

MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

Redatto ai sensi del
Decreto Legislativo 231/2001



Sommario

1. Premessa.....	3
2. Definizioni	3
3. Struttura del Modello	4
4. Principi generali per l'elaborazione del Modello	4
5. La normativa di riferimento	5
5.1 I reati commessi da soggetti apicali.....	6
5.2 I reati commessi da sottoposti	6
5.3 Le fattispecie di reato.....	7
5.4 I requisiti del Modello	8
5.5 Gli obiettivi	8
5.6 La definizione di rischio accettabile	9
5.7 Gli altri elementi fondamentali del Modello 231	10
6. La redazione del Modello	10
7. Il sistema organizzativo	11
7.1 Le linee Guida di categoria	11
7.2 Il sistema organizzativo della banca	11
8. Il sistema dei controlli interni	12
8.1 Consigliere con delega al Sistema dei Controlli Interni ed il Comitato Rischi	12
8.2 Le attività sensibili (ex art.6 co.2 lett. a).....	13
8.3 I principi di controllo	13
9. L'Organismo di Vigilanza	14
10. I flussi informativi	14
11. Il sistema disciplinare	16
12. Formazione e Informazione.....	18
13. Il Whistleblowing.....	18
13.1 Whistleblowing e contenuto del Modello.....	18
14. La privacy	19

PARTE GENERALE

1. Premessa

Il presente documento descrive il Modello di Organizzazione e di Gestione adottato dalla Banca al fine di prevenire la realizzazione dei reati previsti dal Decreto Legislativo 231/2001.

Trattasi, in conformità alla previsione dell'art. 6 del D. Lgs. 231/2001, di un aggiornamento del Modello esistente, sia nella Parte Generale che in quella Speciale, reso opportuno sia per verificarne la perdurante idoneità a prevenire i reati, sia per adattarlo alle recenti novità legislative che hanno interessato il mondo del credito cooperativo, prima tra tutte la nascita del Gruppo Bancario Iccrea, costituito in seguito alla emanazione della Legge n. 49 del 2016 (e successive modifiche), che ha riformato il Sistema del Credito Cooperativo e ha previsto l'obbligo di adesione delle Banche di Credito Cooperativo a una Capogruppo formalmente autorizzata dagli Organi di Vigilanza.

2. Definizioni

I termini qui riportati saranno utilizzati con il seguente significato:

- "D.Lgs. 231" o, più semplicemente, "Decreto": il Decreto Legislativo 8 giugno 2001 n. 231, recante «Disciplina della responsabilità amministrativa delle persone giuridiche, delle associazioni e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300» ed ogni sua successiva modifica ed integrazione;

- "Reati 231": i reati indicati nel D.Lgs 231 e quelli, contenuti in diversi provvedimenti di legge, dalla cui realizzazione può derivare la responsabilità amministrativa dell'Ente ai sensi della medesima disciplina;

- "Modello 231" o "MOG": il Modello di Organizzazione e Gestione ex art. 6, c. 1, lett. a), del D.Lgs. 231/2001;

- "Banca": la Banca di Credito Cooperativo per cui il presente Modello è stato redatto;

- "Soggetti apicali": le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Banca - o di una sua unità organizzativa dotata di autonomia funzionale, se presente - nonché le persone che esercitano, anche di fatto, la gestione e il controllo della Banca (art. 5, comma 1, lettera a) del D.Lgs. n. 231/2001)

- "Sottoposti": le persone sottoposte alla direzione o alla vigilanza dei soggetti apicali (art. 5, comma 1, lettera b) del D. Lgs. n. 231/2001);

- "Fornitori": le controparti contrattuali della Banca quali, ad esempio, gli appaltatori ed i fornitori di opere, di beni e servizi nonché tutti coloro con i quali l'Ente stabilisce forme di collaborazione;

- "Linee Guida": le linee guida redatte dalle associazioni di categoria, con particolare riferimento a quelle pubblicate dall'ABI ("Linee Guida dell'Associazione bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche" del Marzo 2008) e dal Gruppo di lavoro interdisciplinare composto da ABI, CNDCEC, CNF e Confindustria ("Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del dlgs. 8 giugno 2001 n. 231") del Febbraio 2019);

- "Organismo di Vigilanza" o "ODV": l'Organismo dotato di autonomi poteri di vigilanza e controllo cui è affidata la responsabilità di vigilare sul funzionamento e l'osservanza del modello avente i requisiti di cui all'art. 6, comma 1, lettera b) del D.Lgs. n. 231/2001 e di curarne l'aggiornamento.

3. Struttura del Modello

Il presente Modello è composto da una Parte Generale ed una Speciale.

La Parte generale illustra la struttura del Modello, la normativa di riferimento, le modalità con cui la Banca ha implementato il Modello 231 ed alcuni cenni al funzionamento dell'Organismo di Vigilanza.

La Parte Speciale è divisa in 2 Sezioni.

La Sezione I riporta l'elenco di tutte le tipologie di reato specificamente sanzionate dal Decreto ("Elenco dei reati 231"), indipendentemente dalla probabilità/possibilità che esse possano essere perpetrate dai soggetti apicali o dai sottoposti e collaboratori dell'Associazione, e le relative sanzioni. Grazie ad esso l'ODV dell'Ente è in grado di calcolare in modo oggettivo il c.d. "rischio inerente", sulla base della entità delle sanzioni che il legislatore ha previsto di comminare, per ogni categoria di reati, al verificarsi di ciascuno di essi.

La Sezione II, che costituisce il nucleo principale del Modello, ha invece ad oggetto l'esposizione dei risultati della attività di Analisi dei rischi specificamente svolta nell'Ente.

Completano il Modello, di cui costituiscono parte integrante e sostanziale, tutti i documenti di formazione interna, ancorché non conservati agli atti dell'Organismo di Vigilanza, che sono stati esaminati per la redazione del Modello e che vanno a formare l'insieme dei presidi e dei controlli esistenti per calmierare il rischio reato: statuto, processi, regolamenti, ordini di servizio, note operative etc., oltre al testo del Decreto Legislativo 231/2001.

