chi esegue, l'attività di chi autorizza e quella di chi controlla.

- Tracciabilità dei processi.

L'operatività svolta all'interno di BdL è regolata da meccanismi che consentono l'individuazione delle attività svolte, degli autori, delle fonti e degli elementi informativi relativi alle comunicazioni inerenti le specifiche di cui ai reati previsti dal D.Lgs. 231/01.

La Direzione Controlli inserisce nella propria pianificazione le verifiche sulle attività sensibili ai reati in considerazione e, con periodicità trimestrale, relaziona in merito l'Organismo di Vigilanza che, almeno semestralmente, predispone un rapporto scritto sull'attività svolta per il Consiglio di Amministrazione, per il Collegio Sindacale e per il Direttore Generale. Il preposto alla Direzione Controlli, membro di diritto dell'Organismo di Vigilanza, è inoltre tenuto a segnalare immediatamente al medesimo ogni dato rilevante ai fini della prevenzione dei reati in oggetto, avvalendosi anche di tutte le segnalazioni che pervengono al suddetto Organismo, comprese quelle inviate alla casella di posta elettronica all'uopo predisposta e inserita nel sito istituzionale della Banca.

## **Art. 2.2 Controlli specifici per le singole tipologie di reati**

### **2.2.1 Controlli preventivi dei reati contro la Pubblica Amministrazione**

(Normativa aziendale di riferimento: Amministrazione e Contabilità, Commerciale, Credito, Finanza, Information Technology, Legale, Sistemi di Pagamento).

Per la prevenzione dei reati contro la Pubblica Amministrazione BdL ha determinato di avvalersi, oltre che dei controlli di carattere generale innanzi esaminati, anche dei seguenti controlli di natura più specifica.

A) Il controllo sui soggetti che gestiscono l'attività di riferimento. In ogni caso, è quanto meno data ad essi istruzione di attenersi alle seguenti disposizioni:

- a) obbligo di segnalazione del contatto /rapporto iniziale con la PA;
- b) autorizzazione formale alla stipula dell'atto o all'esecuzione di un'operazione;
- c) registrazione dell'operazione come da procedure aziendali.

B) Il divieto di accesso a risorse finanziarie in autonomia (anche solo per autorizzare disposizioni di pagamento) da parte del soggetto che intrattiene rapporti con la Pubblica Amministrazione. In ogni caso, viene quanto meno richiesto che sussista:

- a) autorizzazione formale alla disposizione di pagamento;
- b) documentazione giustificativa delle risorse finanziarie utilizzate, con motivazione, attestazione di inerenza e congruità, approvata dal superiore gerarchico e archiviata.

C) Il divieto di conferimento in autonomia di contratti di consulenza o similari da parte del soggetto che intrattiene rapporti con la Pubblica Amministrazione, o comunque, quanto meno:

- a) autorizzazione formale al conferimento dell'incarico, con limiti di spesa, vincoli e responsabilità;
- b) lista di fornitori / consulenti / professionisti, gestita dal Servizio competente;
- c) gestione della lista di fornitori (inserimento / eliminazione) basata su criteri oggettivi, di cui, all'interno della lista, deve essere data motivazione e documentazione;

d) documentazione giustificativa degli incarichi conferiti con motivazione, attestazione di inerenza e congruità, approvata dal superiore gerarchico e archiviata.

D) Il divieto di concessione in autonomia di utilità da parte del soggetto che intrattiene rapporti con la Pubblica Amministrazione, o comunque, quanto meno:

- a) autorizzazione formale a conferire utilità;
- b) elenco degli omaggi gestito dal servizio competente e, comunque, da soggetto diverso da quello che intrattiene rapporti con la Pubblica Amministrazione;
- c) documentazione giustificativa delle spese effettuate per la concessione di utilità con motivazione, attestazione di inerenza e congruità, approvata dal superiore gerarchico e archiviata;
- d) lista degli usuali fornitori, gestita (inserimento / eliminazione) dal Servizio Centro Acquisti in base a criteri oggettivi, con individuazione, all'interno della lista, del fornitore della singola utilità, adeguatamente motivata e documentata;
- e) "budget" e consuntivi che evidenzino separatamente le spese per ciascuna tipologia di utilità.

E) Il divieto in autonomia di assunzione di personale da parte del soggetto che intrattiene rapporti con la Pubblica Amministrazione o, più in generale, divieto in capo allo stesso di procedere all'instaurazione di rapporti di lavoro mobilità interna, avanzamenti di carriera, trattamenti economici nominativi e trasferimenti nominativi per i Dirigenti. Compiti, questi, che sono tutti in capo al Consiglio d'Amministrazione o alla struttura aziendale competente delegata, che procederà con modalità operative e responsabilità definite e con oggettivi criteri di selezione dei candidati.

F) Per ogni iniziativa della banca che comporti in stato patrimoniale appostazione ad immobilizzazioni di opere o manufatti per la cui realizzazione sia prevista autorizzazione o verifica da parte della P.A., l'inserimento nella relativa pratica di un esemplare di tabella di incidenza standard dei costi ricorrenti, anche figurativi, suddivisi per categoria di spesa, previamente vistata dal Controllo di gestione, nonché – a definizione della pratica stessa – di tabella consuntiva d'incidenza percentuale dei costi, anche figurativi, sostenuti vistata dal responsabile.

G) Obbligo di segnalazione di eventuali anomalie relative a:

- a) incrementi di operatività con la banca dei clienti beneficiari di sovvenzioni pubbliche erogate tramite la banca;
- b) condizioni più favorevoli di quelle di mercato applicate a pubblici ufficiali od incaricati di pubblico servizio ovvero a membri di organi della Comunità europea o funzionari della stessa o di Stato estero e loro coniugi, figli e genitori;
- c) assunzioni, promozioni, gestione della carriera ed instaurazione di rapporti di collaborazione e consulenza con i soggetti di cui alla precedente lettera b);
- d) scostamenti a consuntivo delle percentuali sub F).

H) L'esistenza di adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel D.Lgs. n. 196 del 2003 e/o relative alle "best practices" di riferimento, consistenti quanto meno in:

- a) cancellazione dati, liste di controllo e archivi affidata esclusivamente ad una Funzione competente, assicurandone la tracciabilità;
- b) liste di controllo degli accessi ai sistemi informativi e segnalazioni automatiche all'amministratore del sistema di operazioni non autorizzate (cancellazioni, tentativi di accesso, alterazione delle funzionalità del sistema, ecc.).

Inoltre, nei rapporti con la Pubblica Amministrazione devono essere rispettati i seguenti principi:

1. la stipulazione di contratti / convenzioni con soggetti pubblici da parte della Banca a seguito della partecipazione a procedure ad evidenza pubblica (asta pubblica, appalto-concorso, licitazione privata e trattative privata) deve essere condotta in conformità ai principi, criteri e disposizioni dettate dal presente Modello;

2. qualunque tipo di erogazione di fondi: (a) deve essere deliberata previa adeguata istruttoria cui partecipino soggetti e/o funzioni diverse all'interno della Banca, in modo da minimizzare il rischio di una manipolazione illecita dei dati ed aumentare la condivisione delle conoscenze e delle decisioni all'interno della Banca; (b) presuppone una approfondita conoscenza della clientela, così da consentire una valutazione della coerenza e della compatibilità dell'operazione con il profilo cliente, soprattutto laddove quest'ultimo non svolga attività di rilievo economico;

3. l'erogazione del credito da parte della Banca deve essere eseguita nel rispetto delle prescrizioni contenute nella procedura aziendale interna predisposta in ottemperanza alle norme di riferimento che regolano gli affidamenti (TUB) e alle istruzioni di vigilanza sulle aziende di credito;

4. ai Collaboratori Esterni che materialmente intrattengono rapporti con la P.A. per conto della Banca, deve essere formalmente conferito potere in tal senso dalla Banca, con apposita clausola contrattuale.

5. di qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la P.A. deve esserne informato l'Organismo di Vigilanza con nota scritta;

6. i contratti tra BdL e i Collaboratori Esterni devono essere definiti per iscritto in tutte le loro condizioni e termini, e rispettare quanto indicato ai successivi punti;

7. i Consulenti sono scelti con metodi trasparenti e secondo specifica procedura aziendale, facendo ricorso, ove possibile, ai Consulenti "accreditati" nelle c.d. "recommended list";

8. i Partner Commerciali devono essere scelti con metodi trasparenti e secondo specifica procedura (es. utilizzando apposite check list o una procedura formalizzata di beauty contest);

9. nei contratti con i Consulenti e con i Partner Commerciali deve essere contenuta apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al Decreto e delle sue implicazioni per BdL; di non essere mai stati implicati in procedimenti giudiziari relativi ai reati nello stesso contemplati (o se lo sono stati devono comunque dichiararlo ai fini di una maggiore attenzione da parte di BdL in caso si addivenga all'instaurazione del rapporto di consulenza o partnership); di impegnarsi al rispetto delle prescrizioni contenute nel Decreto;

10. nei contratti con i Consulenti e con i Partner Commerciali deve essere contenuta apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al Decreto (es. clausole risolutive espresse, penali);

11. alle ispezioni giudiziarie, tributarie e amministrative (es. relative alla L. 626/94, verifiche tributarie, INPS, autorità di vigilanza ecc.) devono partecipare i soggetti a ciò espressamente delegati o da questi ultimi sub-delegati, ovvero i soggetti responsabili delle unità operative. L'Organismo di Vigilanza dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, generata dalla segnalazione della possibile commissione di reati ai sensi del Decreto, mediante apposita comunicazione interna, inviata a cura della Direzione della Banca di volta in volta interessata.

### **2.2.2 Controlli preventivi dei reati concernenti le falsità in monete, carte di pubblico credito e valori di bollo**

(Normativa aziendale di riferimento: Commerciale, Estero, Sistemi di Pagamento, Credito, Information Technology).

Anche per la prevenzione dei reati concernenti le falsità, ai controlli di carattere generale innanzi esaminati si aggiungono controlli maggiormente specifici, che, in particolare, consistono in:

- Sussistenza di strumenti idonei alla verifica dell'autenticità del denaro e dei valori bollati.
- Controlli sul soggetto che maneggia denaro contante e/o valori bollati, consistenti alternativamente in:

- a) vincoli alla disponibilità di denaro contante e valori bollati;
- b) organizzazione idonea a limitare la disponibilità in denaro contante e valori bollati;
- c) monitoraggio, per quanto di rispettiva competenza, da parte dei responsabili del controllo di linea e della Direzione Controlli, dei reclami della clientela in materia.

### **2.2.3 Controlli preventivi dei reati societari**

(Normativa aziendale di riferimento: Amministrazione e Contabilità)

Diversamente dalle categorie di reati sin qui considerate (nonché da quella, di cui si dirà in appresso, dei reati aventi finalità di terrorismo, di quelli contro la personalità individuale e di quelli ascrivibili al crimine organizzato transnazionale), i reati societari che assumono rilevanza ai fini del D.Lgs. n. 231/01 si presentano come una categoria non omogenea bensì composta da fattispecie per molti aspetti diverse fra loro.

Pertanto, in considerazione sia della quantità di tali reati sia delle peculiarità che ciascuno di essi presenta rispetto agli altri, BdL ha ritenuto di individuare "standard" di controllo diversi e specifici per taluni di essi, fermi restando, peraltro, i controlli di carattere generale applicati, come si è già detto, a tutte le tipologie di reati.

Inoltre, resta fermo l'obbligo di attenersi alle disposizioni dettate dal Codice Civile, dalle leggi speciali e dalla normativa degli Organi di Vigilanza al fine di regolamentare la formazione delle comunicazioni sociali e, in generale, dei documenti contabili nonché, comunque, il compimento di attività di rilevanza contabile-amministrativa.

### **False comunicazioni sociali\*\*\***

Relativamente allo svolgimento di attività potenzialmente connesse al reato di false comunicazioni sociali (predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché adempimenti di oneri informativi obbligatori per legge o per disposizioni di Autorità di vigilanza), i controlli previsti si attuano tramite:

- **Regolamenti di gruppo:** esistono e sono diffuse al personale coinvolto in attività di predisposizione del bilancio, oltre alla generale normativa aziendale, anche norme di gruppo che definiscono con chiarezza i principi contabili da adottare per la definizione delle poste di bilancio civilistico e consolidato e le modalità operative per la loro contabilizzazione. Tali norme vengono tempestivamente integrate/aggiornate dalle indicazioni fornite dall'ufficio competente sulla base delle novità in termini di normativa civilistica e diffuse ai destinatari sopra citati.
- **Istruzioni di chiusura contabile:** esistono istruzioni chiare rivolte ai servizi nelle quali si stabilisce quali dati e notizie debbano essere forniti al servizio competente per la redazione del bilancio civilistico e consolidato, nonché per la redazione di relazioni e comunicazioni sociali, con indicazione altresì di tempi e modalità.
- **Livello di servizio/ flusso informativo:** deve essere effettuata un'attenta verifica della conformità del flusso informativo proveniente dalle diverse funzioni aziendali rispetto alle istruzioni definite e comunicate.
- **Lettere di attestazione:** è obbligatorio da parte dei vertici dei servizi e delle società del Gruppo, ai fini della redazione del bilancio consolidato, fornire al responsabile una lettera di attestazione sulla veridicità e completezza delle informazioni fornite.
- **Formalizzazione/Tracciabilità delle attività svolte:** è necessario che la trasmissione dei dati ed informazioni al servizio responsabile avvenga attraverso un sistema informatico, che consente la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il responsabile del servizio deve garantire la tracciabilità delle informazioni contabili non generate in automatico dal sistema.
- **Attività di formazione:** esiste un programma di formazione di base rivolto a tutti i responsabili dei servizi coinvolti nella redazione del bilancio e degli altri documenti connessi in merito alle principali nozioni e problematiche giuridiche e contabili sul bilancio.
- **Formalizzazione e conservazione del fascicolo di bilancio:** esistono regole chiare e formalizzate che identificano ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio, dall'approvazione da parte del Consiglio d'Amministrazione sino al deposito e alla pubblicazione (anche informatica) dello stesso nonché alla relativa archiviazione.
- **Formalizzazione delle modifiche dei dati contabili:** la possibilità di effettuare modifiche alle situazioni contabili è riconosciuta esclusivamente al servizio che le ha generate, con modalità appositamente regolamentate e tali da assicurarne la tracciabilità.

