MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del Decreto Legislativo n. 231/2001

Approvato dal Consiglio di Amministrazione con delibera del 28 settembre 2021

Aggiornamento n.1 del 28 maggio 2024

carifermo
cassa di risparmio di fermo s.p.a.

INDICE

PREMESSA

Il presente documento descrive il Modello di Organizzazione, Gestione e Controllo ai sensi del Decreto Legislativo 231/2001 adottato dalla Cassa di Risparmio di Fermo S.p.a. (di seguito anche "Carifermo" o "la Banca"), volto a prevenire la commissione dei reati presupposto individuati all'interno del Decreto.

GLOSSARIO

Nel presente documento si intendono per:

- ABI: Associazione Bancaria Italiana

- Apicali: le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Banca o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché 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).

- Attività a rischio/attività sensibile: attività svolte dalla Banca, nel cui ambito possono in linea di principio essere commessi i reati di cui al D.Lgs 231/2001 così come identificate nelle Parti Speciali del Modello;

- Autorità di Vigilanza: si intendono le Autorità di regolamentazione e controllo delle banche;

- Autorità: si intendono le Autorità di Vigilanza o altre Autorità;

- Azienda/Banca/Società: Cassa di Risparmio di Fermo S.p.a. o Carifermo;

- Codice Etico: il Codice Etico adottato dalla Banca;

- Destinatari: (i) persone fisiche che rivestano funzioni di rappresentanza, amministrazione o direzione della Banca o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo della Banca medesima; (ii) persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati;

- Dipendenti o Personale dipendente: tutti i dipendenti della Banca (compresi i dirigenti);

- Disposizioni interne: insieme dei Regolamenti, delle Policy e delle norme interne adottate dalla Banca;

- D.Lgs.231/2001 o Decreto: il Decreto Legislativo 8 giugno 2001 n.231, recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni, anche prive di personalità giuridica, a norma dell'articolo 11 della Legge 29 settembre 2000, n.300" e successive modifiche ed integrazioni;

- D.Lgs.231/2007: il decreto legislativo n. 231 del 21 novembre 2007 "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" e successive modifiche ed integrazioni;

- Ente: soggetto dotato di personalità giuridica, società ed associazioni anche prive di personalità giuridica;

- Funzionigramma: documento in cui sono indicate le Aree, le Direzioni, gli Uffici, le Funzioni, le Filiali/Agenzie della Banca nonché le responsabilità poste in capo a ciascuna di esse;

- Linee Guida ABI: Linee Guida dell'Associazione Bancaria Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche (rilevanti ai sensi dell'art. 6, comma 3, del D. Lgs. 231/01 in quanto redatte da associazione rappresentativa di categoria e comunicate al Ministero della Giustizia).

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

- Organismo di Vigilanza (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 e di curarne l'aggiornamento, avente i requisiti di cui all'art. 6, comma 1, lettera b) del D. Lgs. n. 231/2001.

- Organi Sociali: Assemblea, Consiglio di Amministrazione, Comitato Esecutivo e Collegio Sindacale;

- Organigramma: documento nel quale è schematizzata l'intera struttura organizzativa della Banca;

- P.A.: la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio, intesa in senso lato e tale da ricomprendere anche le Autorità di Vigilanza e le Autorità fiscali, oltre che la Pubblica Amministrazione di Stati esteri;

- Reato/reato presupposto/illecito penale/fattispecie incriminatrice: i reati richiamati nel D.Lgs.231/2001;

- Responsabilità amministrativa: responsabilità amministrativa della Banca in caso di commissione di uno dei reati presupposto previsti dal D.Lgs. 231/01 da parte di un dipendente o soggetto apicale;

- Sottoposti: le persone sottoposte alla direzione o alla vigilanza dei Soggetti Apicali (art.5, comma 1, lettera b)).