4. Principi generali per l'elaborazione del Modello

I principi generali su cui è stato elaborato il Modello, come richiamati dalle Linee Guida, sono stati i seguenti:

1. **SPECIFICITÀ** - Le attività di analisi e i meccanismi di gestione del rischio descritti nel MOG sono stati elaborati tenendo conto della concreta organizzazione della Banca e dell'attività da essa svolta, in coerenza con gli accertamenti svolti presso la Struttura ed i colloqui avuti con il personale addetto sia in fase di prima redazione del Modello che nelle successive riunioni tenute dall'Organismo di Vigilanza.
2. **ADEGUATEZZA** - Poiché un Modello è adeguato solo quando dimostra la reale capacità di prevenire i comportamenti non voluti, nella sua redazione sono state rispettate le seguenti indicazioni, tratte anche dalla giurisprudenza più recente:
 - a. espressa indicazione delle fattispecie illecite rispetto alle quali l'esposizione della Banca risultata particolarmente sensibile o, al contrario, trascurabile;
 - b. bilanciamento tra i presidi esplicitati nel Modello ed il rinvio all'impianto documentale esistente;
 - c. richiamo a procedure e regolamenti, ove esistenti;
 - d. menzione dei controlli di primo livello (di linea, insiti nelle procedure operative), di secondo livello (ad es. Collegio Sindacale, Compliance, Risk

- management, AML) e di terzo (Internal Audit, Società di revisione);
- e. coordinamento e integrazione del Modello con eventuali altri sistemi di e/o terzo livello gestione e controllo aziendale, compreso il Sistema Informativo.
3. **ATTUABILITÀ** - Le misure organizzative ed i processi di lavoro devono essere concretamente attuabili in riferimento alla struttura dell'Ente e ai suoi processi operativi.
 4. **EFFICIENZA** - Il sistema dei controlli interni deve essere coerente con le caratteristiche dell'Ente e la complessità del Modello, con riferimento anche alla sostenibilità in termini economico-finanziari ed organizzativi.
 5. **DINAMICITÀ** - Il Modello e tutta la documentazione ad esso attinente devono essere oggetto di una costante attività di verifica e aggiornamento, attraverso un'analisi periodica e/o continuativa della sua efficacia ed efficienza.
 6. **UNITÀ** - Il Modello organizzativo deve essere sviluppato procedendo a una valutazione dei rischi e dei processi sensibili che abbracci l'intera organizzazione dell'Ente e non anche una sola parte.
 7. **CONDIVISIONE** - La diffusione nell'Ente dei principi stabiliti nel Modello garantisce l'attenzione al rispetto delle regole da parte di tutti coloro che lavorano per e con l'Ente stesso.
 8. **COERENZA** - I contenuti del Modello devono essere coerenti con le risultanze dell'attività di *risk assessment*.

5. La normativa di riferimento

Il D. Lgs. 231/2001, emanato in attuazione della delega di cui all'art. 11 della Legge 29 settembre 2000 n. 300, ha inteso conformare la normativa italiana in materia di responsabilità degli enti a quanto stabilito da alcune Convenzioni internazionali ratificate dal nostro Paese, tra cui la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

La sua entrata in vigore ha portato all'introduzione di una forma di responsabilità amministrativa degli enti, autonoma rispetto alla responsabilità penale delle persone fisiche autrici dei reati, derivante dalla commissione - o dalla tentata commissione - di alcuni illeciti espressamente richiamati dal Decreto (c.d. "reati presupposto"). Scopo della disciplina è quello di coinvolgere gli Enti nella punizione di taluni reati commessi nel loro interesse o a loro vantaggio.

Requisito essenziale per la imputabilità dell'Ente è che tali reati siano stati commessi da soggetti apicali o da sottoposti nell'interesse o a vantaggio dell'Ente medesimo. Quest'ultimo infatti non risponde se gli illeciti sono stati perpetrati dai predetti soggetti nell'interesse esclusivo proprio o di terzi (art. 5, comma 2). Occorre inoltre che l'illecito sia stato commesso nell'interesse o a vantaggio dell'Ente, dove l'*interesse* sussiste quando l'autore del reato ha agito con l'intento di favorire l'ente, indipendentemente dal fatto che poi tale obiettivo sia stato raggiunto, mentre il *vantaggio* sussiste quando l'ente ha tratto, o avrebbe potuto trarre, dal reato un risultato positivo, anche se non necessariamente di natura economica.

La violazione delle norme del Decreto comporta per l'Ente, oltre a sanzioni pecuniarie di rilevante entità, la possibile applicazione di misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la P.A., l'interdizione dall'esercizio

dell'attività, l'esclusione o revoca di finanziamenti e contributi ed il divieto di pubblicizzare beni e servizi.

5.1 I reati commessi da soggetti apicali

Entrando più nel particolare, il Decreto distingue tra reati commessi da soggetti apicali (la cui individuazione deve essere effettuata tenendo conto delle mansioni e delle funzioni in concreto svolte da ciascun soggetto e dalla conseguente capacità di esercitare un'influenza significativa sulla Banca o su un ramo di essa) e reati commessi da sottoposti (sostanzialmente costituiti da tutti coloro che sono legati all'Ente da rapporto di lavoro subordinato o parasubordinato, nonché i collaboratori esterni).

L'art. 6 stabilisce che, in caso di reato commesso da un soggetto apicale (dovendosi intendere per esso colui che riveste funzioni di rappresentanza dell'Ente - ad es. il Presidente - colui che amministra o dirige l'Ente - ad es. un Consigliere di Amministrazione o un Direttore Generale - o colui che esercita, anche di fatto, la gestione e il controllo di parte della Banca - ad es. un Direttore Amministrativo con autonomia di funzioni e spesa), l'Ente è esonerato da qualunque responsabilità se prova che:

- l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento è stato affidato ad un Organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo (ODV - Organismo di Vigilanza);
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo preposto.

Ciò sempre che il fatto-reato sia stato commesso eludendo fraudolentemente i controlli ed i presidi adottati dalla Banca.

In buona sostanza, nel caso di reato commesso da soggetti apicali sussiste in capo all'Ente una presunzione di responsabilità dovuta al fatto che tali soggetti esprimono e rappresentano la politica e, quindi, la volontà dell'Ente stesso; una presunzione, quest'ultima, che solo l'adozione del Modello e la relativa dimostrazione della sussistenza delle succitate condizioni consente di superare.

In tal caso, pur sussistendo la responsabilità personale in capo al soggetto apicale autore materiale del reato, l'Ente non è comunque responsabile anche laddove tale Soggetto abbia agito nell'interesse oppure a vantaggio della Banca.

5.2 I reati commessi da sottoposti

Analogamente, l'art. 7 del Decreto stabilisce la responsabilità amministrativa dell'ente per i reati dei sottoposti, se la loro commissione è stata resa possibile dall'inosservanza degli obblighi di direzione o di vigilanza.

In tale ipotesi, l'inosservanza di detti obblighi è esclusa se l'Ente dimostra di aver adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di organizzazione e gestione idoneo a prevenire reati della specie di quello verificatosi.