### **Falso in prospetto\*\*\***

Relativamente allo svolgimento di attività potenzialmente connesse al reato di falso in prospetto (predisposizione di prospetti a fini di sollecitazione all'investimento o di ammissione alla quotazione nei mercati regolamentati, predisposizione di documenti da

pubblicare in occasione di un'offerta al pubblico di strumenti finanziari), i principali controlli si attuano tramite:

- **Identificazione del responsabile:** è garantita l'individuazione dei responsabili delle Funzioni Aziendali che provvedono direttamente o indirettamente alla redazione di prospetti e/o documenti da pubblicare, in occasione di un'offerta al pubblico di strumenti finanziari.
- **Formalizzazione / Tracciabilità delle attività svolte:** devono essere formalizzate tutte le attività svolte per la redazione del documento/prospetto e deve essere assicurata la tracciabilità dell' "iter" procedurale.
- **Formalizzazione e conservazione del prospetto:** esistono regole chiare e formalizzate che identificano ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento dei documenti/prospetti di cui sopra e alla relativa archiviazione.

### **Falsità nelle relazioni o nelle comunicazioni delle società di revisione\*\*\***

Relativamente allo svolgimento di attività potenzialmente connesse a tale reato (gestione dei rapporti con la Società di Revisione contabile in ordine all'attività di comunicazione a terzi relativa alla situazione economica, patrimoniale o finanziaria della Società revisionata, nonché dei rapporti con ogni interlocutore della società di revisione), i principali controlli si attuano tramite:

- **Obblighi di collaborazione:** è obbligatorio collaborare strettamente con la Società di Revisione, da parte di tutti coloro che all'interno della Banca abbiano conoscenza di dati incidenti direttamente o indirettamente sulla situazione economica, patrimoniale o finanziaria di BdL.
- **Selezione della società di revisione e indipendenza del mandato:** i criteri di scelta della Società di Revisione e di verifica dell'indipendenza del mandato sono fissati in via preventiva.
- **Formalizzazione/Tracciabilità delle attività svolte:** esistono regole chiare e formalizzate che identificano ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento dei documenti/prospetti descritti nei punti precedenti e alla relativa archiviazione, nonché procedure che assicurano la tracciabilità delle attività svolte.

### **Impedito controllo\*\*\***

Relativamente alle attività potenzialmente connesse al reato di impedito controllo (redazione, tenuta e conservazione dei documenti su cui altri organi societari o i soci potrebbero esercitare il controllo), i principali controlli si attuano tramite:

- **Obbligo di collaborazione:** è obbligatoria la collaborazione fra le diverse Funzioni Aziendali che detengono dati della Banca e i soggetti che svolgono una funzione di controllo (Collegio Sindacale e Società di Revisione).
- **Esistenza di regole di Corporate governance e di comportamento:** esistono istruzioni chiare per quanto concerne la conservazione dei documenti contabili che concorrono alla formazione del bilancio (da intendersi sia quali regole di Corporate Governance sia quali norme comportamentali).
- **Obbligo di informativa verso l'Internal Audit:** è stabilito l'obbligo di comunicazione sistematica all'Internal Audit di ogni richiesta di informazioni o documentazione ricevuta

dall'Organo amministrativo o dai suoi delegati e proveniente dai soci, da altri organi sociali o dalla società di revisione.

- **Esistenza, presso la Capogruppo, di Comitati di controllo e di un Comitato per le remunerazioni.**

- **Recepimento del Codice Preda.**

- **Formalizzazione/Tracciabilità delle attività svolte:** esistono regole chiare e formalizzate che identificano ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento dei documenti/prospetti di cui sopra ed alla relativa archiviazione nonché procedure che assicurano la tracciabilità delle attività svolte.

### **Indebita restituzione dei conferimenti e formazione fittizia del capitale \*\*\***

Relativamente alle attività potenzialmente connesse a tali reati (gestione delle incombenze societarie, operazioni sul capitale, operazioni su azioni o quote, operazioni di conferimento di ramo d'azienda o di conferimenti di beni o crediti, operazioni di trasformazione), i principali controlli si attuano tramite:

- **Obbligo di preventiva informazione al collegio sindacale per ottenere parere preventivo e di segnalazione per iniziative di operazioni su azioni o quote:** esistono regole e procedure che obbligano le Funzioni Aziendali coinvolte in questo tipo di attività ad informare preventivamente il Collegio Sindacale che, a sua volta, dovrà esprimere un parere preventivo, oltre a segnalare agli organi competenti la tipologia dell'operazione.

- **Disposizioni aziendali dirette al personale:** esistono disposizioni aziendali dirette al personale coinvolto nella predisposizione di documenti per le delibere del Consiglio d'Amministrazione in merito ad acconti su dividendi, conferimenti, fusioni e scissioni.

### **Illegale ripartizione degli utili e delle riserve\*\*\***

Relativamente alle attività potenzialmente connesse a tale reato (gestione delle incombenze societarie; redazione, tenuta e conservazione di bilanci, relazioni e altre documentazioni societarie), i principali controlli si attuano tramite:

- **Obbligo di preventiva informazione al collegio sindacale:** esiste l'obbligo di preventiva informazione per l'ottenimento di pareri preventivi o, quanto meno, l'obbligo di segnalazione di iniziative o deliberazioni in merito alla ripartizione degli utili o delle riserve.

- **Disposizioni aziendali concernenti la tenuta e l'archiviazione del bilancio e dei prospetti su operazioni straordinarie:** esistono disposizioni aziendali dirette al personale coinvolto nell'archiviazione e nella tenuta del bilancio e dei prospetti su operazioni straordinarie nonché procedure volte ad assicurare la tracciabilità dell' "iter" procedurale.

\*\*\* In funzione di prevenzione è previsto inoltre l'obbligo

a) per tutte le Direzioni di apporre in calce agli allegati alle situazioni contabili sottoposte al C.d.A. per l'approvazione di qualsiasi tipo di situazioni economiche o patrimoniali e del progetto di bilancio attestazioni di correttezza ed adeguatezza delle appostazioni contabili ed accantonamenti proposti;

b) l'effettuazione di almeno due riunioni tra la società di revisione, il collegio sindacale e l'Organismo di Vigilanza prima delle sedute del Consiglio di Amministrazione dedicate all'approvazione dei conti al 30 giugno ed al 31 dicembre di ogni anno, che abbiano per oggetto la valutazione di eventuali criticità emerse nello svolgimento delle rispettive attività.

### **Illecite operazioni sulle azioni o quote sociali o della società controllante e operazioni in pregiudizio dei creditori**

Relativamente alle attività potenzialmente connesse a tali reati, i principali controlli si attuano tramite:

- **Disposizioni aziendali dirette al personale:** esistono disposizioni aziendali dirette al personale coinvolto nella predisposizione di documenti per le delibere del Consiglio d'Amministrazione in merito ad acconti su dividendi, conferimenti, fusioni e scissioni.
- **Disposizioni aziendali concernenti la tenuta e l'archiviazione del bilancio e dei prospetti su operazioni straordinarie:** esistono disposizioni aziendali dirette al personale coinvolto nell'archiviazione e nella tenuta del bilancio e dei prospetti su operazioni straordinarie nonché procedure volte ad assicurare la tracciabilità dell'iter procedurale.

### **Omissa comunicazione del conflitto d'interessi**

La legge punisce i soggetti i quali, svolgendo funzioni di amministrazione di certe società, tra cui quelle bancarie, omettono di comunicare un proprio interesse in conflitto con quello della società e, nel caso di amministratore delegato, di astenersi dal compiere l'operazione relativamente alla quale sussiste il conflitto.

Gli standard di controllo consistono in procedure formalizzate che impongono la periodica rilevazione delle cariche societarie rivestite e dei rapporti di controllo e di collegamento intrattenuti dagli amministratori e che disciplinano la verbalizzazione di ogni dichiarazione d'interesse, per conto proprio o di terzi, resa dagli amministratori.

### **Illecita influenza sull'assemblea**

Relativamente alle attività potenzialmente connesse al reato di illecita influenza sull'assemblea (attività di preparazione delle riunioni assembleari, attività di rilevanza societaria e adempimento di oneri societari, contatti con soci, contatti con organi di stampa), i principali controlli si attuano tramite:

- **Obblighi informativi:** esistono disposizioni aziendali formalizzate che identificano ruoli e responsabilità, relativamente agli obblighi informativi della Società (nei confronti di Consob e Borsa) con riferimento alla stipulazione di patti parasociali, obblighi di norma assolti direttamente dalla Controllante.
- **Regolamento assembleare:** la Banca è dotata di un regolamento assembleare, adeguatamente diffuso agli azionisti.
- **Regole per l'esercizio del diritto di voto:** sono definite regole formalizzate per il controllo dell'esercizio del diritto di voto e per il controllo della raccolta e dell'esercizio delle deleghe di voto.
- **Gestione del verbale d'assemblea:** esistono disposizioni aziendali chiare e formalizzate che identificano ruoli e responsabilità, relativamente alla trascrizione, pubblicazione ed archiviazione del verbale d'assemblea.

### **Aggiotaggio**

Relativamente alle attività sensibili potenzialmente connesse a questa fattispecie di reato (predisposizione e comunicazione di notizie/dati verso l'esterno relativi alla Società o ad altre società del Gruppo, operazioni di compravendita di azioni o quote delle società stesse ecc.), i principali controlli si attuano tramite:

- **Formalizzazione/Tracciabilità delle fonti e delle informazioni prodotte:** le fonti e le informazioni prodotte verso l'esterno sono formalizzate e il soggetto responsabile dell'emissione (ovverosia della predisposizione e comunicazione all'esterno) dei comunicati stampa e di elementi informativi similari deve assicurare la tracciabilità delle relative fonti e delle informazioni.
- **Sicurezza informatica:** esistono adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel D.Lgs. n. 196 del 2003 e nelle "best practices" internazionali.
- **Disposizioni aziendali per l'identificazione e diffusione di informazioni "price sensitive":** esistono disposizioni aziendali che contengono le modalità di identificazione delle informazioni "price sensitive" e regolamentano la loro diffusione.
- **Vincoli di confidenzialità delle informazioni rilevanti per dipendenti e consulenti esterni:** esistono vincoli formalizzati (procedure o circolari interne, clausole contrattuali) per il mantenimento della confidenzialità delle informazioni rilevanti di cui dipendenti/consulenti esterni vengano a conoscenza. Tali vincoli prevedono il divieto di diffusione dell'informazione rilevante all'interno o all'esterno della Banca, se non tramite il canale istituzionalmente previsto.
- **Processo di comunicazione all'esterno ed archiviazione delle evidenze:** esistono disposizioni aziendali formalizzate che identificano ruoli e responsabilità per la comunicazione all'esterno e l'archiviazione del documento approvato.
- **Presidi organizzativi specifici atti a garantire la separatezza tra le diverse unità organizzative aziendali.**

#### **Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza**

Relativamente alle attività potenzialmente connesse a tale reato (comunicazioni alle Autorità Pubbliche e gestione dei rapporti con le stesse), i principali controlli si attuano tramite:

- **Obbligo di collaborazione:** esistono direttive che sanciscono obblighi di collaborazione e trasparenza nei rapporti con le Autorità di vigilanza.
- **Formalizzazione/Tracciabilità/Archiviazione e segnalazioni nell'ambito delle attività d'ispezione:** esistono disposizioni aziendali che identificano il soggetto responsabile per la gestione dei rapporti con l'Autorità di vigilanza in caso di ispezioni, appositamente delegato dai vertici aziendali. Tali disposizioni aziendali disciplinano anche le modalità di archiviazione, la tracciabilità delle informazioni fornite, nonché l'obbligo di segnalazione iniziale e di relazione sulla chiusura delle attività.
- **Formalizzazione/Tracciabilità/Archiviazione nelle comunicazioni scritte alle autorità di vigilanza:** il soggetto che redige le comunicazioni scritte alle Autorità di vigilanza deve assicurare la tracciabilità delle relative fonti e degli elementi informativi, nonché l'archiviazione delle relative richieste pervenute.
- **Sicurezza informatica:** esistono adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel D.Lgs. n. 196 del 2003 e nelle "best practices" internazionali.

#### **2.2.4 Controlli preventivi dei reati ed illeciti amministrativi di Market Abuse**

(Normativa aziendale di riferimento: Regolamento relativo agli Obblighi di Comunicazione di cui all'art. 114 TUF, Regolamento Registro Insider e Codice di Comportamento Internal dealing, Regolamentazione in materia di Sicurezza e successive integrazioni e modifiche).

I principi di controllo relativi ai reati e agli illeciti amministrativi di market abuse sono di seguito indicati.

- Formalizzazione / Tracciabilità delle fonti e delle informazioni prodotte: le fonti e le informazioni prodotte verso l'esterno devono essere formalizzate e il soggetto responsabile dell'emissione (ovverosia della predisposizione e comunicazione all'esterno) dei comunicati stampa e di elementi informativi similari deve assicurare la tracciabilità delle relative fonti e delle informazioni.
- Sicurezza informatica: devono esistere adeguate misure di sicurezza per il trattamento informatico dei dati, quali quelle contenute nel D.Lgs. n. 196 del 2003 e nelle "best practices" internazionali.
- Disposizioni aziendali per l'identificazione e diffusione di informazioni "price sensitive": esistono disposizioni aziendali che contengono le modalità di identificazione delle informazioni "price sensitive" e regolamentano la loro diffusione.
- Vincoli di confidenzialità delle informazioni rilevanti per Dipendenti e Consulenti esterni: esistono vincoli formalizzati (procedure emesse o emanate o circolari interne, clausole contrattuali) per il mantenimento della confidenzialità delle informazioni rilevanti di cui Dipendenti/Consulenti esterni vengano a conoscenza. Tali vincoli prevedono il divieto di diffusione dell'informazione rilevante all'interno o all'esterno della Banca, se non tramite il canale istituzionalmente previsto.
- Processo di comunicazione all'esterno ed archiviazione delle evidenze: esistono disposizioni aziendali formalizzate che identificano ruoli e responsabilità per la comunicazione all'esterno e l'archiviazione del documento approvato.
- Separatezza tra le diverse unità organizzative aziendali: esistono specifici presidi organizzativi atti a garantire tale separatezza.