1 IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO DAL DECRETO LEGISLATIVO 231/2001

Il D. Lgs. n. 231/2001 (d'ora innanzi il Decreto), recante "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica", emanato in attuazione della legge delega 29 settembre 2000, n. 300, ha adeguato la normativa italiana in materia di responsabilità amministrativa delle persone giuridiche ad alcune convenzioni internazionali quali:

- 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 dei funzionari della Comunità europea o degli Stati membri;
- la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Il D.Lgs.231/2001 ha introdotto nell'ordinamento nazionale una peculiare forma di responsabilità, nominalmente amministrativa, ma sostanzialmente a carattere afflittivo-penale a carico degli Enti per reati tassativamente elencati e commessi nel loro interesse o vantaggio:

i) da persone fisiche che rivestono posizioni c.d. "apicali", ossia che esercitino funzioni di rappresentanza, di amministrazione o di direzione degli enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione ed il controllo degli enti medesimi;

ii) da persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.

La responsabilità dell'ente va ad aggiungersi alla responsabilità della persona fisica che ha materialmente commesso determinati fatti illeciti ed è autonoma rispetto ad essa.

L'Ente può essere chiamato a rispondere solo della commissione di reati e illeciti tassativamente previsti dal D.Lgs.231/2001, nella formulazione risultante dal suo testo originario e dalle successive integrazioni, nonché dalle leggi che espressamente richiamano la disciplina del Decreto.

I presupposti applicativi della normativa possono essere, in estrema sintesi, indicati come segue:

a) L'inclusione dell'Ente nel novero di quelli rispetto ai quali il Decreto trova applicazione;
b) L'avvenuta commissione di un reato compreso tra quelli elencati dal Decreto (c.d. "reati presupposto"), nell'interesse o a vantaggio dell'Ente;
c) L'essere l'autore del reato un soggetto investito di funzioni apicali o subordinate all'interno dell'Ente;
d) La mancata adozione o attuazione da parte dell'Ente di un modello organizzativo idoneo a prevenire la commissione di reati del tipo di quello verificatosi;
e) Il mancato affidamento di autonomi poteri di iniziativa e controllo ad un apposito organismo dell'Ente (o l'insufficiente vigilanza da parte di quest'ultimo);

f) L'elusione fraudolenta da parte del soggetto apicale o subordinato del modello di prevenzione adottato dall'Ente stesso.

Oltre all'esistenza dei richiamati requisiti, che consentono di collegare oggettivamente il reato all'Ente, il legislatore ha richiesto la presenza di un requisito soggettivo, identificato in una "colpa organizzativa", intesa come stato imputabile all'Ente consistente nel non aver istituito un efficiente ed efficace sistema di prevenzione dei reati indicati dal Decreto. Pertanto, nel caso in cui sia commesso uno dei reati previsti dal Decreto, alla responsabilità penale della persona fisica che ha materialmente realizzato il fatto illecito si aggiunge la responsabilità "amministrativa" dell'ente.

Dal concorso di tutte queste condizioni consegue l'assoggettabilità dell'Ente a sanzioni di svariata natura, accomunate dal carattere particolarmente gravoso, tra le quali spiccano per importanza quella pecuniaria e quelle interdittive, variamente strutturate (fino alla chiusura coattiva dell'attività).

1.1 La tipologia di reati integranti la Responsabilità degli Enti (i c.d. "reato presupposto")

Originariamente prevista per i reati contro la Pubblica Amministrazione (di seguito anche "P.A."), o contro il patrimonio della P.A., la responsabilità degli enti è stata estesa – per effetto di provvedimenti normativi susseguitisi nel corso del tempo – a numerosi altri reati e illeciti amministrativi.