Pertanto, nell'ipotesi prevista dal succitato art. 7, contrariamente a quella di cui all'art.6, l'adozione del Modello di organizzazione costituisce una presunzione a suo favore, comportando l'inversione dell'onere della prova a carico dell'accusa che dovrà, quindi, dimostrare la mancata adozione ed efficace attuazione del Modello.

5.3 Le fattispecie di reato

La Sezione III del Decreto richiama i reati per i quali è configurabile la responsabilità amministrativa degli enti specificando l'applicabilità delle sanzioni per gli stessi.

Le prime versioni del Decreto, per via dell'origine comunitaria della disciplina in chiave anticorruzione, si riferivano ad una serie di reati tutti sostanzialmente riconducibili ai rapporti con la Pubblica Amministrazione, con l'obiettivo di sanzionare condotte di tipo corruttivo volte ad agevolare l'attività d'impresa. Nel corso degli anni l'elenco si è però notevolmente esteso, fino a ricomprendere gran parte delle fattispecie illecite riconducibili all'attività d'impresa.

Solo per completezza si fa presente che, alla data di redazione del presente aggiornamento le categorie di reati richiamate sono:

- vari delitti contro la Pubblica Amministrazione
- falsità in monete, in carte di pubblico credito e in valori di bollo
- reati societari, compresa la corruzione tra privati
- reati con finalità di terrorismo o di eversione dell'ordine democratico
- delitti contro la personalità individuale
- reati e illeciti amministrativi di manipolazione del mercato e di abuso di informazioni privilegiate
- 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
- reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita
- reati informatici
- delitti di criminalità organizzata
- delitti in materia di violazione del diritto d'autore
- delitti contro l'industria e il commercio
- reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
- relativi a pratiche di mutilazione degli organi genitali femminili
- reati ambientali
- reati di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare
- reati di razzismo e xenofobia
- reati transnazionali
- reati relativi alle attività di filiera degli oli vergini di oliva
- reati contro le frodi sportive
- reati fiscali

precisando comunque che la futura estensione della disciplina 231 ad altre categorie non inficerà la validità della presente Parte generale.

Come è facile intuire, non tutte le categorie di reato sono riconducibili alla attività effettivamente svolta dall'Ente (anzi: alcune di esse ne sono completamente estranee). Di ciò si terrà conto nella Parte speciale del presente Modello, in cui la valutazione del rischio-reato è tarata sulla attività effettivamente svolta dall'Ente e limitata alle sole categorie di illeciti in concreto rilevanti.

Si noti anche che non tutti i reati sono dolosi, ovvero per la cui realizzazione è necessaria la volontà e consapevolezza della loro realizzazione da parte dell'agente. Alcuni sono colposi, come quelli in materia di salute e sicurezza sul lavoro e taluni reati ambientali. Tale precisazione è importante sia per determinare la soglia di accettabilità del rischio reato (di cui si dirà nei paragrafi che seguono), sia per la concreta individuazione dei sistemi di controllo preventivo.

È importante anche sottolineare che i reati previste dal Decreto, per comportare la

responsabilità dell'Ente, non è necessario che siano commessi; tale responsabilità scatta anche solo se tentati. L'art. 26 co. 1 stabilisce infatti che, nei casi di realizzazione nella forma di tentativo dei delitti, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) siano semplicemente ridotte da un terzo alla metà, salvo precisare che ne sarà esclusa l'irrogazione laddove la Banca "impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento".

5.4 I requisiti del Modello

Il D.Lgs. 231 attribuisce un valore esimente al Modello di Organizzazione e Gestione nella misura in cui quest'ultimo risulti idoneo a prevenire i reati di cui al citato Decreto e, al contempo, le sue indicazioni vengano efficacemente attuate da parte degli organi dirigenti (in primis il Consiglio di Amministrazione).

Tale Modello, come sopra accennato, deve dunque rispondere ai seguenti requisiti:

- individuare le attività nel cui ambito esiste la possibilità che vengano commessi Reati 231;
- prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della Banca in relazione ai reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del modello;
- introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

5.5 Gli obiettivi

Con l'introduzione del Modello 231 la Banca, attraverso l'individuazione delle "attività sensibili ex D.Lgs. 231" e la definizione di prassi operative "idonee a prevenire i reati", si propone i seguenti obiettivi:

- rendere consapevoli tutte le persone facenti parte della struttura associativa, sia di governo sia esecutiva, che eventuali comportamenti illeciti possono comportare sanzioni penali ed amministrative sia per il singolo che per l'Ente;
- garantire l'esistenza di idonei presidi e controlli volti a garantire ed assicurare la correttezza dei comportamenti della Struttura stessa e delle persone che la rappresentano, nel rispetto della normativa esterna ed interna;
- rafforzare i meccanismi di controllo, monitoraggio e sanzionatori atti a contrastare la commissione di reati;
- enfatizzare le scelte in materia di conformità, di etica, di trasparenza, di correttezza perseguite dalla Banca, come pubblicizzate anche sul sito internet istituzionale del Movimento del Credito Cooperativo.

Obiettivo ultimo dell'adozione del Modello è, in definitiva, ottenere l'esonero da responsabilità della Banca per fatti-reati commessi dai suoi esponenti aziendali e dai suoi dipendenti, provando che:

i. in caso di reato presupposto commesso dai cosiddetti "soggetti apicali":

a) l'organo dirigente ha adottato (e provato di avere efficacemente attuato) prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi ed ha affidato ad un proprio organismo, dotato di autonomi poteri di iniziativa e di controllo, l'onere di vigilare e di curare il loro aggiornamento;

b) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione ovvero non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di controllo di cui al precedente punto 1.

ii. in caso di reato presupposto commesso da persone sottoposte alla direzione e alla vigilanza di un apicale:

a) non vi è stata inosservanza degli obblighi di direzione o vigilanza. Tale inosservanza è in ogni caso esclusa se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

L'onere di provare l'avvenuta adozione delle misure preventive ricadrà sulla Banca nel solo caso in cui l'autore del reato sia un soggetto apicale. Qualora, al contrario, l'autore del reato sia un soggetto sottoposto all'altrui direzione o vigilanza, l'onere probatorio relativo alla mancata adozione delle misure preventive spetterà all'Autorità Giudiziaria.

Se quello sopra menzionato è lo scopo principale dell'adozione del Modello, non è da sottacere, in quanto altrettanto importante, un ulteriore obiettivo: eseguire una check list dell'attività (processi, presidi organizzati e documentali, controlli) e garantirsi, attraverso il lavoro dell'Organismo di Vigilanza e la sua interlocuzione con gli organi di governo, un costante monitoraggio.