I presidi relativi all'abuso di informazioni privilegiate e manipolazione di mercato possono essere così sintetizzati :

- presidi relativi alla disciplina delle informazioni su eventi e circostanze rilevanti (ad esempio, Codice di Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi art. 114 TUF);
- presidi relativi alla identificazione dei soggetti rilevanti che hanno effettuato operazioni e relativi adempimenti agli obblighi di comunicazione. (ad esempio, Codice di Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi art. 114 TUF);
- presidi relativi alla disciplina dei tempi e delle modalità di trasmissione delle comunicazioni alla Consob, alla Società e al Pubblico. (ad esempio, Codice di Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi art. 114 TUF);
- presidi relativi all'individuazione del soggetto preposto al ricevimento, gestione e diffusione delle informazioni (ad esempio, Codice di Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi art. 114 TUF);
- presidi relativi alla disciplina delle operazioni compiute, da soggetti rilevanti oggetto dell'obbligo di comunicazioni, durante il c.d. *Black Out Periods*, ossia 30

- gg. precedenti riunioni del Consiglio d'Amministrazione e 30 gg. precedenti eventuali assemblee straordinarie/ordinarie (ad esempio, Codice di Comportamento Internal Dealing);
- presidi relativi alla previsione di sanzioni pecuniarie per mancata comunicazione (ad esempio, Codice di Comportamento Internal Dealing e Regolamento Concernente gli Obblighi di comunicazione ai sensi art. 114 TUF);
  - presidi relativi all'istituzione di un apposito Registro delle persone che hanno accesso a informazioni privilegiate e alla disciplina dello stesso Registro; in particolare: alimentazione del registro, tipologia delle informazioni, comunicazioni agli interessati, criteri di gestione del registro, modalità di tenuta, aggiornamento, ricerca dati nel registro, conservazione della documentazione e del registro, direttive e procedure sulla circolazione delle informazioni, divieti imposti ai soggetti iscritti nel registro, coordinamento con registri terzi (ad esempio, Regolamento di Gruppo BPM concernente il Registro degli Insider ai sensi dell'art. 115 bis TUF);
  - presidi relativi alla previsione dell'obbligo di riservatezza sulle informazioni privilegiate e procedure idonee alla gestione delle informazioni riservate (ad esempio, Regolamento di Gruppo BPM concernente il Registro degli Insider ai sensi dell'art. 115 bis TUF e Codice Etico);
  - presidi relativi alla gestione dei rapporti con la stampa e dell'attività di comunicazioni esterna è affidata ad apposite funzioni dedicate, secondo le modalità previste dall'Ordinamento Generale d'Istituto (in particolare, l'Ordinamento Funzionale);
  - presidi relativi alla definizione e attuazione delle politiche di gestione e di incentivazione del personale appartenente a tutti i livelli aziendali sono realizzate e attuate in modo da non generare l'erroneo convincimento che il raggiungimento di determinati standard di produttività sia di per sé, indipendentemente dalle concrete modalità seguite, oggetto di valutazione positiva da parte della Banca (ad esempio, Codice Etico e Codice di Comportamento del Settore Bancario e Finanziario);
  - direttive e procedure sulla circolazione delle informazioni (ad esempio, Regolamento Registro degli "Insider");
  - presidi relativi al rispetto dei principi di correttezza, trasparenza e veridicità dei dati forniti al mercato e/o ai clienti, sia con riferimento a quelli direttamente attinenti alla Banca, sia a quelli diffusi, con la consulenza o comunque l'ausilio della Banca;
  - presidi relativi al rispetto dei principi di correttezza, adeguatezza, trasparenza e veridicità con riferimento ai comportamenti posti in essere dalla Banca nei confronti dei clienti (ad esempio, la Modulistica, la contrattualistica e circolari interne banca);
  - presidi relativi alla cura della veridicità, della completezza informativa e dell'aggiornamento del sito, con particolare riguardo ai suoi contenuti finanziari. (ad esempio, Modulistica, contrattualistica e circolari interne banca);
  - presidi relativi all'organizzazione dei contenuti del sito in modo coerente e chiaro, privilegiando l'aspetto della fruibilità e della facilità di accesso da parte dell'utente. (ad esempio, Direttive e procedure sulla circolazione delle informazioni del Regolamento Registro degli "Insider" ).

Quanto previsto in argomento risulta, inoltre, coordinato agli adempimenti connessi alla procedura di gestione della "Insider's list".

## **2.2.5 Controlli preventivi dei reati aventi finalità di terrorismo o di eversione dell'ordine democratico e dei delitti contro la personalità individuale**

(Normativa aziendale di riferimento: regolamenti e circolari normative di settore)

La prevenzione dei reati aventi finalità di terrorismo o di eversione dell'ordine democratico e di quelli contro la personalità individuale si fonda innanzitutto sul rispetto da parte della banca delle norme dettate per gli intermediari dalla Banca d'Italia, dalla Consob e dall'Ufficio Italiano dei Cambi in materia di antiriciclaggio e di segnalazione di operazioni finanziarie sospette.

In proposito si ricorda che profili di rischio rilevanti con riferimento a tutti i reati in oggetto possono ravvisarsi anche solo nei casi in cui il soggetto in posizione apicale o dipendente agisca in concorso con soggetti terzi (salvo che per le pratiche di mutilazione degli organi genitali femminili, in cui si richiede anche che il reato sia commesso all'interno di una struttura BdL). <sup>(1)</sup>

Inoltre, anche ai fini della prevenzione di tali reati BdL si avvale degli "standards" di controllo già esaminati con riguardo a tutte le categorie di reati.

Con riferimento ai reati in considerazione, tali controlli riguarderanno essenzialmente la fase di istruttoria relativa alla valutazione dei clienti della Banca – italiani e soprattutto stranieri – e delle attività da essi svolte.

A tali controlli, di carattere generale, si aggiungono dei controlli specifici, relativi ai reati in esame, ed in particolare:

- Procedure formalizzate di istruttoria per la valutazione dei clienti e delle attività da essi svolte in Italia e all'estero, anche avvalendosi di elenchi di nominativi di soggetti segnalati essere coinvolti (o potenzialmente coinvolti) in attività terroristiche.
- Relativamente alle operazioni di finanziamento, controlli sui soggetti che gestiscono l'attività di riferimento, in particolare attraverso:

- a) identificazione dei soggetti che svolgono materialmente l'attività istruttoria e del soggetto che autorizza l'operazione con il cliente;
- b) formalizzazione e tracciabilità delle attività svolte;
- c) predisposizione di un'informativa di riepilogo da inviare sia ai superiori gerarchici sia ai responsabili del controllo di primo livello nonché, in versione sintetica e standardizzata, alla Direzione Controlli;
- d) registrazione delle operazioni come da procedure aziendali;
- e) controlli specifici ulteriori, istituiti in ottemperanza alla normativa antiriciclaggio (attraverso l'uso, fra l'altro, di check-list nonché di procedure informatiche volte ad evidenziare operazioni sospette).

-----  
*(1) Affinché possa configurarsi un concorso dei soggetti in posizione apicale o dipendenti nel reato, è necessario che tale condotta si risolva – quanto meno – in un'agevolazione del fatto delittuoso dell'autore e che l'operatore sia a conoscenza della finalità illecita che il cliente persegue. E' evidente che la forma di concorso che presenta maggiori profili di*

*rischio per i soggetti in posizione apicale o dipendenti è quella connessa al finanziamento di soggetti che pongano in essere reati connessi alla tratta di persone o alla pedo-pornografia. Si rammenta infine che, affinché sussista la possibilità di imputare l'illecito alla banca, è necessario che il reato sia stato commesso nell'interesse o a vantaggio della banca medesima e non semplicemente avvalendosi della sua struttura per il perseguimento di profitto riferibile esclusivamente al soggetto attivo.*

## **2.2.6 Controlli preventivi dei reati transnazionali**

(Normativa aziendale di riferimento : circolare normativa)

Con riferimento a tali reati, i controlli riguardano prevalentemente la fase di istruttoria relativa alla valutazione dei clienti della Banca e le attività da essi svolte anche eventualmente nel prosieguo del rapporto, mentre in particolare per i reati di intralcio alla giustizia si ha riguardo alle attività della Banca relative ai contenziosi giudiziari e alle comunicazioni di informazioni richieste dall'Autorità giudiziaria.

## **2.2.7 Controlli preventivi dei reati relativi alla tutela della salute e della sicurezza sul lavoro**

(Normativa aziendale di riferimento: regolamenti e circolari normative di settore)

La prevenzione dei 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 si fonda innanzitutto sul rispetto da parte della banca delle norme di legge in materia.

In ottemperanza al D. Lgs. 19 settembre 1994 n. 626 e successive modificazioni, la banca ha istituito i previsti presidi (Responsabile del servizio di prevenzione e protezione, Rappresentante aziendale per la sicurezza, Medico competente, lavoratori incaricati, nell'ambito di tutte le unità operative, dell'attuazione delle misure di prevenzione incendi, di evacuazione in caso di pericolo e di pronto soccorso; i lavoratori hanno inoltre provveduto all'elezione dei Rappresentanti per la sicurezza, nell'ambito delle Rappresentanze Sindacali Aziendali).

La banca si è inoltre adeguata alle prescrizioni in tema di sicurezza e di salute sui luoghi di lavoro, adottando le previste misure generali di tutela.

La Legge n. 123 del 2007 ha modificato ed ampliato i contenuti del comma 3 all'articolo 7 del D.Lgs. n. 626 del 1994, relativamente al regime degli appalti, introducendo i seguenti obblighi :

- cooperazione e coordinamento con l'impresa appaltatrice o lavoratore autonomo;
- elaborazione di un unico documento di valutazione dei rischi indicante le misure adottate per eliminare le interferenze (da allegare al contratto di appalto);
- indicazione dei costi relativi alla sicurezza del lavoro nei contratti di somministrazione, di appalto e di subappalto.

Allo scopo la banca, in qualità di committente, deve concordare con il commissionario la stesura di un Documento di Valutazione Rischi Coordinato (DVRC) contenente valutazioni "coordinate" circa l'analisi dei rischi, la metodologia e le misure adottate per

eliminare le situazioni interferenziali tra le imprese vincolate dall'appalto ed i lavoratori presenti nelle unità interessate.

Obiettivo del nuovo art. 7 comma 3 del citato Decreto è senza dubbio il mantenimento del livello accettabile di rischio residuo insito in ogni ambiente di lavoro, affinché ogni altra condizione aggiuntiva non comporti una matematica sommatoria di rischi, bensì un'attenta e più efficace programmazione degli interventi e delle modalità di somministrazione delle prestazioni offerte.

Al momento della stipula del contratto e comunque prima dell'effettivo inizio del rapporto lavorativo con la banca la ditta fornitrice deve presentare un'idonea documentazione relativa alla formazione ed informazione del proprio personale in merito alle mansioni da svolgere ed alle procedure di sicurezza adottate in relazione alla tipologia di attività richiesta.

Conseguentemente, la ditta fornitrice deve presentare una prima stesura del Documento di Valutazione Rischi Coordinato, riferito all'intervento specifico, contenente le mansioni svolte dalla ditta, le situazioni di interferenza, qualora siano oggettivamente riscontrabili, l'eventuale confinamento delle lavorazioni, al fine di evitare danni o creare situazioni di pericolo al personale della banca alterando le condizioni di sicurezza presenti presso le infrastrutture della banca.

La stesura definitiva del DVCR avviene poi di concerto con le persone designate allo scopo dalla banca, nel rispetto delle disposizioni interne in materia di prevenzione e sicurezza degli ambienti di lavoro (i dipendenti delle aziende fornitrici devono attenersi scrupolosamente alle direttive della banca in tema di primo intervento in caso di incendio, piani di evacuazione, uscite di sicurezza e relativi percorsi espressamente segnalati, osservando le istruzioni impartite dal personale della banca all'uopo incaricato).

Nel "regolamento di sicurezza", facente parte dell'Ordinamento Generale di Istituto, sono contemplate le norme generali in materia atte a salvaguardare e proteggere il patrimonio aziendale (risorse umane e materiali), individuando inoltre le strutture preposte a tale compito (di coordinamento, operative, di controllo), nonché le competenze e le responsabilità di ciascuna di esse. L'azione congiunta delle richiamate strutture costituisce il presupposto per la prevenzione e la limitazione dei rischi connessi all'attività della banca, sia sotto il profilo della sicurezza sul lavoro che della tutela della salute, ai quali devono peraltro concorrere tutte le unità operative ed i dipendenti, ai quali è affidato un ruolo attivo e propositivo.

Il sistema dei controlli interno prevede inoltre l'effettuazione di verifiche periodiche specifiche (osservanza delle misure di sicurezza, attivazione degli impianti di allarme secondo le disposizioni, regolare approvvigionamento degli armadietti di pronto soccorso, posizionamento degli estintori ecc.).

Ai controlli interni si aggiungono quelli esperiti periodicamente dal Responsabile del Servizio di prevenzione e protezione e del Medico incaricato.

La Direzione Personale provvede infine agli aspetti formativi e propone annualmente un questionario relativo all'utilizzo del video-terminale, predisponendo i conseguenti controlli sanitari ove previsto.

## **2.2.8 Controlli preventivi dei reati di ricettazione, riciclaggio e impiego di danaro, beni o utilità di provenienza illecita**

(Normativa aziendale di riferimento : regolamenti e circolari normative di settore)

Il Decreto Legislativo 21 novembre 2007, n. 231, di attuazione della terza Direttiva Antiriciclaggio, costituisce il provvedimento di revisione globale delle misure di contrasto al fenomeno di riciclaggio ed introduce nel corpo del D.Lgs. 231/2001 l'art. 25 octies, che estende la responsabilità amministrativa degli enti ai reati in argomento.

Le rilevanti novità introdotte dalla nuova disciplina riguardano :

- le nozioni stesse di riciclaggio, autoriciclaggio, transazioni sospette e finanziamento del terrorismo, che nel Decreto sono alla base delle segnalazioni e degli approfondimenti sia sul piano giuridico che su quello operativo;
- i nuovi criteri dettati, soprattutto in tema di obblighi di adeguata verifica della clientela in funzione del rischio associato al tipo di cliente, al rapporto d'affari, al prodotto o transazione, come pure con riguardo alle peculiarità delle professioni giuridiche, economiche e degli operatori non finanziari;
- le nuove misure di prevenzione d'ordine patrimoniale e la connessa tematica della tassazione dei proventi derivanti da attività illecite;
- i nuovi organi preposti al controllo dei flussi finanziari e all'analisi delle transazioni;
- i riflessi delle nuove misure sul piano penale.

Come per i reati aventi finalità di terrorismo o di eversione dell'ordine democratico e transnazionali, la prevenzione dei reati di riciclaggio si fonda innanzitutto sul rispetto, da parte della banca delle norme di legge in materia di antiriciclaggio e di segnalazione di operazioni finanziarie sospette.

Ai fini della prevenzione dei suddetti reati BdL si avvale degli "standards" di controllo già esaminati con riguardo a tutte le categorie di reati.

Ai controlli di carattere generale si aggiungono i medesimi controlli specifici previsti per i già citati reati con finalità di terrorismo o eversione dell'ordine democratico e transnazionali.