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

- Reati commessi nei rapporti con la Pubblica Amministrazione (art. 24 D.Lgs.231/2001) [Articolo modificato dalla L.161/2017 e dal D.Lgs.75/2020];

- Delitti informatici e trattamento illecito di dati (art.24-bis D.Lgs.231/2001) [Articolo aggiunto dalla L.48/2008, modificato dal D.Lgs.n.7 e 8/2016 e dal D.L. n.105/2019];

- Reati in materia di criminalità organizzata (art.24-ter D.Lgs.231/2001) [Articolo aggiunto dalla L.94/2009 e modificato dalla L.69/2015];

- Reati commessi nei rapporti con la Pubblica Amministrazione (art.25 D.Lgs.231/2001) [Articolo modificato dalla L.190/2012, dalla L.3/2019 e dal D.Lgs.75/2020];

- Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art.25-bis D.Lgs.231/2001) [Articolo aggiunto dal D.L.350/2001 convertito con modificazioni in L.409/2001; modificato poi dalla L.99/2009 e modificato dal D.Lgs.125/2016];

- Delitti contro l'industria e il commercio (art.25-bis.1 D.Lgs.231/2001) [Articolo aggiunto dalla L.99/2009];

- Reati societari (art.25-ter D.Lgs.231/2001) [Articolo aggiunto dal D.Lgs.61/2002; modificato dalla L.190/2012, dalla L.69/2015 e dal D.Lgs.38/2017];

- Reati con finalità di terrorismo o di eversione dell'ordine democratico (art.25-quater D.Lgs.231/2001) [Articolo aggiunto dalla L.7/2003];

- Pratiche di mutilazione degli organi genitali femminili (art.25-quater1 D.Lgs.231/2001) [Articolo aggiunto dalla L.7/2006];

- Reati contro la personalità individuale (art.25-quinquies D.Lgs.231/2001) [Articolo aggiunto dalla L.228/2003, modificato dalla L.199/2016];

- Abusi di mercato (art.25-sexies D.Lgs.231/2001) [Articolo aggiunto dalla L.62/2005];

- Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza del lavoro (art.25-septies D.Lgs.231/2001) [Articolo aggiunto dalla L.123/2007, modificato dalla L.3/2018];

- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio (art.25-octies D.Lgs.231/2001) [Articolo aggiunto dal D.Lgs.231/2007 e modificato dalla L.186/2014];

- Delitti in materia di strumenti di pagamento diversi dai contanti (art.25-octies.1 D.Lgs.231/2001) [Articolo aggiunto dal D.Lgs.184/2021 e modificato dalla L.137/2023];

- Delitti in materia di violazione del diritto d'autore (art.25-novies D.Lgs.231/2001) [Articolo aggiunto dalla L.99/2009];

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art.25-decies D.Lgs.231/2001) [Articolo aggiunto dalla L.116/2009];

- Reati ambientali (art.25-undecies D.Lgs.231/2001) [Articolo aggiunto dal D.Lgs.121/2011, modificato dalla L.68/2015 e poi dal D.Lgs.21/2018];

- Reati di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art.25-duodecies D.Lgs.231/2001) [Articolo aggiunto dal D.Lgs.109/2012, modificato dalla L.161/2017];

- Razzismo e Xenofobia (art.25-terdecies D.Lgs.231/2001) [Articolo aggiunto dalla L.167/2017, modificato dal D.Lgs.21/2018];

- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art.25-quaterdecies D.Lgs.231/2001) [Articolo aggiunto dalla L.39/2019];

- Reati Tributari (art.25-quinquiesdecies D.Lgs.231/2001) [Articolo aggiunto dalla L.157/2019 e dal D.Lgs.75/2020];

- Contrabbando (art.25-sexiesdecies D.Lgs.231/2001) [Articolo aggiunto dal D.Lgs.75/2020];

- Delitti contro il patrimonio culturale (art.25-septiesdecies D.Lgs.231/2001) [Articolo aggiunto dalla L.22/2022 e modificato dalla L.6/2024];

- Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici (art.25-duodevicies D.Lgs.231/2001) [Articolo aggiunto dalla L.22/2022];

- Reati Transnazionali (art.10 L. 16 marzo 2006, n.146).