L'implementazione del Modello si inserisce infatti in una più ampia politica aziendale volta, unitamente ad altri strumenti di governance (a partire dal Codice Etico) a sensibilizzare coloro che operano in nome e per conto della Banca affinché tengano, nell'espletamento delle proprie attività, comportamenti corretti e conformi alle normative interne, tali da prevenire il rischio di commissione di reati o quantomeno ridurre tale rischio ad un livello di accettabilità, come meglio spiegato nel paragrafo successivo.

5.6 La definizione di rischio accettabile

Ad un qualunque sistema di controllo, fatta eccezione per casi particolarissimi relativi ad attività estremamente pericolose, non si può chiedere la garanzia assoluta che un rischio non sfoci mai in un fatto illecito. Quello che invece si può ragionevolmente pretendere è che il rischio di verificazione di tale fatto illecito sia minimizzato e ridotto ad un livello "accettabile".

Più in particolare, il rischio è considerato accettabile quando il controllo aggiuntivo per evitare il verificarsi di un evento ha un costo superiore a quello della risorsa da proteggere.

Ai fini 231, la soglia di accettabilità è rappresentata, nei *reati dolosi*, da

**un sistema di prevenzione tale da non potere essere aggirato
se non attraverso una condotta fraudolenta
da parte dell'autore materiale del reato**

Infatti, l'art. 6 del decreto prevede che l'Ente non risponda del reato se, tra le altre cose, riesce a provare che (lettera c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione.

Per i *reati colposi* il concetto di "elusione fraudolenta" appare difficilmente compatibile, mancando la necessità che vi sia stata volontà dell'evento lesivo, sia esso costituito dall'integrità fisica dei lavoratori o dell'ambiente. In questi casi, taluni hanno sostenuto la necessità di riferire il requisito dell'elusione fraudolenta del modello alla sola condotta inosservante della regola cautelare. Ne consegue, secondo tale interpretazione, che l'Ente, per andare esente da responsabilità, dovrebbe solo fornire la prova che non vi è stato alcun accordo con l'autore materiale del reato per eludere il modello. Dimostrazione, quest'ultima, compatibile con i reati colposi. Da ciò, inoltre, l'ulteriore corollario secondo cui

**il rischio, nei reati colposi, è considerato accettabile
quando l'evento dannoso si è verificato solo perché c'è stata una violazione delle
regole del MOG e delle normative di legge poste a presidio della sicurezza del luogo di
lavoro e dell'ambiente.**

5.7 Gli altri elementi fondamentali del Modello 231

Completano il Modello i seguenti elementi:

- il **SISTEMA ORGANIZZATIVO**, costituito dall'insieme organico di principi, regole, disposizioni, schemi organizzativi relativi alla gestione ed al controllo dell'attività sociale e strumentali, tra l'altro, alla realizzazione ed alla diligente gestione di un sistema di controllo delle attività sensibili – finalizzato alla prevenzione della commissione, o della tentata commissione, dei reati previsti dal Decreto. Ne fanno parte:

- lo Statuto sociale;
- il Codice etico;
- le deliberazioni del Consiglio di Amministrazione;
- le indicazioni del Collegio Sindacale;
- la normativa interna.

Tali disposizioni possono essere scritte od orali, di applicazione generale o limitate a categorie di soggetti od individui, permanenti o temporanee.

- l'**ORGANISMO DI VIGILANZA**, che è l'organo dell'Ente a cui è affidata la responsabilità di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento.

6. La redazione del Modello

Le attività svolte nella redazione del Modello e del presente aggiornamento sono state le seguenti:

a. Identificazione dei processi sensibili al rischio reato

La Banca, in ossequio a quanto previsto dall'art. 6 co. 2 lett. a), ha individuato le cosiddette "aree sensibili" o "a rischio", cioè i processi esposti al rischio di commissione di uno dei Reati 231.

In particolare, tale attività si è sostanziata:

- nella disamina della struttura aziendale, identificando soggetti apicali e sottoposti;
- nella individuazione dei processi aziendali, dei loro presidi documentali (Codici, Regolamenti, Ordini di Servizio, Note Operative) e dei relativi controlli;
- nella analisi dei reati previsti dal Decreto e individuazione delle possibili modalità di realizzazione della condotta illecita all'interno dei processi di lavoro (anche attraverso l'esemplificazione di alcune fattispecie concrete);
- nella individuazione della probabilità di accadimento del reato in relazione alla specifica attività sensibile precedentemente individuata.

L'esito di tale attività di verifica è riportato nella Parte Speciale. Si precisa che si tratta di un *work in progress*, tenuto conto che al suo interno saranno riportati di volta in volta i risultati del lavoro di costante valutazione ed aggiornamento da parte dell'Organismo di Vigilanza, che li sottoporrà alla disamina degli Organi di governo.

7. Il sistema organizzativo

7.1 Le linee Guida di categoria

L'art 6 comma 3 d.lg. 231 stabilisce che i Modelli di organizzazione, gestione e controllo possono essere adottati sulla base di Codici di comportamento (o Linee guida) redatte dalle associazioni rappresentative di categoria. Tra queste rientra anche l'Associazione Bancaria Italiana, che nel 2001 ha rilasciato una prima edizione aggiornata delle linee guida (poi aggiornata nel febbraio 2004) e che, nel febbraio 2019, ha partecipato alla stesura dei "Principi Consolidati per la redazione dei Modelli Organizzativi" insieme a CNF, Confindustria e CNDCEC.

Le Linee Guida ABI evidenziano la creazione all'interno delle banche, anche su impulso della Autorità di vigilanza, di un sistema integrato di controlli che coinvolge soggetti diversi. Particolare rilievo assume, in tale assetto organizzativo, la funzione di internal auditing, recentemente affidata alla Capogruppo ICCREA Banca.

Tale sistema consiste in un insieme di regole, procedure e funzioni di controllo che "devono mirare ad assicurare il rispetto delle strategie aziendali ed il conseguimento della efficacia e dell'efficienza dei processi aziendali; la salvaguardia del valore delle attività e la protezione dalle perdite; l'affidabilità e l'integrità delle informazioni contabili e gestionali; la conformità delle operazioni con la legge, con la normativa di vigilanza nonché con le politiche, i piani, i regolamenti e le procedure interne".

7.2 Il sistema organizzativo della banca

La Banca, in ossequio alle Linee Guida dell'ABI, ha variamente definito e documentato il proprio sistema organizzativo ed i relativi meccanismi di funzionamento, assolvendo all'impegno di aggiornarli costantemente per rispondere alle sue esigenze strategiche ed organizzative e per adeguarsi ai requisiti richiesti dalla normativa di legge e di settore.