Ad integrazione dei richiamati controlli specifici, il D.Lgs. n. 231/2007 ha imposto alle banche l'obbligo di raccogliere alcune informazioni aggiuntive sulla propria clientela, al fine di valutarne in maniera più efficace il rischio di riciclaggio, disponendo l'applicazione di precise sanzioni nel caso di inottemperanza a tale obbligo.

Le informazioni aggiuntive richieste devono essere fornite direttamente dai clienti, sotto la propria responsabilità, attraverso la compilazione del "Modulo per l'identificazione e l'adeguata verifica della clientela" nel quale vengono evidenziati i seguenti ulteriori elementi :

- scopo e natura prevista del rapporto continuativo;
- identificazione del titolare effettivo;
- struttura di proprietà e di controllo del cliente.

Lo stesso Modulo deve essere compilato e sottoscritto (da clienti e non) all'atto dell'effettuazione di operazioni per cassa di importo pari o superiore a 5.000 Euro.

L'eventuale rifiuto da parte del cliente di fornire alla banca le informazioni aggiuntive previste comporta l'impossibilità di procedere all'apertura di un rapporto continuativo e/o all'esecuzione di operazioni per cassa di importo pari o superiore a 5.000 Euro.

L'operatore bancario (soggetto in posizione apicale o dipendente) può rispondere del reato di riciclaggio soltanto nell'ipotesi in cui abbia la consapevolezza della provenienza delittuosa dei beni oggetto dell'operazione di trasferimento o comunque di immissione nel circuito economico. Diversamente, le condotte di omessa adeguata verifica della clientela, omessa registrazione delle relative informazioni e omessa comunicazione, ove

non sorrette da tale atteggiamento soggettivo, saranno sanzionate a norma dell'art. 55 del D.Lgs. n. 231/2007 e la loro eventuale integrazione da parte dell'operatore bancario, ancorchè, in ipotesi, nell'interesse o vantaggio della banca, non potrà comportare il sorgere della concorrente responsabilità amministrativa dell'ente ai sensi del D.Lgs. n. 231/2001, non essendo detti reati ricompresi nell'elencazione dei cosiddetti reati presupposti a norma degli art. 24 e ss. .

Per ciò che concerne il reato di ricettazione, è fatto divieto di intrattenere rapporti commerciali con soggetti (persone fisiche o giuridiche) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della legalità.

A ciò si aggiunge un'attenta gestione dei rapporti con i fornitori, aggiornando il relativo "portafoglio acquisti" (fornitori/prodotti e servizi) e curandone la valutazione nell'ambito di una lista gestita dalla funzione che si occupa degli acquisti, secondo principi e criteri oggettivi (che comprendono sia requisiti tecnici sia requisiti di immagine), nonché acquisendo e archiviando correttamente la documentazione amministrativa di riferimento, al fine di garantire la trasparenza degli accordi.

Peraltro, la gestione dei suddetti rapporti commerciali presuppone gli interventi degli Enti Responsabili di Spesa, chiamati a definire requisiti e specifiche tecniche del bene/servizio richiesto e della funzione che si occupa degli acquisti per le fasi di negoziazione (intesa come mezzo per ottenere l'adeguamento del fornitore alle esigenze dell'azienda attraverso le condizioni più favorevoli in termini di prezzo, qualità, servizio e clausole contrattuali) e di emissione degli ordini.

La fase di analisi/scelta del fornitore, infine, viene di solito svolta congiuntamente dalle due suddette funzioni.

### **2.2.9 Controlli preventivi dei reati informatici**

(Normativa aziendale di riferimento : Ordinamento Generale d'Istituto Banca Popolare di Milano, regolamenti e circolari interne)

La legge 18 marzo 2008 n. 48 reca la ratifica e l'esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica e le norme di adeguamento dell'ordinamento interno, prevedendo l'introduzione nel novero dei reati presupposto di cui al D.Lgs. 8 giugno 2001, n. 231 dell'art. 24-bis recante la previsione di nuove fattispecie di illecito amministrativo commesse in dipendenza di delitti informatici e trattamento illecito di dati.

Il contratto di conduzione informatica sottoscritto tra Banca di Legnano e Banca Popolare di Milano stabilisce le funzioni che la D.I.C.T.O. (Direzione Information Communication Technology e Operations) della Capogruppo svolge per conto di BdL.

Il Regolamento di Sicurezza di BdL specifica le funzioni assegnate alla D.I.C.T.O. e precisamente :

- la responsabilità dell'attuazione di tutti gli interventi necessari ad assicurare la riservatezza, l'integrità e la disponibilità del patrimonio informatico della Banca e di tutto il software;
- lo studio, la definizione e l'attuazione degli standard tecnici e operativi in tema di protezione del patrimonio informatico della Banca;

- l'effettuazione delle attività di controllo e monitoraggio finalizzate alla rilevazione di eventuali anomalie nel rispetto delle regole di sicurezza logica;
- l'attuazione dei piani per la garanzia di continuità degli impianti di elaborazione dati (Disaster Recovery) e telecomunicazione, con esclusione degli aspetti impiantistici relativi all'alimentazione elettrica ed al condizionamento.

Il medesimo Regolamento, sulla scorta dell'omologa fonte normativa della Capogruppo, stabilisce inoltre i principi generali di accesso e di utilizzo del sistema informatico aziendale.

Le entità di riferimento, vale a dire quelle coinvolte nel processo di sicurezza logica del sistema informatico aziendale, sono :

- le risorse logiche (oggetti), che costituiscono l'insieme delle diverse e numerose informazioni gestite dai sistemi e rappresentano l'entità passiva dell'accesso che può essere acquisita e modificata dai soggetti che ne posseggono i diritti;
- gli utenti (soggetti), ossia tutti coloro che accedono a vario titolo alle diverse risorse logiche dei sistemi e rappresentano l'entità attiva dell'accesso, in grado di esercitare sugli oggetti i diritti che possiede;
- le modalità di accesso, ossia l'insieme delle azioni che un soggetto è autorizzato ad eseguire su un singolo o un insieme di oggetti e nell'ambito di predeterminati vincoli temporali, spaziali e di contesto in cui opera il sistema.

Le modalità di accesso degli utenti alle risorse sono regolamentate da un sistema di autorizzazioni che prevede :

- l'accesso al sistema informatico è consentito solo alle persone autorizzate;
- l'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento della propria attività lavorativa;
- il sistema deve identificare e autenticare individualmente gli utenti; identificazione ed autenticazione devono avvenire prima di tutte le altre interazioni tra il sistema e l'utente.

Il meccanismo di identificazione ed autenticazione in uso è rappresentato dall'assegnazione agli utenti di un codice identificativo (UserID), che si identifica con la matricola, e di una parola chiave segreta (Password) eventualmente integrate da informazioni aggiuntive necessarie ad identificare l'utente in particolari condizioni di accesso al sistema (es.: numero telefonico di chiamata).

La password è personale e non può essere comunicata a terzi; il codice identificativo attribuisce in modo univoco la paternità delle operazioni eseguite.

La funzione autorizzativa è demandata al responsabile dell'unità operativa di cui l'utente fa parte.

La gestione e la conservazione delle password sono inoltre regolamentate da apposite disposizioni interne.

Analogo meccanismo di identificazione ed autenticazione è utilizzato per autorizzare l'accesso temporaneo al sistema da parte di personale esterno, al quale è fatto espresso divieto di copiare dati e programmi di proprietà della Banca, di installare ed utilizzare sulle stazioni di lavoro prodotti software senza la preventiva specifica autorizzazione della Banca e di utilizzare le risorse del Sistema Informatico della Banca per scopi diversi da quelli espressamente previsti nel contratto di collaborazione.

Per quanto riguarda la gestione degli autenticator per reti interbancarie, oltre al rispetto delle normative derivanti da specifici accordi, si procede in modo tale da evitare la concentrazione in un unico soggetto di informazioni/autorizzazioni necessarie all'effettuazione di trasferimento fondi su reti informatiche.

Sono infine regolamentati anche gli accessi fisici ai locali che ospitano gli elaboratori centrali e i log di accesso ai sistemi sono registrati e conservati.

La Direzione Internal Auditing della Capogruppo, per il tramite dell'Area Auditing I.T.- Settore I.C.T. Audit, garantisce l'effettuazione di controlli finalizzati ad accertare l'adeguatezza e il rispetto delle misure di sicurezza fisica e logica predisposte per la salvaguardia del patrimonio informatico, nonché dei suoi requisiti tecnici e funzionali, fornendo inoltre consulenza tecnica sulla sicurezza anche alle altre Società del Gruppo. I servizi prestati attraverso Reti Telematiche sono affidati ad apposita società di servizi del Gruppo ([We@Service Spa](#)) che ha il compito di sviluppare la piattaforma informatica Internet della divisione [We@Bank](#). I livelli di sicurezza sono garantiti da sofisticati meccanismi di assegnazione e gestione delle password di accesso e da specifiche linee guida per la sicurezza nell'impiego dell'eventuale firma elettronica/digitale. Il sistema dei controlli sull'attività della predetta società è stato organizzato in relazione alle aree funzionali in essa individuate (strategie di business e indirizzi di marketing, rischio tecnologico, area societaria e contabilità amministrazione).

Per quanto riguarda infine i rischi di frode esterna derivante da clonazione di carte di credito/debito, sono state diramate istruzioni relative al costante monitoraggio delle apparecchiature ai fini della tempestiva rilevazione di manomissioni e dell'avvio delle conseguenti procedure di allarme; è inoltre prevista un'attività di quotidiana verifica dei movimenti che transitano sui rapporti a seguito dell'utilizzo delle carte (attività denominata "Presidio Monetica"), al fine di limitare/evitare il perpetrarsi di azioni fraudolente a danno della clientela, tramite l'immediato blocco e la cattura delle carte sospette di clonazione sul circuito nazionale ed estero.

### **Art. 3 - Normativa e documentazione aziendale di riferimento**

- **Ordinamento Generale d'Istituto**, costituito dalla regolamentazione interna *pro tempore* vigente disciplinante, in particolare: l'assetto direzionale dell'Istituto, l'ordinamento funzionale, i profili di ruolo della rete commerciale, i comitati, i fidi, i poteri delegati relativi ai fidi e alle disposizioni applicative, la finanza e le disposizioni applicative, la deontologia dell'attività in cambi, la deontologia dell'attività in titoli, il codice di comportamento del settore bancario e finanziario, il modello di controllo, la cassa e custodia valori, la sicurezza e disposizioni applicative, il telex-swift e la rete nazionale interbancaria, la beneficenza, i budget di spesa e degli acquisti e poteri delegati, i poteri delegati (poteri di firma, poteri di pricing), il personale, il trattamento dei dati personali e le disposizioni applicative, il gruppo BPM e le disposizioni applicative, le operazioni "significative" e con parti correlate, il registro degli insider ai sensi dell'art.115 bis TUF e gli obblighi di comunicazione ai sensi dell'art. 114 TUF.
- **Normativa Aziendale** costituita dalla regolamentazione interna *pro tempore* vigente, in particolare in materia di amministrazione e contabilità, commerciale, credito, estero, finanza information technology, legale, personale, servizi generale, sistemi di pagamento.
- **Codice Etico.**
- **Reportistica prodotta dal "repository" organizzativo aziendale istituito dalla Capogruppo.**

## **Art. 4 - Organismo di Vigilanza**

### **Art. 4.1 - Individuazione e compiti dell'Organismo di Vigilanza**

Il Decreto Legge 231/01, all'art. 6, indica come condizione per l'esenzione dalla responsabilità amministrativa dell'ente, l'affidamento del compito di vigilare sul funzionamento e sull'osservanza del Modello Organizzativo nonché di curarne l'aggiornamento, ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

L'Organismo di Vigilanza è costituito ai sensi e per gli effetti del Decreto ed è dotato di pieni ed autonomi poteri di iniziativa e di controllo sulle attività della Banca.

L'Organismo di Vigilanza, nell'esecuzione della sua attività ordinaria, vigila, attraverso le funzioni della Banca interessate, tra l'altro:

- sull'osservanza del Modello da parte delle strutture interessate della Banca e sul relativo aggiornamento;
- sull'effettiva efficacia e capacità dei processi operativi e della rispettiva normativa in relazione alla struttura aziendale e al contesto di riferimento, di prevenire comportamenti illeciti;
- sull'opportunità di aggiornamento del Modello e dei processi di controllo, proponendo al Consiglio di Amministrazione tramite il Direttore Generale e le funzioni interessate, sulla base di verifiche e laddove se ne riscontri l'esigenza, le modifiche o integrazioni eventualmente necessarie in conseguenza di:
  - significative violazioni delle prescrizioni del Modello;
  - significative modificazioni dell'assetto interno della Banca e/o delle modalità di svolgimento delle attività d'impresa;
- sull'effettiva formazione del personale con riguardo al Modello, alle procedure, al Decreto e alla normativa da questo richiamata.

Con riferimento all'attività di aggiornamento del Modello, essendo lo stesso un "atto di emanazione dell'organo dirigente" (in conformità alle prescrizioni dell'art. 6, co. 1, lett. a) del Decreto) le successive modifiche e integrazioni di carattere sostanziale del Modello stesso sono rimesse alla competenza del Consiglio di Amministrazione della Banca.

E' tuttavia riconosciuta al Direttore Generale, autonomamente o su impulso dell'Organismo di vigilanza, la possibilità di effettuare eventuali integrazioni delle Aree a Rischio, nonché la facoltà di apportare al Modello eventuali modifiche o integrazioni di carattere non sostanziale quali ad esempio aggiornamenti normativi (come, fra l'altro, modifiche formali alle rubriche dei reati previsti dal decreto), denominazioni di società o funzioni o cambiamento di ruoli di funzioni.

Tali facoltà si ritengono giustificate in virtù della necessità di garantire un costante e tempestivo adeguamento del Modello ai sopravvenuti mutamenti della normativa o di natura operativa e/o organizzativa all'interno della Banca.

Le proposte di modifica ed integrazione del Modello, in applicazione anche di quelle apportate dalla Capogruppo e da questa comunicate, potranno essere presentate

dall'Organismo di Vigilanza della Banca ai suddetti organi sociali, sentite le competenti funzioni aziendali.

Le suddette variazioni dovranno essere sottoposte annualmente al Consiglio di Amministrazione della Banca che potrà procedere con la successiva attività di ratifica.