I reati presupposto contemplati dal Decreto sono descritti nell'allegato "Catalogo Reati", oggetto di aggiornamento in occasione di eventuali successivi interventi legislativi.

1.2 Le Sanzioni a carico dell'Ente

Sotto il profilo sanzionatorio, la responsabilità introdotta dal Decreto coinvolge principalmente il patrimonio dell'ente che ha tratto vantaggio dalla commissione del reato. Per tutti gli illeciti è prevista l'applicazione di una sanzione pecuniaria; mentre per le ipotesi di maggiore gravità sono previste anche misure interdittive.

Le sanzioni amministrative per gli illeciti amministrativi dipendenti da reato sono:

- sanzioni pecuniarie;
- sanzioni interdittive;
- confisca dei beni;
- pubblicazione della sentenza.

Per l'illecito amministrativo da reato si applica sempre la sanzione pecuniaria, fatto salvo l'esimente indicata nel successivo paragrafo, la quale consiste nel pagamento di una somma di denaro nella misura stabilita dalla Legge, comunque non inferiore a € 10.329 e non superiore a € 1.549.000.

Il Giudice determina la sanzione pecuniaria tenendo conto della gravità del fatto, del grado di responsabilità dell'Ente, nonché dell'attività svolta da questa per eliminare o attenuare le conseguenze del fatto o per prevenire la commissione di ulteriori illeciti.

Sono inoltre previsti dei casi di riduzione della sanzione pecuniaria tra i quali, ad esempio:

a) Il caso in cui l'autore del reato abbia commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne abbia ricavato vantaggio o ne abbia ricavato vantaggio minimo;

b) Il caso in cui l'Ente abbia adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

Le sanzioni interdittive consistono in:

a) Interdizione, definitiva o temporanea, dall'esercizio dell'attività;

b) Sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

c) Divieto, temporaneo o definitivo, di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;

d) Esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli già concessi;

e) Divieto, temporaneo o definitivo, di pubblicizzare beni o servizi.

Le sanzioni interdittive si applicano quando ricorre almeno una delle seguenti condizioni:

f) L'Ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso da un Soggetto Apicale ovvero da un Soggetto Subordinato quando, in quest'ultimo caso, la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;

g) In caso di reiterazione degli illeciti.

Quand'anche sussistano una o entrambe le precedenti condizioni, le sanzioni interdittive tuttavia non si applicano se sussiste anche solo una delle seguenti circostanze:

a) L'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'Ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;

b) Il danno patrimoniale cagionato è di particolare tenuità;

c) Prima della dichiarazione di apertura del dibattimento di primo grado, concorrono tutte le seguenti condizioni:

   i. l'Ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;

   ii. l'Ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di un Modello;

   iii. l'Ente ha messo a disposizione il profitto conseguito ai fini della confisca.

Nei confronti dell'Ente è sempre disposta, con la sentenza di condanna, la confisca del prezzo o del profitto del reato. La confisca consiste nell'acquisizione coattiva da parte dello Stato del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato e fatti in ogni caso salvi i diritti acquisiti dai terzi in buona fede; quando non è possibile eseguire la confisca in natura, la stessa può avere ad oggetto somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato.

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

La pubblicazione della sentenza di condanna consiste nella pubblicazione di quest'ultima una sola volta, per estratto o per intero, a cura della cancelleria del Giudice, a spese dell'Ente, in uno o più giornali indicati dallo stesso Giudice nella sentenza nonché mediante affissione nel comune ove l'Ente ha la sede principale.