Ferma restando l'osservanza di quanto previsto dalle fonti normative primarie e secondarie, i principali riferimenti documentali che regolano l'organizzazione della Struttura - e che sono stati esaminati ai fini della redazione del Modello - sono:

- a) lo Statuto: costituisce il documento fondamentale su cui è basato il sistema di governo societario della Struttura: definisce, la sede, l'oggetto sociale, il capitale sociale, nonché i compiti e le responsabilità dei soggetti apicali;
- b) il Codice Etico: rappresenta il compendio delle linee programmatiche e di condotta che guidano l'esistenza dell'Ente, fungendo da ausilio e supporto alla realizzazione ed implementazione di un valido modello di organizzazione e gestione;
- c) la Carta dei Valori, che esprime i valori sui quali si fonda l'azione della Banca, la sua strategia e la sua prassi. Racchiude le regole di comportamento e rappresenta gli impegni della Banca;
- d) la Carta della Coesione Sociale, strumento di riferimento per la gestione del rafforzamento del sistema a rete nonché una cornice valoriale che fissa i principi che orientano gli accordi collaborativi tra ciascuna BCC e gli altri soggetti del sistema del Credito Cooperativo.
- e) i Regolamenti aziendali: variamente definiti in base al grado di dettaglio (regolamenti, processi, note operative, ordini di servizio etc.), descrivono la struttura organizzativa e i processi di lavoro della Struttura, gli organi di governo, i compiti e le responsabilità

delle unità organizzative (un loro elenco completo è riportato nella Parte Speciale).

- f) Il Documento di Valutazione dei rischi ex art 17 del D. Lgs. n. 81/2008, che contiene una relazione sulla valutazione dei rischi per la sicurezza e la salute durante il lavoro, nella quale sono specificati i criteri adottati per la valutazione stessa; l'individuazione delle misure di prevenzione e di protezione e dei dispositivi di protezione individuale, conseguente alla valutazione dei rischi e il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza.

8. Il sistema dei controlli interni

La Banca, al fine di gestire e controllare con maggiore efficienza la propria attività, ha adottato alcune procedure di controllo volte ad assicurare il rispetto delle strategie aziendali e il conseguimento del corretto svolgimento dei processi operativi. Tali procedure sono così articolate:

1° livello

Controlli di linea, effettuati dalle stesse strutture produttive che hanno posto in essere le operazioni o incorporati nelle procedure e diretti ad assicurare il corretto svolgimento delle operazioni.

2° livello

Controlli sulla gestione dei rischi, condotti a cura di una struttura interna (Funzione di Risk Controlling/Management), contraddistinta dalla piena separatezza dalle funzioni operative, avente il compito di definire le metodologie di misurazione dei rischi, verificare il rispetto dei limiti assegnati alle varie funzioni operative e controllare la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio/rendimento, quantificare il grado di esposizione ai rischi e gli eventuali impatti economici; controlli di conformità normativa, svolti dalla Funzione indipendente all'uopo costituita con il compito specifico di promuovere il rispetto delle leggi, delle norme, dei codici interni di comportamento per minimizzare il rischio di non conformità normativa e i rischi reputazionali a questo collegati contribuendo, per gli aspetti di competenza, alla realizzazione del modello aziendale di monitoraggio e gestione dei rischi.

3° livello

Attività del Collegio Sindacale, delle funzioni di revisione interna (Internal Auditing) ed esterna (Società di revisione), volta a valutare l'adeguatezza e la funzionalità del complessivo Sistema dei Controlli Interni e ad individuare andamenti anomali delle procedure e della regolamentazione.

8.1 Consigliere con delega al Sistema dei Controlli Interni ed il Comitato Rischi

Nel sistema dei controlli interni riveste particolare importanza il "Consigliere con delega al Sistema dei Controlli Interni", nominato presso ciascuna Banca Affiliata del Gruppo nei casi in cui non venga istituito, sulla base di quanto previsto dalle politiche di governo societario del GBCI, un Comitato Rischi.

Il suddetto Comitato (ove istituito) svolge, in linea con le politiche del Gruppo, i seguenti compiti:

- fornisce il proprio parere al Consiglio di Amministrazione in relazione alle proposte di nomina dei Responsabili delle Funzioni Aziendali di Controllo e del Delegato SOS;

- interloquisce direttamente con i Responsabili delle Funzioni Aziendali di Controllo della propria Entità e ne segue costantemente le attività e le relative risultanze;
- monitora l'esecuzione delle linee di indirizzo definite dal Consiglio di Amministrazione, nonché dagli Organi Aziendali della Capogruppo, avvalendosi dell'apporto delle Funzioni Aziendali di Controllo, valutando costantemente l'adeguatezza e l'efficacia del Sistema di Controllo Interno;
- esamina preventivamente i piani delle attività, le relazioni annuali e gli ulteriori flussi informativi relativi alle attività di controllo svolte dalle Funzioni Aziendali di Controllo ed indirizzate al Consiglio di Amministrazione;
- esprime valutazioni e formula pareri al Consiglio di Amministrazione sul rispetto dei principi cui devono essere uniformati il Sistema dei Controlli Interni e l'organizzazione aziendale.

8.2 Le attività sensibili (ex art.6 co.2 lett. a)

Nel corso dell'analisi effettuata sono stati espressamente individuati, per ogni attività sensibile, gli strumenti del sistema organizzativo interno (Regolamenti, Controlli etc.) posti a presidio, valutandone il grado di idoneità rispetto alla capacità di prevenzione dei comportamenti illeciti.

Per l'individuazione delle attività sensibili è stata analizzata, insieme al personale della Banca, la realtà operativa aziendale. In particolare, per ogni attività a potenziale rischio di commissione reati sono stati raccolti i seguenti dati:

- l'effettivo svolgimento dell'attività sensibile presso la struttura, al fine di limitare l'analisi al perimetro di effettivo rischio aziendale;
- il soggetto responsabile dell'attività (Unità Organizzativa o Funzione);
- il processo di riferimento;
- le contromisure adottate (normativa, poteri di firma e poteri autorizzativi, segregazione dell'attività, tracciabilità, altri presidi);
- l'indicazione delle criticità emerse e delle aree di miglioramento, sempre in ottica di prevenzione dei reati

prendendo in considerazione i regolamenti aziendali come sopra definiti e le Unità operative (uffici, funzioni) interessate a presidiare e/o controllare le suddette attività.

Le risultanze di tale analisi costituiscono, come sopra precisato, il contenuto della Parte Speciale del presente Modello.