L'Organismo di Vigilanza, in particolare, ha il compito di:

- assicurare una costante ed indipendente azione di sorveglianza sul regolare andamento dell'operatività e dei processi della Banca, al fine di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose ai sensi del Decreto, attraverso la valutazione della funzionalità del complessivo sistema dei controlli interni e la sua idoneità a garantire l'efficacia e l'efficienza dei processi aziendali di controllo rilevanti nonché la conformità delle operazioni sia alle politiche stabilite dagli organi di governo aziendali sia alle normative interne ed esterne;
- curare l'aggiornamento del Modello e delle regole e dei principi organizzativi in esso contenuti o richiamati laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative e formulare osservazioni e suggerimenti in proposito con le modalità di segnalazione innanzi definite, verificando l'attuazione ed efficacia delle soluzioni proposte;
- segnalare alle funzioni della Banca competenti le situazioni nelle quali è opportuno o necessario instaurare gli adeguati procedimenti disciplinari, ai sensi di legge e di contratto collettivo applicabile, idonei a sanzionare il mancato rispetto delle misure indicate nei modelli di organizzazione, gestione e controllo e nel Codice Etico;
- predisporre, tramite le funzioni Banca competenti, un efficace sistema di comunicazione interna che, garantendo la massima riservatezza e tutela del segnalante, permetta a tutti coloro che vengano a conoscenza di situazioni illecite, nonché di situazioni non conformi al Modello di organizzazione, gestione e controllo ed al Codice Etico adottati, di segnalare all'Organismo di Vigilanza ogni notizia rilevante ai fini del Decreto quali, a titolo esemplificativo, ma non esaustivo, quelle emergenti da:
  - risultanze dell'attività di controllo (attività di monitoraggio, report riepilogativi, indici consuntivi);
  - anomalie o tipicità riscontrate nello svolgimento delle varie attività;
  - decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
  - richieste di assistenza legale inoltrate da dirigenti e/o Dipendenti per procedimenti relativi a reati previsti dal Decreto;
  - provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o altra autorità, dai quali si evince lo svolgimento di indagini, anche nei confronti di ignoti, per reati di cui al Decreto;
  - notizie relative a commesse attribuite da enti pubblici o soggetti che svolgono funzioni di pubblica utilità;
  - modifiche organizzative/procedurali riferibili al Decreto.

A seguito dell'entrata in vigore del D.Lgs. n. 231/2007, recante attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché

della direttiva 2006/70/CE che ne reca misure di esecuzione, l'Organismo di Vigilanza avrà, inoltre, il compito di:

- comunicare, senza ritardo, alle autorità di vigilanza di settore tutti gli atti o i fatti di cui viene a conoscenza nell'esercizio dei propri compiti, che possano costituire una violazione delle disposizioni emanate dalle stesse autorità relativamente alle modalità di adempimento degli obblighi di adeguata verifica del cliente, all'organizzazione, alla registrazione, alle procedure ed ai controlli interni volti a prevenire l'utilizzo della Banca a fini di riciclaggio o di finanziamento del terrorismo;
- comunicare, senza ritardo, al legale rappresentante della banca o a un suo delegato, le infrazioni alle disposizioni relative alle segnalazioni di operazioni sospette di cui abbia notizia;
- comunicare, entro 30 giorni, al Ministero dell'economia e delle finanze le infrazioni relative (i) alle disposizioni sul trasferimento di denaro contante o di libretti di deposito bancari, (ii) all'emissione di assegni bancari o circolari, (iii), al saldo dei libretti di deposito bancario, (iv) e le infrazioni relative al divieto di conti e libretti di risparmio anonimi o con intestazione fittizia di cui abbia notizia;
- comunicare, entro 30 giorni, alla UIF le infrazioni alle disposizioni relative agli obblighi di registrazione di cui abbia notizia.

Nello svolgimento della propria attività di controllo, l'Organismo di Vigilanza si avvale dell'ausilio delle diverse funzioni aziendali interne, tra cui la Direzione Controlli e la Funzione Compliance, che operano seguendo appositi protocolli elaborati e costantemente aggiornati in base alle risultanze dell'analisi dei rischi e degli interventi di audit.

A seguito dell'attività della Direzione Controlli, l'Organismo di Vigilanza analizza il livello dei controlli presenti nell'operatività e nei processi aziendali. I punti di debolezza rilevati sono segnalati ai responsabili delle funzioni aziendali interessate al fine di rendere più efficienti ed efficaci l'applicazione delle regole.

L'Organismo di Vigilanza ha facoltà di chiedere alla Direzione Controlli di inserire nei propri protocolli verifiche specifiche volte, in particolare per le Aree a Rischio, a valutare l'adeguatezza dei controlli a prevenire comportamenti illeciti.

Nell'adempimento della propria funzione l'Organismo di Vigilanza, ha accesso, tramite le funzioni aziendali, a tutte le attività svolte dalla Banca e alla relativa documentazione, inclusi i verbali del Consiglio di Amministrazione. In caso di attribuzione a soggetti terzi di attività rilevanti per il funzionamento del sistema dei controlli interni, l'Organismo di Vigilanza deve poter accedere anche alle attività svolte da tali soggetti.

Al fine di garantire un'autonomia anche finanziaria, all'Organismo di Vigilanza viene attribuito un budget di spesa, su base annua, per l'esercizio delle funzioni di vigilanza, aggiornamento e formazione ad esso attribuite dal Modello in ragione ed in proporzione delle necessità riscontrate. In caso di necessità eccedenti, il Consiglio di Amministrazione porrà a disposizione dell'Organismo di Vigilanza gli importi necessari.

## **Art. 4.2 - Composizione e meccanismi di elezione, sostituzione e sospensione dei componenti**

L'Organismo di Vigilanza è composto da soggetti in grado di assicurarne un adeguato livello di professionalità e continuità di azione, aventi, tra l'altro, il compito di valutare l'adeguatezza del Modello e del Codice Etico adottati dalla Banca, nonché di vigilare sul loro funzionamento ed osservanza, al fine di prevenire la commissione dei reati previsti dal Decreto (e sue successive modifiche ed integrazioni).

L'Organismo di Vigilanza è composto come segue:

- un componente esterno al Gruppo, designato quale Presidente;
- un Consigliere di Amministrazione che non abbia incarichi esecutivi;
- un componente dell'Organismo di Vigilanza della Capogruppo;
- il Direttore Controlli pro-tempore, designato quale Segretario.

Condizione di eleggibilità, per ciascuno dei membri dell'Organismo di Vigilanza, è il possesso dei requisiti di onorabilità stabiliti dall'art. 5 del Regolamento del Ministero dell'Economia e delle Finanze, recante norme per l'individuazione dei requisiti di onorabilità, professionalità e indipendenza degli esponenti aziendali delle banche, adottato con D.M. n. 161 del 18 marzo 1998 e dell'assenza di una delle cause di sospensione disciplinate nell'art. 6 del medesimo Regolamento.

Le ipotesi considerate dall'art. 6 del Regolamento del Ministero dell'Economia e delle Finanze citato costituiscono, altresì, causa di sospensione dalla carica di membro dell'Organismo di Vigilanza.

E' causa d'ineleggibilità ovvero di decadenza dalla carica, l'intervento di sentenza di condanna (o di patteggiamento), pur se non passata in giudicato, per avere commesso uno dei reati di cui al Decreto, ovvero un reato che comporti l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione, anche temporanea, dagli uffici direttivi delle persone giuridiche o delle imprese.

Nel caso in cui uno dei componenti dell'Organismo di Vigilanza venga a trovarsi in una situazione d'incompatibilità con la carica, il Consiglio di Amministrazione procede alla sua sostituzione.

L'Organismo di Vigilanza è funzione permanente.

Il Consiglio di Amministrazione, all'atto di nomina dei componenti dell'Organismo di Vigilanza, determina la durata della carica degli stessi.

In assenza di specifica determinazione, essa, per ciascun componente, si intende coincidente con la durata in carica del Consiglio di Amministrazione che li ha nominati. I componenti dell'Organismo sono immediatamente rieleggibili.

L'eventuale remunerazione spettante ai componenti dell'Organismo è stabilita all'atto della nomina o con successiva decisione del Consiglio di Amministrazione. Ai membri dell'Organismo spetta, in ogni caso, il rimborso delle spese sostenute per le ragioni d'ufficio.

### **Art. 4.3 - Periodicità e modalità di convocazione**

L'Organismo di Vigilanza si riunisce almeno trimestralmente, ma può essere convocato in caso di urgenza da ciascuno dei suoi Componenti.

In linea di principio, l'Organismo di Vigilanza è convocato dal proprio Presidente con preavviso di almeno cinque giorni di calendario (fatti salvi i casi di urgenza, nei quali detto termine è ridotto a due giorni), mediante lettera raccomandata, fax o e-mail contenente l'indicazione della data, del luogo, dell'ora della riunione e del relativo ordine del giorno.

Il Consiglio di Amministrazione, il Direttore Generale, il Collegio Sindacale e il Presidente del Consiglio di Amministrazione hanno la facoltà di convocare in qualsiasi momento l'Organismo di Vigilanza.

### **Art. 4.4 Modalità di svolgimento delle riunioni**

Per la validità delle riunioni dell'Organismo di Vigilanza devono essere presenti almeno due componenti del medesimo.

Le decisioni sono prese a maggioranza assoluta dei componenti presenti.

L'Organismo può tuttavia validamente deliberare anche in assenza di formale convocazione, qualora partecipino alla riunione tutti i suoi Componenti.

Il Segretario dell'Organismo redige i verbali delle riunioni. Ogni verbale è sottoscritto dal Presidente e dal Segretario. Eventuali copie ed estratti dei verbali sono certificati conformi dal Segretario, alla cura del quale è anche affidata la custodia dei verbali.

Il Presidente dà esecuzione alle delibere approvate direttamente o tramite le competenti Funzioni Banca e ne verifica l'effettiva attuazione sulla quale riferisce all'Organismo di Vigilanza.

L'Organismo di Vigilanza ha facoltà, inoltre, di invitare alle proprie riunioni il Direttore Generale e persone estranee che facciano parte o meno della Banca.

Nello svolgimento dei propri compiti l'Organismo può infatti avvalersi di consulenti esterni.

In particolare, potranno presenziare alle riunioni dell'Organismo di Vigilanza Consulenti, tecnici e responsabili delle funzioni centrali e/o periferiche, della Banca o del Gruppo, chiamati a riferire su argomenti di stretta competenza.

Alle riunioni dell'Organismo di Vigilanza devono essere invitati a partecipare il Presidente del Collegio Sindacale, il Presidente del Comitato per il Controllo Interno e il Responsabile della Funzione Compliance; il Collegio e il Comitato possono inoltre designare un proprio Membro a partecipare, in via permanente, alle riunioni dell'Organismo. Il Presidente, contestualmente all'invio dell'avviso di convocazione ai Componenti dell'Organismo, lo trasmette anche ai Presidenti del Collegio Sindacale e del Comitato per il Controllo Interno, nonché al Responsabile della Funzione Compliance, corredato dall'eventuale documentazione a supporto.

Gli incontri con gli Organi ai quali l'Organismo di Vigilanza riferisce devono essere verbalizzati e copie dei verbali devono essere custodite a cura del Segretario, unitamente ai verbali delle riunioni dell'Organismo stesso.

#### **Art. 4.5 - Flussi informativi verso l'Organismo di Vigilanza**

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte dei Dipendenti, degli organi societari e dei Collaboratori Esterni in merito ad eventi che potrebbero ingenerare responsabilità della Banca ai sensi del Decreto.

Valgono al riguardo le seguenti prescrizioni di carattere generale:

- i Dipendenti e gli organi societari devono segnalare all'Organismo di Vigilanza le notizie relative alla commissione, o alla ragionevole convinzione di commissione, dei reati contemplati dal Decreto, nonché le notizie relative alle ipotesi di violazioni delle regole di comportamento o procedurali contenute nel Modello;
- i Collaboratori Esterni sono tenuti ad effettuare le segnalazioni con le modalità e nei limiti previsti contrattualmente;
- le segnalazioni devono essere fatte dai Dipendenti direttamente all'Organismo di Vigilanza o al superiore gerarchico il quale provvederà a indirizzarle all'Organismo di Vigilanza;
- i Collaboratori Esterni, per quanto riguarda la loro attività svolta nei confronti della Banca, effettuano la segnalazione direttamente all'Organismo di Vigilanza;
- l'Organismo di Vigilanza valuta le segnalazioni ricevute e adotta, tramite le funzioni della Banca competenti, 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;
- in caso di segnalazioni anonime, l'Organismo di Vigilanza procede preliminarmente a valutarne la fondatezza, verificando quanto esse appaiano dettagliate e verosimili;
- la Banca garantisce i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione e assicura in ogni caso la massima riservatezza circa l'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Banca o delle persone accusate erroneamente e/o in mala fede.

Oltre alle segnalazioni relative a violazioni di carattere generale sopra descritte, gli organi societari, i Dipendenti e, nei modi e nei limiti previsti contrattualmente, i Collaboratori Esterni devono obbligatoriamente ed immediatamente trasmettere all'Organismo di Vigilanza le informazioni concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal Decreto qualora tali indagini coinvolgano la Banca o suoi Dipendenti od organi societari;
- i rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto.

Infine, tutti coloro che vengano a conoscenza di informazioni relative alla commissione di reati o di fatti e/o comportamenti non conformi alle regole di condotta elaborate da BdL e contenuti nel Modello e nel Codice Etico possono effettuare segnalazioni

spontanee all'Organismo di Vigilanza, utilizzando i contatti comunicati dallo stesso Organismo e indicati sul sito internet di BdL.

Periodicamente l'Organismo di Vigilanza, qualora lo ritenga necessario, propone, tramite le funzioni della Banca competenti, al Direttore Generale o al Consiglio di Amministrazione eventuali modifiche della lista sopra indicata relativa alle informazioni obbligatorie.

#### **Art. 4.6 - Attività di reporting dell'Organismo di Vigilanza verso il vertice aziendale**

Almeno semestralmente, l'Organismo di Vigilanza predispone un rapporto scritto per il Consiglio di Amministrazione, per il Collegio Sindacale e per il Direttore Generale sull'attività svolta (indicando in particolare i controlli effettuati e l'esito degli stessi, l'eventuale aggiornamento della mappatura delle aree a rischio ecc.).

Qualora l'Organismo di Vigilanza rilevi criticità riferibili a qualcuno dei soggetti referenti, la corrispondente segnalazione è da destinarsi prontamente agli altri soggetti sopra individuati.

Il *reporting* ha ad oggetto :

- l'attività svolta dall'Organismo di Vigilanza;
- le eventuali criticità (e spunti per il miglioramento) emerse sia in termini di comportamenti o eventi interni alla Banca, sia in termini di efficacia del Modello.

### **Art. 5 – Sistema disciplinare**

#### **Art. 5.1 - Principi generali**

Ai sensi dell'art. 6 comma II lettera e) del Decreto il Modello deve contenere un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello stesso.