8.3 I principi di controllo

In linea generale, i principi di controllo che devono sovrintendere all'attività dell'Ente possono essere così riassunti:

- a) ogni operazione deve essere documentabile e successivamente verificabile;
- b) la verificabilità deve essere garantita nel tempo attraverso misure, anche informatiche, che prevengono la perdita e l'alterabilità dei dati;
- c) ogni processo non può essere svolto in autonomia da un solo soggetto (c.d. principio di segregazione);
- d) i poteri dei singoli, oltre a non essere illimitati, devono essere chiaramente definiti e conosciuti all'interno dell'organizzazione;
- e) i poteri autorizzativi devono essere coerenti con le responsabilità;
- f) i controlli devono essere documentati.

9. L'Organismo di Vigilanza

In attuazione delle disposizioni previste dal Decreto, il Consiglio di Amministrazione ha deliberato di costituire un Organismo di Vigilanza con la responsabilità di vigilare sul funzionamento e l'osservanza del Modello 231 e di individuarne gli eventuali interventi correttivi, proponendone allo stesso Consiglio di Amministrazione l'aggiornamento.

L'Organismo di Vigilanza, che gode di autonomia finanziaria avendo ricevuto dal CdA massima disponibilità a far fronte ad ogni motivata richiesta di fondi per lo svolgimento della sua attività indipendentemente dalla individuazione di uno specifico budget, è tenuto a:

- promuovere, coordinandosi con le funzioni aziendali competenti, idonee iniziative per la diffusione della conoscenza e della comprensione dei principi del Modello 231, definendo specifici programmi di informazione/formazione e comunicazione interna;
- riferire periodicamente al Consiglio di Amministrazione e al Comitato dei Sindaci circa lo stato di attuazione del Modello 231;
- definire e comunicare alle strutture della Banca, previa informativa al Consiglio di Amministrazione, i flussi informativi che debbono essergli inviati con indicazione dell'unità organizzativa responsabile dell'invio, della periodicità e delle modalità di comunicazione;
- definire e comunicare a tutte le strutture della Banca le modalità con cui effettuare le segnalazioni;
- valutare le eventuali segnalazioni;
- accertare e segnalare al Consiglio di Amministrazione, per gli opportuni provvedimenti, le violazioni del Modello 231 che possano comportare l'insorgere di responsabilità;
- proporre al Consiglio di Amministrazione l'adozione di eventuali provvedimenti disciplinari a seguito di violazioni del Modello 231.

Per completezza si riportano qui di seguito le indicazioni dettate dalla Capogruppo sulle principali responsabilità ascrivibili all'Organismo di Vigilanza ex d.lgs. n. 231/2001:

“L'Organismo di Vigilanza ai sensi del D.Lgs. 231/2001 (di seguito alternativamente anche “OdV”), ove presente presso le singole Entità del GBCI, vigila sull'efficace attuazione, sul funzionamento, sull'osservanza e sull'aggiornamento del modello di organizzazione, gestione e controllo previsto dalla normativa in parola e sulla sua adeguatezza a prevenire e contrastare la commissione dei reati presupposto del Decreto. Al fine di adempiere alle proprie responsabilità in materia, l'OdV propone e verifica le iniziative più idonee a diffondere presso gli Organi Aziendali, tra il personale e i fornitori di beni e servizi del GBCI la conoscenza ed il rispetto del Codice Etico di Gruppo e del modello suddetto. L'OdV per l'adempimento dei compiti allo stesso attribuiti, può avvalersi del supporto delle Funzioni Aziendali di Controllo per ottenere informazioni, in possesso di quest'ultime, in merito alla valutazione dei rischi in relazione agli ambiti di proprio interesse. Le Funzioni Aziendali di Controllo forniscono all'Organismo di Vigilanza informazioni su particolari violazioni o carenze rilevanti riscontrate nelle materie di interesse durante lo svolgimento delle proprie attività pianificate”.

10. I flussi informativi

L'Organismo di Vigilanza ha la responsabilità di vigilare sul funzionamento e l'osservanza del Modello 231 e di provvedere al relativo aggiornamento.

Cardine di tale funzione è l'attività di segnalazione, da parte dei destinatari della normativa, di tutti quegli eventi che potrebbero far sorgere una responsabilità della Banca ai sensi del Decreto.

A tal fine l'Organismo di Vigilanza:

- accede a tutti i documenti ed informazioni aziendali rilevanti per lo svolgimento delle funzioni ad esso attribuite senza necessità di autorizzazioni, fermo restando l'obbligo di riservatezza relativamente alle informazioni acquisite;
- si avvale, previa richiesta al Consiglio di Amministrazione, di soggetti terzi di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello 231;
- richiede alla Struttura di fornire tempestivamente le informazioni, i dati e/o le notizie necessarie per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi del Modello e per la verifica dell'effettiva attuazione dello stesso;
- riceve ogni comunicazione rilevante o comunque pertinente ai fini del rispetto della normativa 231;
- riceve le comunicazioni inoltrate alla Banca dai dirigenti e/o dai dipendenti di avvio di procedimenti giudiziari a loro carico;
- riceve i rapporti predisposti nell'ambito delle attività di controllo da funzioni interne e/o da soggetti esterni;
- riceve i verbali delle Autorità Giudiziaria e di Vigilanza di settore dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle norme del Decreto 231.

Al fine di consentire la segnalazione da parte dei destinatari del presente Modello 231 di eventuali notizie relative alla commissione o al tentativo di commissione dei reati oltre che di violazione delle regole previste dal Modello 231 stesso, la Banca si impegna a garantire idonei canali di comunicazione nei confronti dell'Organismo di Vigilanza, anche tramite uno specifico indirizzo di posta elettronica.

In generale, la gestione dei c.d. "flussi informativi", deve avvenire nel rispetto delle seguenti indicazioni:

- le segnalazioni devono essere inviate all'ODV dal Responsabile dell'Unità Organizzativa o dalla Funzione di riferimento (tra cui possono rientrare anche il CdA o il Collegio Sindacale), con la frequenza o al verificarsi degli eventi individuata nel Modello per ciascuna categoria di Reati;
- è data comunque facoltà a chiunque di inviare una segnalazione all'ODV, non anonima, anche senza il coinvolgimento del superiore gerarchico. Tali segnalazioni dovranno rivestire la forma scritta, sebbene senza alcuna necessità di formule sacramentali;
- l'ODV sarà libero di compiere tutte le attività di indagine ed istruttorie ritenute a sua discrezione utili e/o opportune per verificare la fondatezza della segnalazione, avendo preliminarmente ricevuto dalla Banca garanzia di massima collaborazione nelle indagini;
- l'ODV, nei casi in cui particolari esigenze lo richiedano, garantirà la riservatezza dell'identità del segnalante, fatta eccezione per i casi in cui ciò non sia possibile per rispettare un obbligo di legge o per consentire il diritto di difesa alla Banca o alle persone eventualmente menzionate nella segnalazione.