Il Modello di organizzazione, di gestione e di controllo di BdL prevede un adeguato sistema disciplinare in caso di violazione delle regole di condotta imposte ai fini della prevenzione dei reati contemplati dal Decreto.

Lo svolgimento del procedimento disciplinare è affidato alla Direzione Personale la quale, anche su attivazione o segnalazione da parte dell'Organismo di Vigilanza, istruisce le pratiche e formula le proposte di sanzione al Direttore Generale.

Il Direttore Generale decide in autonomia i provvedimenti disciplinari sino a due giorni di sospensione dal servizio e dal trattamento economico.

Il Consiglio di Amministrazione, su proposta del Direttore Generale, delibera infine l'adozione di provvedimenti disciplinari più gravi (da tre a dieci giorni di sospensione dal servizio e dal trattamento economico, licenziamenti per giusta causa o giustificato motivo).

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

BdL da tempo utilizza procedure e modelli di organizzazione e sistemi di controllo le cui violazioni sono soggette al sistema sanzionatorio vigente.

Viene pertanto espresso – con assoluta ed inequivocabile chiarezza – che nessun comportamento illecito, o illegittimo, o scorretto può essere giustificato o considerato meno grave, in quanto pretesamente compiuto nell'asserito "interesse" o nell'asserito "vantaggio" della Banca.

Al contrario, stante l'inequivoca, insuperabile e priva di eccezioni volontà di BdL di non intendere in alcun caso avvalersi di siffatti "interessi" o "vantaggi", tale intento – ove posto in essere nonostante le contrarie misure realizzate dall'Azienda – costituirà uno degli specifici campi di intervento del presente sistema disciplinare.

### **Art. 5.2 - Sanzionabilità del tentativo**

Sono altresì sanzionati gli atti od omissioni diretti in modo non equivoco a violare le regole stabilite da BdL, anche se l'azione non si compie o l'evento non si verifica.

### **Art. 5.3 - Sanzioni per i lavoratori dipendenti**

L'inosservanza delle regole poste o richiamate dal presente Modello adottato dalla BdL, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da parte del personale dipendente che non rivesta la qualifica di dirigente, può dar luogo, secondo la gravità dell'infrazione, all'irrogazione di sanzioni disciplinari nel pieno rispetto delle disposizioni di cui all'art. 7 della legge 20 maggio 1970 n. 300 e della vigente contrattazione collettiva applicabile e precisamente:

- rimprovero verbale
- rimprovero scritto
- sospensione dal servizio e dal trattamento economico
- licenziamento per giustificato motivo
- licenziamento per giusta causa.

Fermo restando tale principio, si precisa peraltro quanto segue:

- rimprovero verbale: si applica in caso di lieve inosservanza dei principi e delle regole di comportamento previste dal presente Modello, di lieve violazione delle procedure e norme interne, nonché delle istruzioni o delle direttive impartite dai superiori, nonché in caso di lieve negligenza nell'espletamento del lavoro;
- rimprovero scritto: si applica nei casi precedenti quando vi siano circostanze particolari che, fermo il carattere lieve della mancanza, richiedano un maggior intervento;

- sospensione dal servizio e dal trattamento economico fino ad un massimo di 10 giorni: si applica in caso di inosservanza dei principi e delle regole di comportamento previste dal presente Modello, di violazione delle procedure e norme interne, nonché delle istruzioni o delle direttive impartite dai superiori in casi di una certa gravità o connotati da recidiva; in caso di negligenza di una certa gravità o che abbia avuto riflessi negativi per l'azienda o per i terzi; in caso di omessa segnalazione o tolleranza di gravi irregolarità commesse da altri;
- licenziamento per giustificato motivo: si applica in caso di notevole inadempimento dei principi e delle regole di comportamento previste dal presente Modello, ovvero delle procedure e norme interne, ovvero delle istruzioni o delle direttive impartite dai superiori, ovvero in caso di commissione di uno dei reati o degli illeciti amministrativi sanzionati dal Decreto Legislativo n. 231/2001 e successive modifiche;
- licenziamento per giusta causa: si applica in caso di comportamento in contrasto con le prescrizioni e/o le procedure e/o le norme interne previste dal presente Modello, che leda l'elemento fiduciario che caratterizza il rapporto di lavoro o risulti talmente grave da non consentire comunque la prosecuzione nemmeno provvisoria del rapporto stesso.

Particolare rigore sarà osservato in ordine ai casi di responsabilità per omesso controllo da parte di persone investite, in generale o in casi particolari, delle relative funzioni (controllo, vigilanza, sorveglianza).

Restano ferme e si intendono qui richiamate tutte le disposizioni, previste dalla Legge e dai contratti collettivi applicati, relative alle procedure ed agli obblighi da osservare nell'applicazione delle sanzioni.

L'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni avverranno nel rispetto di quanto previsto dalla legge (es. Statuto Lavoratori), dal CCNL, dallo Statuto BdL e dalle disposizioni aziendali.

#### **Art. 5.4 - Sanzioni per i soggetti in posizione apicale**

In caso di violazione, da parte di Dirigenti, delle procedure previste dal presente Modello o di adozione, nell'espletamento delle Attività Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, la Banca provvede ad applicare le misure più idonee, tenuto conto della gravità della violazione e della eventuale reiterazione, del livello di responsabilità e dell'intenzionalità, in conformità a quanto previsto dalla normativa vigente e dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti delle imprese creditizie, finanziarie e strumentali.

Tale rapporto di lavoro è peculiare, caratterizzato dal vincolo fiduciario e dalla particolare necessità, per la Banca, di affidarsi a soggetti dalla spiccata professionalità, disponibilità e competenza per l'attuazione dei principi di condotta e per il rispetto dei principi di legge e delle procedure e delle norme aziendali tutte.

Considerato che i provvedimenti contemplati dal Contratto Collettivo Nazionale di Lavoro dei Dirigenti comportano la risoluzione del rapporto di lavoro, gli stessi andranno applicati nei casi di massima gravità della violazione commessa, mentre, per le infrazioni meno gravi, la Banca, in ossequio al principio giuridico della proporzionalità e gradualità della sanzione, si riserva la facoltà di applicare le seguenti sanzioni:

- rimprovero verbale

- nel caso di lieve inosservanza dei principi e delle regole di comportamento previste dal presente Modello, di comportamento non conforme o non adeguato alle prescrizioni del Modello, ovvero di violazione delle procedure e norme interne previste e/o richiamate;

- rimprovero scritto

- mancanze punibili con il rimprovero verbale, ma che, per conseguenze specifiche o per recidiva, abbiano una maggior rilevanza;
- omessa segnalazione o tolleranza di irregolarità in materia lieve commesse da altri.

- licenziamento ex art. 2118 c.c.

- inosservanza delle procedure interne previste dal Modello e negligenza rispetto alle prescrizioni in esso contenute;
- omessa segnalazione o tolleranza di gravi irregolarità commesse da altri appartenenti al Personale;
- adozione di comportamento che possa configurare una possibile ipotesi di reato sanzionato dal D.Lgs. 231/2001 di una gravità tale da esporre la Banca ad una situazione oggettiva di pericolo o tale da determinare riflessi negativi per la stessa.

- licenziamento per giusta causa

- nel caso di adozione di un comportamento palesemente non conforme o non adeguato alle prescrizioni del Modello, tale da determinare la possibile concreta applicazione a carico della Banca delle misure previste dal D.Lgs. 231 /2001 e riconducibile a mancanze di una gravità tale da far venir meno la fiducia sulla quale è basato il rapporto di lavoro e da non consentirne la prosecuzione nemmeno provvisoria.

### **Art. 5.5 - Misure nei confronti degli Amministratori**

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza informa il Collegio Sindacale e l'intero Consiglio affinché possano prendere gli opportuni provvedimenti.

### **Art. 5.6 - Misure nei confronti dei Sindaci**

In caso di violazione del Modello da parte di uno o più Sindaci, l'Organismo di Vigilanza informa l'intero Collegio Sindacale ed il Consiglio di Amministrazione affinché possano prendere gli opportuni provvedimenti.

### **Art. 5.7 - Misure nei confronti dei Collaboratori Esterni**

Ogni violazione delle regole previste dal Modello, nonché ogni commissione dei reati, imputabile ai Collaboratori Esterni (ad esempio, società di service, Consulenti o Partner), è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti. Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Banca, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal Decreto.

### **Art. 6 - Formazione**

Ai fini dell'efficacia del presente Modello, è obiettivo di BdL garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute nei confronti dei Dipendenti. Tale obiettivo riguarda tutte le risorse aziendali che rientrano nella categoria anzidetta, sia si tratti di risorse già presenti in azienda sia da inserire. Il livello di formazione ed informazione è attuato con un differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle Aree di Rischio.

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al Decreto è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno funzioni di rappresentanza della Banca.

In particolare, la Banca ha previsto livelli diversi di informazione e formazione attraverso idonei strumenti di diffusione per:

1. Dipendenti che rivestono la qualifica di dirigenti;
2. Dipendenti che non rivestono la qualifica di dirigenti;
3. Collaboratori Esterni.

La formazione del personale, al fine della corretta applicazione del Modello, viene gestita dalla Direzione Personale – Ufficio Sviluppo Risorse Umane, avvalendosi dell'Area Pianificazione Formazione e Addestramento della Funzione Risorse e Politiche Contrattuali della Capogruppo, in collaborazione con i responsabili delle altre Direzioni/Servizi di volta in volta coinvolti nell'applicazione del Modello e con l'Organismo di Vigilanza ai sensi del Decreto, che ha anche funzioni di supervisione.

E' prestata particolare attenzione al personale di nuova assunzione ed alle persone adibite a nuovo incarico.

La formazione è articolata sui livelli di seguito riportati.

## **Art. 6.1 - Dirigenti**

Realizzazione delle seguenti attività formative:

- consegna di documento informativo sul contenuto del Decreto, con raccolta di conferma di avvenuta ricezione (per i soggetti di nuova assunzione la consegna avverrà all'atto dell'assunzione medesima);
- consegna del Codice Etico;
- consegna del Modello di organizzazione e di gestione;
- seminari di presentazione delle finalità e dei contenuti del decreto legislativo;
- aggiornamenti periodici via “intranet” aziendale;
- corso di formazione a distanza;
- eventuali ulteriori iniziative, qualora necessarie.

## **Art. 6.2 - Altro personale**

Realizzazione delle seguenti attività formative:

- consegna di documento informativo sul contenuto del Decreto, con raccolta di conferma di avvenuta ricezione (per i soggetti di nuova assunzione la consegna avverrà all'atto dell'assunzione medesima);
- consegna del Codice Etico;
- consegna del Modello di organizzazione e di gestione, unitamente a nota interna esplicativa delle finalità e del contenuto del Modello medesimo;
- aggiornamenti periodici via “intranet” aziendale;
- corso di formazione “on line” con certificazione finale.

## **Art. 6.3 - Collaboratori Esterni**

Ai soggetti esterni che, a vario titolo, collaborano con BdL, saranno fornite apposite informative sulle politiche e sulle procedure adottate da BdL medesima sulla base del presente Modello e saranno consegnati il testo di quest’ultimo nonché del Codice Etico.

## B - Codice Etico

### Premessa

Per la complessità delle situazioni in cui la Banca si trova ad operare, è importante definire con chiarezza l'insieme dei valori che la Banca riconosce, accetta e condivide e l'insieme delle responsabilità che la stessa assume verso l'interno e verso l'esterno.

Per questa ragione è stato predisposto il Codice Etico al fine di indicare i principi generali di comportamento, la cui osservanza da parte dei dipendenti e dei consulenti della Banca è di importanza fondamentale per il buon funzionamento, l'affidabilità e la reputazione della Banca medesima: fattori che costituiscono un patrimonio decisivo per il successo della stessa.

Spetta all'Organismo di Vigilanza facilitare e promuovere la conoscenza del Codice.

Ogni comportamento contrario alla lettera e allo spirito del Codice sarà sanzionato in conformità con quanto previsto dal Codice medesimo.

Compete al suddetto Organismo vigilare sulla corretta osservanza del Codice, predisponendo adeguati strumenti di informazione, prevenzione e controllo e assicurando la trasparenza delle operazioni e dei comportamenti posti in essere.

L'integrità morale è un dovere costante di tutti coloro che lavorano con e per la Banca.

Le norme del Codice si applicano senza eccezione ai dipendenti della Banca e a tutti coloro che operano per il conseguimento degli obiettivi della stessa.

I soggetti in posizione apicale, quali amministratori, sindaci o soggetti con funzioni di direzione, nonché tutti i dipendenti, i collaboratori e consulenti esterni non devono mai venire meno al rispetto di principi fondamentali quali l'onestà, l'integrità, la correttezza, la trasparenza e l'obiettività nel perseguimento degli obiettivi aziendali.

I sopraindicati soggetti, durante lo svolgimento dell'attività loro demandata, devono rispettare le leggi e le normative vigenti orientando le proprie azioni ed i propri comportamenti ai principi, agli obiettivi ed agli impegni richiamati nel Codice e, in nessun caso, il perseguimento di un interesse o di un vantaggio della Banca può giustificare un comportamento non corretto.

Va evitata ogni forma di discriminazione ed in particolare qualsiasi discriminazione basata su razza, nazionalità, sesso, età, disabilità fisiche e psichiche, orientamenti sessuali, opinioni politiche o sindacali, indirizzi filosofici o convinzioni religiose.

Le molestie sessuali e le vessazioni fisiche o psicologiche non sono tollerate dalla Banca, in qualsiasi forma esse si manifestino.

Fermi restando i divieti generali di fumare nei luoghi di lavoro, la Banca nelle situazioni di convivenza lavorativa tiene in particolare considerazione la salute dei dipendenti, di chi avverte disagio fisico in presenza di fumo e chiedi di esser preservato dal contatto con il "fumo passivo".

Ognuno, nell'ambito delle responsabilità connesse al ruolo ricoperto, deve fornire il massimo livello di professionalità di cui dispone per soddisfare i bisogni della clientela e degli utenti interni.

E' necessario che ciascuno svolga con impegno le attività assegnate, contribuendo in maniera concreta al raggiungimento degli obiettivi aziendali.

Nello svolgimento di qualsiasi attività sociale devono sempre evitarsi situazioni in cui i dipendenti e/o membri di Organi di amministrazione o controllo e/o consulenti e/o clienti e/o fornitori della Banca siano, anche solo apparentemente, in conflitto di interessi con la Banca.

Ogni operazione e transazione deve essere correttamente eseguita, registrata, autorizzata, verificabile, legittima, coerente e congrua. Ciò significa che ciascuna azione

ed operazione deve avere una registrazione adeguata e deve essere supportata da idonea documentazione, al fine di poter procedere in ogni momento all'effettuazione di controlli che ne attestino le caratteristiche e le motivazioni ed individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.