L'invio e la ricezione dei flussi informativi avverrà attraverso messaggi di posta elettronica che coinvolgeranno l'ODV, il CdA, il Collegio Sindacale e gli Uffici interni. Questi ultimi godranno di ampia autonomia in merito all'invio dei c.d. "flussi ad evento" e potranno essere chiamati a rispondere a specifici quesiti dell'ODV in risposta a specifiche richieste.

A tal proposito si osserva che la qualità dei flussi informativi si declina però non solo in termini di idoneità a rappresentare effettivamente il fenomeno monitorato (capacità segnaletica) e di attendibilità, nel senso che il dato riportato deve essere veritiero e corretto, ma anche in termini di tempestività ed aggiornamento, nel senso che le informazioni devono essere il più possibile attuali rispetto al periodo di osservazione.

Per questo motivi la Banca, consapevole dell'opportunità che l'OdV riceva con tempestività flussi informativi su una molteplicità di materie (ad esempio: (a) controlli inerenti la gestione delle risorse finanziarie; (b) formazione; (c) provvedimenti disciplinari; (d) profili legati alla sicurezza informatica ed ai reati cd. informatici; (e) sicurezza sui luoghi di lavoro; (f) antiriciclaggio e rischi connessi (autoriciclaggio, ricettazione); g) rapporti con la Pubblica Amministrazione etc.), ha introdotto un Sistema di flussi che, superando la tradizionale dicotomia tra "flussi periodici" e "flussi ad evento", prevede che la maggior parte delle informazioni sia inviata all'OdV al verificarsi di fatti più o meno significativi (e quindi sia "ad evento"). Tale scelta consente, a parere della Banca, la massima tempestività nella trasmissione delle informazioni rilevanti, non dovendosi mai attendere una scadenza temporale predefinita (qualunque ne sia la periodicità).

Tale Sistema, per calmierare il rischio che alcune informazioni, ancorché rilevanti, non siano state comunque portate a conoscenza dell'OdV, prevede inoltre un doppio meccanismo di salvaguardia, in forza del quale l'Organismo:

- almeno una volta l'anno, riceve da parte di tutte le Unità coinvolte nell'invio dei Flussi una "attestazione del rispetto delle norme di comportamento prescritte nel MOG", così che le suddette Unità possano colmare eventuali inosservanze/ritardi/lacune informative che, per negligenza o altro, hanno impedito all'OdV di conoscere di un fatto;
- può richiedere il rilascio di tale attestazione da qualunque Unità Operativa ogni qual volta lo ritenga opportuno, senza vincoli di periodicità.

ATTENZIONE: l'identificazione di coloro che saranno tenuti all'invio dei flussi è di fondamentale importanza. I soggetti che potrebbero venire a conoscenza del fatto-reato (o comunque dell'evento che l'ODV chiede di conoscere) potrebbero infatti essere molti, con conseguente rischio che ciascuno di essi, confidando nell'altrui segnalazione (in realtà mai avvenuta) omettano di farla, bloccando il flusso informativo.

11. Il sistema disciplinare

Elemento essenziale per il funzionamento del Modello 231 è l'introduzione di un sistema disciplinare idoneo a sanzionare gli eventuali comportamenti ed attività contrastanti con le misure indicate.

Al riguardo, l'art. 6 comma 2 lett. e) prevede che i modelli di organizzazione e gestione devono "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello". Il mancato rispetto delle misure, previste dal Modello 231, viene valutato sotto il profilo disciplinare seguendo modalità differenti a seconda che si tratti di "soggetti sottoposti a direzione o vigilanza" (art. 5, comma 1, lett. b) ovvero di "soggetti apicali" (art. 5, comma 1, lett. a).

11.1 Principi generali in tema di sanzioni disciplinari

L'avvio di un procedimento disciplinare e l'eventuale emanazione delle sanzioni disciplinari, che non potrà trascurare il rispetto della legislazione vigente (ed in particolare dall'art. 2106 del Codice Civile e dell'art. 7 dello Statuto dei Lavoratori), prescinde sia dalla rilevanza penale della condotta sia dalla conclusione dell'eventuale procedimento penale avviato dall'Autorità Giudiziaria nel caso in cui il comportamento da censurare integri una fattispecie di reato. Pertanto, l'applicazione delle sanzioni potrà avere luogo anche se il destinatario abbia posto in essere esclusivamente una violazione dei principi sanciti dal Modello organizzativo o dal Codice Etico.

Saranno ad esempio applicabili sanzioni disciplinari alle seguenti condotte:

- l'inoltro con dolo o colpa grave di segnalazioni all'ODV che si rivelano infondate;
- l'omissione fraudolenta di fatti che, ai sensi del Modello, devono essere portati a conoscenza dell'ODV, al fine di impedire/evitare/ritardare i controlli;
- il compimento di atti ritorsivi o discriminatori nei confronti dei soggetti segnalanti per motivi collegati, direttamente o indirettamente, alla segnalazione, con particolare riferimento alle violazioni delle misure poste a tutela della riservatezza del segnalante.

11.2 Misure nei confronti del personale dipendente

Entrando più nel dettaglio delle singole sanzioni, quando la violazione delle regole comportamentali previste nel Modello sarà commessa da dipendenti destinatari del Contratto Collettivo Nazionale del Lavoro, troveranno applicazione i provvedimenti disciplinari previsti nel suddetto CCNL, che allo stato attuale della normativa sono rappresentate, in ordine di gravità, da: (1) rimprovero verbale; (2) biasimo scritto; (3) sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni; (4) licenziamento per giustificato motivo; (5) licenziamento per giusta causa.

Senza pretesa di completezza ed a titolo esemplificativo, fermo restando che l'individuazione della sanzione applicabile al caso concreto spetterà al datore di lavoro, qui di seguito vengono elencate alcune condotte integranti la violazione del Modello 231 che dovranno essere valutate sotto il profilo disciplinare:

- condotte non conformi alle prescrizioni indicate nel Modello e nei diversi presidi documentali aziendali che ne costituiscono il fondamento (statuto, regolamenti, processi, ordini di servizio, note operative etc.);
- violazioni agli obblighi di informativa nei confronti dell'Organismo di Vigilanza, sia mediante comportamenti omissivi (ad es. mancato o ritardato invio, con colpa grave o dolo, di un Flusso in presenza delle circostanze individuate dal sistema dei Flussi) che commissivi (ad es. invio di un Flusso con dati incompleti o non veritieri);
- condotte che, oltre a essere non conformi alle prescrizioni del Modello, hanno arrecato un danno alla Banca (economico, all'integrità dei suoi beni o reputazionale) od abbiamo esposto il suo personale ad una situazione di pericolo;
- condotte che sono state adottate allo scopo precipuo di compiere una condotta illecita rilevante ai sensi del Decreto 231 o che abbiano determinato il rischio – se non addirittura l'irrogazione - di sanzioni previste dal Decreto 231 a carico della Banca.

11.3 Misure nei confronti dei soggetti apicali

Si premette che le sanzioni previste a carico dei soggetti apicali per le violazioni del Modello 231 costituiscono sanzioni "convenzionali", irrogabili solo laddove tali soggetti si siano impegnati contrattualmente, all'atto della nomina o con successiva adesione, a rispettare le previsioni del Modello e a soggiacere alle sanzioni ivi stabilite.

In tali ipotesi, potranno essere applicate le sanzioni della ammonizione (sia verbale che scritta), la sanzione pecuniaria (fino alla misura massima deliberata dal Consiglio di Amministrazione o, in mancanza di delibera, fino ad un massimo di 10.000 Euro), la revoca da una o più deleghe e, nei casi più gravi, la destituzione dalla carica. Potranno trovare inoltre applicazione le sanzioni previste dal Codice Civile, per la cui individuazione ed irrogazione si rimanda alla normativa vigente.

In tutti i casi dovrà essere rispettato il principio della proporzionalità della sanzione rispetto alla gravità dell'infrazione commessa.

12. Formazione e Informazione.

Il Modello 231 è portato a conoscenza di tutti i destinatari mediante appositi interventi di comunicazione e formazione al fine di garantire la massima diffusione dei principi ispiratori e delle regole di condotta.

La divulgazione del Modello organizzativo non è infatti sufficiente ai fini dell'efficace attuazione del modello organizzativo. Il suo corretto funzionamento presuppone che i soggetti interessati – siano essi apicali o subordinati – ne siano adeguatamente informati e che questi siano messi in condizione, attraverso specifici interventi formativi, di usufruire correttamente dei sistemi, informatici o di altra natura, volti alla segnalazione dei reati o delle irregolarità.

La formazione dovrà essere appropriatamente tarata in funzione dei ruoli/livelli dei destinatari e dovrà riguardare sia la disciplina sulla responsabilità amministrativa degli enti in generale che l'analisi e l'illustrazione del Modello organizzativo specifico della propria realtà di lavoro.

13. Il Whistleblowing

Il "whistleblowing" è la segnalazione compiuta da un lavoratore che, nello svolgimento delle proprie mansioni, si accorge di una frode, un rischio o una situazione di pericolo che possa arrecare danno all'azienda per cui lavora, nonché a clienti, colleghi o qualunque altra categoria di soggetti.

Il 14 dicembre 2017 è stata pubblicata nella Gazzetta Ufficiale n. 291 la Legge 30.11.2017 n. 179, recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato", allo scopo di riformare la materia del whistleblowing estendendola dal settore pubblico (nella quale era stata introdotta con la legge 190/2012) a quello privato (che fino a quel momento la prevedeva in via obbligatoria solo per determinate categorie di soggetti - sostanzialmente le sole banche, ex art. 52 Tub).

La Legge 179 ha integrato dell'art. 6 del Decreto 231/2001, inserendo 4 nuovi commi all'articolo 6 del Decreto. La disciplina prevede ora l'obbligo (comma 2-bis), per ogni Ente che si sia munito di un Modello di Organizzazione, di prevedere adeguati canali informativi che consentano ai segnalanti di "presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti".

13.1 Whistleblowing e contenuto del Modello

Per rispondere alle caratteristiche di idoneità previste dalla legge, il Modello adottato dalla Banca recepisce la normativa sul whistleblowing.

In questo contesto l'Organismo di Vigilanza, unitamente al Responsabile delle Segnalazioni, ha il compito di:

- verificare che il Modello contenga, nella Parte Generale, una specifica sezione dedicata alla normativa in oggetto e, nella Regolamentazione interna, la previsione espressa di sanzioni connesse alla violazione del divieto di atti di ritorsione nei confronti dei segnalanti e all'utilizzo abusivo dei canali di segnalazione;
- dare indicazioni affinché sia predisposta una specifica procedura che disciplini le modalità di segnalazione, mediante la predisposizione di almeno due canali, di cui uno informatico;

- verificare il buon funzionamento dei canali informativi predisposti in applicazione della disciplina, sia in termini di possibilità di inoltrare correttamente le segnalazioni che in termini di garanzia di riservatezza (se non di anonimato, se espressamente consentito) nell'intero processo di gestione della segnalazione.

L'ODV dovrà inoltre vigilare nel continuo sul rispetto dei divieti di ritorsione o di compimento di atti discriminatori nei confronti dei segnalanti per motivi collegati, direttamente o indirettamente, alle segnalazioni" (art. 6 comma 2-bis lett. c del Decreto), come ad es. demansionamenti e trasferimenti, accertandosi che la violazione di tali divieti sia espressamente prevista nel sistema disciplinare aziendale e che sia parimenti sanzionato chi "effettui con dolo o colpa grave segnalazioni che si rivelano infondate".

14. La privacy

Tra i reati presupposto del Decreto figurano alcune condotte attinenti alla normativa sulla privacy, la cui disciplina è contenuta nel Regolamento UE 2016/679 (c.d. GDPR - General Data Protection Regulation), in vigore dal 25.05.2018.

In particolare, l'art. 24-bis, rubricato "Delitti informatici e trattamento illecito dei dati", punisce con sanzioni pecuniarie e talvolta interdittive numerose condotte: accesso abusivo ad un sistema informatico; detenzione e diffusione abusiva di codici di accesso a sistemi informatici; diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche; frode informatica del soggetto che presta servizi di certificazione di firma elettronica; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblica utilità.

Alcune delle ipotesi delittuose sopra richiamate, alla luce della nuova normativa privacy, richiedono da parte dell'Organismo di Vigilanza un costante monitoraggio del processo di adeguamento alla normativa, tenuto conto del fatto che, nonostante la Banca non sia assoggettata agli obblighi di nomina di un DPO (Data Protection Officer) e di tenuta del c.d. Registro dei trattamenti, tratta comunque dati relativi a prestazioni sanitarie, come tali rientranti nel concetto di "particolari di dati personali" (art. 9 GDPR).