## **Capitolo 1 Rapporti Esterni**

### **Art. 1 Disposizioni Generali**

Gli organi sociali e i dipendenti debbono tenere un comportamento improntato alla massima correttezza ed integrità in tutti i rapporti con persone ed enti esterni alla Banca. Non sono ammesse forme di regalo che possano essere, anche solo indirettamente, interpretate come eccedenti le normali manifestazioni di cortesia ammesse nella prassi commerciale, o comunque mirate ad ottenere trattamenti di favore per la Banca o dalla Banca.

E' fatto assoluto divieto di offrire, sia direttamente che indirettamente, denaro e/o doni e/o prestazioni a titolo gratuito a pubblici funzionari, quando tali doni e/o prestazioni possano essere in qualche modo collegati a rapporti di affari tra la Banca e le pubbliche funzioni cui gli stessi afferiscono.

Qualora sia impossibile rifiutare o restituire l'omaggio, oppure il rifiuto possa avere conseguenze negative sul rapporto, il ricevente il dono dovrà informare tempestivamente il suo diretto superiore, che valuterà le azioni da intraprendere.

In tali casi (ad eccezione di quelli aventi ad oggetto omaggi di modico valore, ove non siano connotati da caratteristiche che facciano presumere l'esistenza di un illecito scambio di favori tra cliente e dipendente), il superiore deve informare per iscritto l'Organismo di Vigilanza.

E' fatto assoluto divieto per i dipendenti e/o consulenti della Banca di richiedere e/o accettare, direttamente o indirettamente, denaro e/o doni e/o prestazioni di favore, nel caso in cui ciò potrebbe sembrare essere fatto quale contropartita di una prestazione dovuta nell'ambito dello svolgimento dell'attività sociale della Banca.

Inoltre, nell'avviare relazioni commerciali con nuovi clienti e/o fornitori e nella gestione di quelle già in essere, è necessario, sulla base delle informazioni pubbliche e/o disponibili nel rispetto delle normative vigenti, evitare di:

- intrattenere rapporti con soggetti implicati in attività illecite, in particolare connesse al traffico d'armi, al riciclaggio, al terrorismo, al contrabbando, al traffico di sostanze stupefacenti o psicotrope e, comunque, con soggetti privi dei necessari requisiti di serietà ed affidabilità commerciale;
- mantenere rapporti finanziari con soggetti che, anche in modo indiretto, ostacolano lo sviluppo umano e contribuiscono a violare i diritti fondamentali della persona (ad es. sfruttando il lavoro minorile, favorendo il traffico di migranti ovvero il turismo sessuale, ecc.);
- richiedere prestiti ai clienti.

### **Art. 2 Rapporti con la clientela**

La professionalità, la competenza, la disponibilità, la correttezza e la cortesia rappresentano i principi guida che i destinatari del Codice sono tenuti a seguire nei loro rapporti con la clientela.

I comportamenti assunti sono improntati a tenere strettamente riservate le informazioni acquisite nel corso dell'attività, nel pieno rispetto della vigente normativa in tema di privacy.

Per tutelare l'immagine e la reputazione della Banca è indispensabile che i rapporti con la clientela siano improntati:

- alla piena trasparenza e correttezza;
- al rispetto della legge, con particolare riferimento alle disposizioni in tema di antiriciclaggio, antiusura e trasparenza, nonché alla normativa in materia di vigilanza;
- all'indipendenza nei confronti di ogni forma di condizionamento, sia interno che esterno.

### **Art. 3 Rapporti con i fornitori**

Ogni acquisto in favore della Banca deve essere condotto con lealtà, integrità, riservatezza, diligenza, professionalità e obiettività di giudizio, da personale qualificato che si assume la responsabilità delle proprie valutazioni e dei propri giudizi, assicurando nell'attività di acquisto alla Banca l'osservanza di tutte le disposizioni normative rilevanti.

I dipendenti e/o consulenti addetti al processo di acquisto:

- sono tenuti al rispetto dei principi di imparzialità ed indipendenza nell'esercizio dei compiti e delle funzioni affidate;
- devono mantenersi liberi da obblighi personali verso i fornitori; eventuali rapporti personali dei dipendenti e/o consulenti coi fornitori devono essere segnalati alla Direzione di appartenenza prima di ogni trattativa;
- devono mantenere i rapporti e condurre le trattative con i fornitori in modo da creare una solida base per relazioni reciprocamente convenienti e di lunga durata, nell'interesse della Banca;
- sono tenuti tassativamente a segnalare immediatamente alla Direzione Controlli e all'Organismo di Vigilanza qualsiasi tentativo o caso di alterazione dei normali rapporti commerciali;
- non devono offrire beni o servizi, in particolare sotto forma di regali, a personale di altre società o enti per ottenere informazioni riservate o benefici diretti o indiretti rilevanti, per sé o per la Banca, fermo restando quanto previsto dalle disposizioni generali del presente Codice Etico;
- non devono accettare beni o servizi da soggetti esterni o interni a fronte del rilascio di notizie riservate o dell'avvio di azioni o comportamenti volti a favorire tali soggetti, anche nel caso non vi siano ripercussioni dirette per la Banca.

### **Art. 4 Rapporti con la Pubblica Amministrazione**

1. Ai fini del presente Codice, per Pubblica Amministrazione si deve intendere, oltre a qualsiasi ente pubblico, altresì, qualsiasi agenzia amministrativa indipendente, persona, fisica o giuridica, che agisce in qualità di pubblico ufficiale o incaricato di pubblico servizio ovvero in qualità di membro di organo delle Comunità europee o di funzionario delle Comunità europee o di funzionario di Stato estero. Sempre ai sensi del presente Codice, nella definizione di ente pubblico sono compresi quei soggetti

privati che, per ragioni preminenti di ordine politico-economico, adempiono ad una funzione pubblicistica posta a presidio della tutela di interessi generali, come gli enti gestori dei mercati regolamentati.

2. Non è ammesso, né direttamente, né indirettamente, né per il tramite di interposta persona, offrire o promettere denaro, doni o compensi, sotto qualsiasi forma, né esercitare illecite pressioni, né promettere qualsiasi oggetto, servizio, prestazione o favore a dirigenti, funzionari o dipendenti della Pubblica Amministrazione ovvero a soggetti incaricati di pubblico servizio ovvero a loro parenti o conviventi allo scopo di indurre al compimento di un atto d'ufficio o contrario ai doveri d'ufficio (dovendosi ritenere tale anche lo scopo di favorire o danneggiare una parte in un processo civile, penale o amministrativo al fine di arrecare un vantaggio diretto o indiretto alla Banca).
3. Chi riceva richieste esplicite o implicite di benefici di qualsiasi natura da parte di soggetti della Pubblica Amministrazione, come sopra definiti, dovrà immediatamente:
  - sospendere ogni rapporto con essi;
  - informare per iscritto l'Organismo di Vigilanza ed il suo diretto superiore.
4. Le prescrizioni indicate nei precedenti commi non devono essere eluse ricorrendo a forme diverse di aiuti e contribuzioni che, sotto la veste di incarichi, consulenze, pubblicità, etc., abbiano analoghe finalità di quelle vietate dal presente paragrafo.
5. Nel caso si instaurino rapporti commerciali con la Pubblica Amministrazione, compresa la partecipazione a gare pubbliche, è necessario operare sempre nel rispetto della legge e della corretta prassi commerciale. In particolare non dovranno essere intraprese, direttamente o indirettamente, le seguenti azioni:
  - esaminare o proporre opportunità di impiego e/o commerciali che possano avvantaggiare dipendenti e/o il loro diretto superiore a titolo personale;
  - offrire o in alcun modo fornire omaggi;
  - sollecitare o ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti.
6. Non è consentito utilizzare o presentare dichiarazioni o documenti falsi o attestanti cose non vere, ovvero omettere informazioni per conseguire, a vantaggio o nell'interesse della Banca, contributi, finanziamenti o altre erogazioni comunque denominate concesse dallo Stato, da un Ente Pubblico o dall'Unione Europea.
7. E' vietato indurre chiunque in errore con artifici o raggiri per procurare alla Banca un ingiusto profitto con altrui danno. La violazione di tale divieto è ancora più grave se ad essere indotto in errore è lo Stato o un ente pubblico. Il "profitto ingiusto" può essere diretto o indiretto e comprendere, oltre ai contributi, finanziamenti e altre erogazioni concesse dallo Stato, da un ente pubblico e dall'Unione Europea, anche concessioni, autorizzazioni, licenze o altri atti amministrativi.
8. E' inoltre fatto divieto di utilizzare contributi, finanziamenti, o altre erogazioni comunque denominate, concesse alla Banca dallo Stato, da un Ente Pubblico o dall'Unione Europea, per scopi diversi da quelli per i quali gli stessi sono stati assegnati.
9. E' vietato alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenire illegalmente con qualsiasi modalità sui dati, informazioni e programmi in esso contenuti o ad esso pertinenti, al fine di conseguire un ingiusto profitto con altrui danno. Il divieto è rafforzato se ad essere danneggiato è lo Stato o un ente pubblico.

## **Art. 5 Rapporti con la stampa ed altri mezzi di comunicazione**

1. I rapporti con la stampa ed altri mezzi di comunicazione sono di esclusiva competenza del Presidente e del Direttore Generale;
2. senza la preventiva autorizzazione del Presidente e/o del Direttore Generale, i collaboratori devono astenersi dal rilasciare a rappresentanti della stampa, di altri mezzi di comunicazione ed a qualsiasi terzo dichiarazioni o interviste o comunque dal lasciar trapelare anche semplici notizie riguardanti gli affari della Banca o l'organizzazione di lavoro della stessa.

## **Art. 6 Situazione di Conflitto d'Interessi**

I dipendenti, i membri degli organi sociali e, in genere, tutti coloro che operano in nome e per conto della Banca, devono evitare ogni possibile situazione di conflitto d'interessi. A titolo esemplificativo, ma non limitativo, le situazioni che possono provocare un conflitto di interessi sono le seguenti:

- partecipare a decisioni che riguardano affari con soggetti con cui il dipendente o un familiare stretto del dipendente abbiano interessi oppure da cui potrebbe derivare un interesse personale;
- uso del nome della Banca per usufruire di vantaggi personali;
- proporre o accettare accordi da cui possano derivare vantaggi personali;
- compiere atti, stipulare accordi ed in genere tenere qualsivoglia comportamento che possa, direttamente o indirettamente, causare alla Banca e/o al Gruppo un danno, anche in termini di immagine e/o credibilità sul mercato.
- confliggere con l'interesse della Banca, influenzando l'autonomia decisionale di altro soggetto demandato a definire rapporti commerciali con o per la Banca.

I dipendenti che si trovino in una situazione di conflitto d'interessi, anche solo potenziale, devono darne immediata notizia al proprio superiore diretto che valuterà il comportamento da tenere.

## **Capitolo 2 Rapporti Interni**

### **Art. 7 Trattamento economico dei Vertici Aziendali e degli operatori di mercato e politiche di remunerazione della Banca**

1. La Banca si impegna affinché le remunerazioni erogate a qualsiasi titolo ai componenti degli organi amministrativi e di controllo, ai Vertici Aziendali<sup>1</sup> e agli operatori di mercato, inclusi i *traders*, siano sempre ispirate a criteri di eticità e trasparenza.

---

<sup>1</sup> Per "Vertici Aziendali" si intendono: Direttore Generale, il/i Vice Direttore Generale, se nominato/i, i Dirigenti Responsabili delle Direzioni e Servizi Centrali.

2. In ottemperanza alle Disposizioni di Vigilanza in materia, le politiche di remunerazione degli organi sociali, dei Vertici Aziendali, dei dipendenti e degli altri collaboratori sono sottoposte all'approvazione dell'assemblea ordinaria dei soci. All'assemblea dei soci viene altresì annualmente fornita una adeguata informativa sulla attuazione delle politiche di remunerazione.

3. All'interno del Consiglio di Amministrazione della Capogruppo è costituito un Comitato per la Remunerazione, composto da amministratori non esecutivi e in maggioranza indipendenti, al quale sono, tra l'altro, attribuite funzioni consultive e propositive in materia di remunerazione degli amministratori esecutivi e dei Vertici Aziendali di tutte le Società del Gruppo, nonché di monitoraggio e valutazione della corretta attuazione delle politiche di remunerazione approvate in conformità con le citate disposizioni dell'Autorità di Vigilanza.

4. Le politiche di remunerazione devono essere coerenti con il principio di prudente gestione del rischio e di moderazione dei compensi, nonché con le strategie di lungo periodo.

Salvo motivata deliberazione dell'assemblea dei soci, la Banca non attua piani di incentivazione basati su strumenti finanziari; ove attuati, tali piani dovranno in ogni caso essere strutturati in modo da rispettare rigorosamente i principi di prudente gestione del rischio, di moderazione e di coerenza con le strategie di lungo periodo della Banca.

Le forme di retribuzione incentivante collegate al raggiungimento di specifici obiettivi aziendali possono essere previste solo a favore degli Amministratori esecutivi, del personale dipendente e dei collaboratori, e devono essere strutturate in modo da assicurare il collegamento tra l'incentivo riconosciuto e il carattere effettivo e durevole dei risultati conseguiti, la coerenza con la prudente gestione del rischio e la strategia di lungo periodo. In particolare, tali forme di retribuzione devono essere

- collegate all'effettivo e verificato conseguimento degli obiettivi assegnati, prevedendo a tal fine anche che l'erogazione dell'incentivo sia in parte differito ad un periodo successivo al conseguimento degli obiettivi in modo da poterne controllare il carattere durevole;
- equilibrate con le componenti fisse della retribuzione complessiva, per favorire comportamenti allineati a risultati sostenibili e alla prudente gestione del rischio della Banca, e coerenti con le funzioni individualmente assegnate ai beneficiari;
- realizzate in modo da sterilizzare gli effetti derivanti dalle attività *captiv*e e da misurare il risultato cui è parametrata l'incentivazione al netto degli accantonamenti prudenziali effettuati a fronte dei rischi assunti dalla Banca;
- periodicamente sottoposte a valutazione e controllo anche tramite la comparazione con le politiche di incentivazione attuate dagli altri operatori del mercato.

5. Il trattamento economico riconosciuto ai Vertici Aziendali e, in genere, al personale dipendente in caso di scioglimento del rapporto di lavoro non può eccedere 24 mensilità di retribuzione; nessun beneficio economico, a qualsivoglia titolo, è riconosciuto agli amministratori all'atto della cessazione del rapporto.

## **Art. 8 Disposizioni relative ad attività di natura contabile, amministrativa o finanziaria**

A tutti i dipendenti e/o consulenti che a qualunque titolo (anche quali meri fornitori di dati) siano coinvolti nella formazione del bilancio e di documenti similari, o comunque di documenti che rappresentino la situazione economica, patrimoniale o finanziaria della Banca (come ad es. quelli da pubblicare in occasione di OPA), nonché in particolare agli

amministratori, ai sindaci e chi ricopre posizioni apicali, è vietato esporre fatti non rispondenti al vero, anche se oggetto di valutazione, ovvero omettere informazioni od occultare dati in violazione diretta o indiretta dei principi normativi e delle regole procedurali interne, in modo da indurre in errore i destinatari dei sopra menzionati documenti.

L'eventuale condotta illecita sarà considerata come commessa in danno della Banca stessa.

E' vietato impedire o comunque ostacolare lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, al collegio sindacale, all'Organismo di Vigilanza o alla società di revisione.

E' vietato determinare la maggioranza in assemblea con atti simulati o fraudolenti.

E' vietato diffondere notizie false o porre in essere operazioni simulate o altri artifici tali da provocare una sensibile alterazione del prezzo di strumenti finanziari quotati o non quotati o da incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale della Banca e/o del Gruppo ovvero di qualsivoglia altra società.

A tutti coloro che hanno rapporti con le autorità pubbliche di vigilanza, nonché agli amministratori, ai sindaci e a chi ricopre posizioni apicali è vietato ostacolarne le funzioni.

E' altresì vietato, nelle comunicazioni alle predette autorità, esporre fatti non corrispondenti al vero, anche se oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria della Banca, o occultare con altri mezzi fraudolenti, in tutto o in parte, fatti inerenti la situazione medesima che avrebbero dovuto essere comunicati.

I dipendenti e consulenti della Banca devono evitare ogni comportamento che possa, direttamente o indirettamente, causare fenomeni di insider trading anche da parte di terzi.

I dipendenti, i consulenti, i membri del consiglio di amministrazione, i sindaci e, più in generale, tutti i soggetti che hanno accesso ad informazioni privilegiate (intendendosi per tali le informazioni di carattere preciso che non sono state rese pubbliche, concernenti direttamente o indirettamente uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, che, se rese pubbliche, potrebbero influire in modo sensibile sui prezzi di tali strumenti finanziari) devono astenersi dal diffondere e dall'utilizzare tali informazioni per la compravendita (per sé o per altri) dei suddetti strumenti finanziari, al fine di garantire la massima trasparenza del mercato.

Nel bilancio annuale sono pubblicate le azioni della Banca possedute al termine dell'esercizio, e le compravendite effettuate nel corso dell'esercizio, da parte dei consiglieri, dei sindaci e dei direttori generali della Banca.

## **Art. 9 Norme di comportamento del personale**

Il personale dipendente deve attenersi altresì alle seguenti regole.

Deve essere evitata ogni situazione o attività che possa condurre a conflitti di interesse con la Banca o che potrebbe interferire con la capacità di assumere decisioni imparziali, nel migliore interesse della Banca.

Le informazioni acquisite nello svolgimento delle attività assegnate debbono rimanere strettamente riservate e opportunamente protette e non possono essere utilizzate, comunicate o divulgate, sia all'interno, sia all'esterno della Banca, se non nel rispetto della normativa vigente e delle procedure aziendali.

I dipendenti e/o consulenti della Banca devono rispettare e salvaguardare i beni di proprietà della Banca, nonché impedirne l'uso fraudolento o improprio. L'utilizzo degli strumenti aziendali da parte dei dipendenti e/o consulenti della Banca (per questi ultimi

nei limiti contrattualmente previsti) deve essere funzionale ed esclusivo allo svolgimento delle attività lavorative o agli scopi autorizzati dalle funzioni interne preposte.

I dipendenti e/o consulenti della Banca devono evitare che la situazione finanziaria personale possa avere ripercussioni sul corretto svolgimento della propria attività lavorativa.

E' vietato sollecitare o accettare, per sé o per altri, raccomandazioni, trattamenti di favore, doni o altra utilità da parte dei soggetti con i quali si entra in relazione, evitando di ricevere benefici di ogni genere che possano essere o apparire tali da influenzare la propria indipendenza di giudizio o imparzialità. Qualora il dipendente riceva omaggi o atti di ospitalità non di natura simbolica, dovrà informare il suo diretto superiore per valutare l'eventuale restituzione o ogni altro più opportuno intervento.

Ogni dipendente si deve impegnare a curare le proprie competenze e professionalità, arricchendole con l'esperienza e la collaborazione dei colleghi; assume un atteggiamento costruttivo e propositivo, stimolando la crescita professionale dei propri collaboratori.

L'attività di ogni dipendente e delle strutture operative, di direzione e della rete commerciale, deve essere improntata alla massima collaborazione al fine di ottimizzare la soddisfazione della clientela.

Le decisioni assunte da ciascuno devono basarsi su principi di sana e prudente gestione, valutando in modo oculato i rischi potenziali, nella consapevolezza che le scelte personali contribuiscono al raggiungimento di positivi risultati aziendali.

Tutte le operazioni e transazioni devono essere ispirate alla massima correttezza dal punto di vista della gestione, alla completezza e trasparenza delle informazioni, alla legittimità sotto l'aspetto formale e sostanziale e alla chiarezza e verità nei riscontri contabili, secondo le norme vigenti e le procedure aziendali e devono essere assoggettabili a verifica.

E' fatto obbligo di segnalare al responsabile dell'unità organizzativa di appartenenza eventuali istruzioni ricevute contrastanti con la legge, il Modello di Organizzazione, Gestione e Controllo adottato dalla Banca ai sensi del D.Lgs. 231/2001, il contenuto dei contratti di lavoro, la normativa interna o il presente Codice Etico.

Qualora l'ordine ritenuto illegittimo sia impartito da detto responsabile, la segnalazione va indirizzata all'Organismo di Vigilanza.

In generale, ogni dipendente deve ispirare il proprio comportamento a principi di onestà, correttezza e trasparenza, affinché non vengano posti in essere comportamenti che siano direttamente o indirettamente connessi alla realizzazione dei reati definiti dal D.Lgs. 231/01 quali "illeciti transnazionali" e descritti nel Modello di Organizzazione e Controllo (quali l'associazione per delinquere e il favoreggiamento personale).

## **Art. 10 Personale che riveste la qualifica di incaricato di pubblico servizio**

Coloro che, nello svolgimento dell'attività lavorativa, si trovassero ad assumere la qualifica di incaricato di pubblico servizio non devono:

- abusare della loro qualità o dei loro poteri per costringere o indurre qualcuno a dare o promettere indebitamente, a loro o ad un terzo, denaro, regali o altra utilità;
- ricevere o accettare la promessa di denaro o altra utilità, per loro o per un terzo, al fine di omettere o ritardare un atto d'ufficio o per compiere o aver compiuto un atto contrario ai doveri d'ufficio.

Si precisa che il personale della Banca riveste la qualifica di incaricato di pubblico servizio ogni volta che sia chiamato a svolgere attività di carattere pubblicistico quali, ad esempio, attività di tesoreria, riscossione di tributi, concessione e gestione alla clientela, in regime di Banca delegata dalla Pubblica Amministrazione, di crediti agevolati.

### **Art. 11 Falsificazione di banconote, monete, carte di pubblico credito e valore di bollo**

E' vietato falsificare, detenere, spendere o comunque mettere in circolazione banconote, monete, carte di pubblico credito, valori di bollo contraffatti o alterati. Per carte di pubblico credito si intendono, oltre quelle che hanno corso legale come moneta, le carte e cedole al portatore emesse dal governo.

Chi riceve banconote o monete o carte di pubblico credito sospette di falsità o rubate deve informare il suo superiore diretto, affinché provveda all'opportuna denuncia.

## **Capitolo 3 Il Sistema disciplinare**

### **Art. 12 Principi Generali**

La Banca da tempo utilizza procedure e modelli di organizzazione e sistemi di controllo, le cui violazioni sono soggette alle sanzioni previste dal sistema disciplinare vigente.

La Banca ha adottato un Modello di Organizzazione, Gestione e Controllo ai sensi del Decreto Legislativo n. 231/01, di cui il presente Codice Etico costituisce parte integrante. Nessun comportamento illecito o comunque in violazione di disposizioni del presente Codice, o illegittimo, o anche scorretto, può essere giustificato o considerato meno grave, in quanto compiuto nell'asserito "*interesse*" o nell'asserito "*vantaggio*" della Banca.

Al contrario, stante l'inequivoca, insuperabile e priva di eccezioni volontà della Banca di non intendere in alcun caso avvalersi di siffatti "*interessi*" o "*vantaggi*", tale intento – ove posto in essere nonostante le contrarie misure realizzate dall'Azienda – costituirà uno degli specifici campi di intervento del presente sistema disciplinare.

L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello di Organizzazione, Gestione e Controllo e dal Codice Etico sono adottate dalla Banca in piena autonomia, indipendentemente dal reato che eventuali condotte possano determinare.

### **Art. 13 Sanzionabilità del tentativo**

Sono altresì sanzionati gli atti od omissioni diretti in modo non equivoco a violare le regole stabilite dalla Banca, anche se l'azione non si compie o l'evento non si verifica.

### **Art. 14 Sanzioni per i Dipendenti**

L'inosservanza delle regole indicate nel Modello adottato dalla Banca ai sensi del Decreto, nonché le violazioni delle disposizioni e dei principi stabiliti nel Codice Etico da parte del personale dipendente che non rivesta la qualifica di dirigente, può dar luogo, secondo la gravità dell'infrazione, all'irrogazione di sanzioni disciplinari nel pieno rispetto delle disposizioni di cui all'art. 7 della legge 20 maggio 1970 n. 300 e della vigente contrattazione collettiva applicabile e precisamente:

- rimprovero verbale;
- rimprovero scritto;
- sospensione dal servizio e dal trattamento economico;
- licenziamento per giustificato motivo;
- licenziamento per giusta causa.

Fermo restando quanto sopra, si precisa peraltro quanto segue:

- ogni deliberata, o comunque dolosa commissione di reati di cui al Decreto, ovvero violazione dei doveri fondamentali propri della funzione o carica o qualifica rivestita comporterà senz'altro la risoluzione del rapporto di lavoro, a prescindere dal danno economico che i detti comportamenti abbiano eventualmente determinato;
- anche ogni colposa o imprudente o negligente o omissiva condotta o comportamento in violazione del Decreto potrà comportare la medesima sanzione, in relazione alla gravità della vicenda o alle conseguenze pregiudizievoli (non necessariamente solo economiche) cagionate, o alla eventuale recidiva, o all'impatto sull'ambiente aziendale, o in relazione all'importanza dei principi o delle procedure violate, o alle ricadute sulla fiducia e sulla affidabilità circa i futuri comportamenti;
- nei casi di minore importanza, privi di ricadute pregiudizievoli, saranno comunque adottati provvedimenti disciplinari conservativi graduati secondo l'importanza e la serietà dell'accaduto.

Particolare rigore sarà osservato in ordine ai casi di responsabilità per omesso controllo da parte di persone investite, in generale o in casi particolari, delle relative funzioni (controllo, vigilanza, sorveglianza).

Restano ferme e si intendono qui richiamate tutte le disposizioni, previste dalla Legge e dai contratti collettivi applicati, relative alle procedure ed agli obblighi da osservare nell'applicazione delle sanzioni.

L'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni avverranno nel rispetto di quanto previsto dalla legge (es. Statuto Lavoratori), dal CCNL, dallo Statuto BdL e dalle disposizioni aziendali.

## **Art. 15 Sanzioni per i soggetti in posizione apicale**

In caso di violazione, da parte di Dirigenti, delle procedure previste dal presente Modello o di adozione, nell'espletamento delle Attività Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso nonché di violazione delle disposizioni e dei principi stabiliti nel Codice Etico, la Banca provvede ad applicare le misure più idonee in conformità a quanto normativamente previsto, secondo i criteri indicati al punto 5.4 del Modello.

Nei confronti del personale dirigente le valutazioni circa le sanzioni applicabili saranno operate tenuto conto, oltre che del livello di responsabilità e dell'intenzionalità e gravità della condotta, anche della peculiarità del rapporto di lavoro, caratterizzato dal forte senso di fiducia, dalla mancanza, per i dirigenti medesimi, di un sistema di sanzioni conservative, dalla particolare necessità, per la Banca, di affidarsi a soggetti dalla spiccata professionalità, disponibilità e competenza per l'attuazione dei principi di condotta e per il rispetto dei principi di legge e delle procedure e delle norme aziendali tutte.

#### **Art. 16 Misure nei confronti degli Amministratori**

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione, l'Organismo di Vigilanza informa il Collegio Sindacale e l'intero Consiglio affinché possano prendere gli opportuni provvedimenti.

#### **Art. 17 Misure nei confronti dei Sindaci**

In caso di violazione del Modello da parte di uno o più Sindaci, l'Organismo di Vigilanza informa l'intero Collegio Sindacale e il Consiglio di Amministrazione affinché possano essere presi gli opportuni provvedimenti.

#### **Art. 18 Misure nei confronti dei Collaboratori Esterni**

Ogni violazione delle regole previste dal Modello, nonché ogni commissione dei reati, imputabile ai Collaboratori Esterni (ad esempio, società di service, Consulenti o Partner), è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti. Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Banca, come nel caso di applicazione alla stessa da parte del giudice delle misure previste dal Decreto.

### **Capitolo 4 Attuazione del Codice Etico**

#### **Art. 19 Organismo di Vigilanza**

Il compito di vigilare sul rispetto del presente Codice, relazionando almeno semestralmente il Consiglio di Amministrazione ed il Collegio Sindacale, spetta all'Organismo di Vigilanza costituito ai sensi del D.Lgs. 231/01 dal Consiglio d'Amministrazione e regolato da apposito regolamento, che forma parte integrante del Modello di organizzazione, gestione e controllo della Banca, approvato dal Consiglio medesimo, a cui si fa espresso richiamo.

#### **Art. 20 Formazione**

La Banca, in accordo con l'Organismo di Vigilanza, si impegna a comunicare a tutti i soggetti interessati i valori ed i principi contenuti nel Codice Etico, affinché gli stessi vengano applicati nelle scelte correnti.

In particolare la Banca eroga appositi corsi di formazione ed organizza incontri e seminari, allo scopo di sviluppare nel tempo, fra l'altro, la capacità di riconoscere, analizzare e risolvere i dilemmi etici che possano sorgere nella comune operatività.