1.3 Il Modello Organizzativo quale possibile esimente della responsabilità amministrativa

L'articolo 6 del Decreto prevede una particolare forma di esonero dalla responsabilità amministrativa qualora il reato sia stato commesso dalle persone che rivestono posizioni c.d. "apicali" e l'Ente dimostri:

a) di aver adottato ed efficacemente attuato, prima della commissione del fatto, un modello organizzativo idoneo a prevenire i reati della specie di quello verificatosi;

b) di aver affidato ad un Organismo dell'ente, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e sull'osservanza dei modelli e di curare il loro aggiornamento;

c) che il reato sia stato commesso eludendo fraudolentemente i modelli di organizzazione e gestione;

d) che non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo deputato al controllo.

Nel caso in cui, invece, il reato sia stato commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza. Detta inosservanza è, in ogni caso, esclusa qualora l'ente, prima della commissione del reato, abbia adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi, secondo una valutazione che deve essere necessariamente a priori.

Il Decreto prevede inoltre che, in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, il Modello di Organizzazione, Gestione e Controllo debba rispondere alle seguenti esigenze:

- individuare le aree di rischio, ovvero le attività aziendali nel cui ambito possono essere commessi i reati;
- predisporre specifici "protocolli" al fine di programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
- escludere che un qualunque soggetto operante all'interno dell'Ente possa giustificare la propria condotta adducendo l'ignoranza delle discipline aziendali e di evitare che, nella normalità dei casi, il reato possa essere causato dall'errore – dovuto anche a negligenza o imperizia – nella valutazione delle direttive aziendali;
- configurare un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- prevedere modalità di individuazione e di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere un sistema di controlli preventivi tali da non poter essere aggirati se non intenzionalmente;
- prescrivere obblighi di informazione nei confronti dell'Organismo di Vigilanza deputato a controllare sul funzionamento e sull'osservanza del Modello.

L'articolo 6 del D.Lgs.231/2001 dispone, infine, che i Modelli di Organizzazione, Gestione e Controllo possono essere adottati sulla base di codici di comportamento redatti dalle associazioni rappresentative degli Enti, comunicati al Ministero della giustizia.

Il Modello di Carifermo è stato predisposto e aggiornato ispirandosi anche alle Linee Guida redatte dall'Associazione Bancaria Italiana (ABI) e approvate dal Ministero della Giustizia.

2 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N.231 DI CASSA DI RISPARMIO DI FERMO S.P.A. (CARIFERMO)

2.1 Gli strumenti e i presidi aziendali esistenti quali presupposti del Modello

Il presente Modello si integra all'interno della normativa, delle policy, dei regolamenti e del sistema di controlli interno già esistenti ed operanti all'interno della Cassa di Risparmio di Fermo S.p.a.

Il contesto organizzativo della Banca è costituito dall'insieme di regole, di strutture, di policy e di regolamenti che ne garantiscono il corretto funzionamento; si tratta di un sistema estremamente articolato che è definito e verificato internamente, anche al fine di rispettare le previsioni normative a cui Cassa di Risparmio di Fermo S.p.a. è sottoposta in qualità di Banca (Testo Unico Bancario, Istruzioni di Vigilanza Banca d'Italia, Testo Unico dell'intermediazione finanziaria e i relativi regolamenti attuativi). In tale sua qualità la Banca è inoltre sottoposta ad attività di vigilanza di Banca d'Italia e degli altri organi competenti, i quali svolgono verifiche e controlli sull'operato della Banca e su aspetti relativi alla sua struttura organizzativa, come previsto dalla normativa vigente. È pertanto evidente che tale complesso di norme speciali, nonché la sottoposizione all'esercizio costante della vigilanza da parte delle Autorità preposte, costituiscono anche uno strumento a presidio della prevenzione di comportamenti illeciti in genere, inclusi quelli previsti dalla normativa specifica che dispone la responsabilità amministrativa degli enti.

Quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali e ad effettuare i controlli sull'attività di impresa, anche in relazione ai reati e agli illeciti da prevenire, la Banca ha individuato:

- le Regole di Corporate Governance desumibili dai documenti societari (Statuto, etc.);
- il Codice Etico;
- il Funzionigramma;
- la Policy Anticorruzione;
- il Sistema dei Controlli Interni (SCI);
- il Sistema di Deleghe e Poteri;
- il Regolamento dei Flussi Informativi;
- le Policy, i Regolamenti interni e le Disposizioni aziendali.

Le policy, i regolamenti, le regole e i principi di cui agli strumenti sopra elencati non sono riportati dettagliatamente nel presente Modello ma fanno parte del più ampio sistema di organizzazione, gestione e controllo che lo stesso intende integrare e che tutti i soggetti destinatari, sia interni che esterni, sono tenuti a rispettare, in relazione al tipo di rapporto in essere con la Banca.

Nei paragrafi che seguono si illustrano, per grandi linee, esclusivamente i principi di riferimento del Codice Etico, del Sistema dei Controlli Interni, del Sistema dei poteri e delle deleghe, nonché del Regolamento dei Flussi Informativi.

2.2 Le linee guida dell'ABI

Il Modello Organizzativo della Cassa di Risparmio di Fermo S.p.a., è modulato sulle sue specificità strutturali, organizzative ed operative e tiene conto delle "Linee Guida dell'Associazione Bancaria

Italiana per l'adozione di modelli organizzativi sulla responsabilità amministrativa delle banche" (d'ora innanzi Linee Guida) riscontrate come idonee dal Ministero della Giustizia:

- Linee Guida ABI del febbraio 2004 (documento integrale comprensivo degli 11 allegati relativi all'analisi dei reati);
- Aggiornamento Linee Guida – Abusi di mercato, 22 novembre 2007;
- Aggiornamento Linee Guida – Abuso di informazioni privilegiate e manipolazione del mercato, 3 dicembre 2007;
- Aggiornamento Linee Guida – Illeciti amministrativi di abuso di informazioni privilegiate e manipolazione del mercato, 6 marzo 2008;
- Aggiornamento Linee Guida – Reati di riciclaggio, 9 gennaio 2009 e 5 febbraio 2009;
- Aggiornamento Linee Guida – Criminalità informatica, 27 gennaio 2010;
- Aggiornamento Linee Guida – Linee guida per l'adozione e l'aggiornamento dei modelli organizzativi ex d.lgs. n. 231/2001: Reati Ambientali, 12 luglio 2012.

Le Linee guida tengono conto delle peculiarità della realtà bancaria.

Con riferimento alle "esigenze" individuate dal legislatore in relazione ai Modelli, i punti fondamentali sviluppati dalle Linee Guida sono:

a) ***analisi delle attività o funzioni aziendali*** nell'ambito delle quali possono essere commessi i reati, al fine di individuare i presidi da adottare in relazione all'esistenza di rischi concreti di commissione dei reati;
b) ***previsione di regole*** dirette a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire (*modalità di gestione del rischio*) ed individuazione delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
c) ***obblighi di informazione*** nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza dei Modelli;
d) ***sistema disciplinare*** idoneo a sanzionare il mancato rispetto delle misure indicate nei Modelli.

Si evidenzia che nel febbraio 2019 è stato emanato il documento *"Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del D.Lgs. 8 giugno 2001, n.231",* nato dalla collaborazione tra Confindustria, il Consiglio Nazionale Forense (CNF), il Consiglio dei Dottori Commercialisti (CNDCEC) e l'Associazione Bancaria Italiana (ABI). Lo scopo dichiarato del documento è garantire una effettiva attuazione all'interno delle aziende dei principi del Modello 231 mediante la creazione di un sistema di compliance costruito su idonei presidi che consentano un'effettiva opera di contenimento del rischio e non una "mera aderenza formale al dettato del Decreto".

2.3 Il Codice Etico e la Policy Anticorruzione

La Banca riconoscendo e promuovendo i più elevati standard di comportamento, a conferma dell'importanza attribuita ai profili etici e a comportamenti improntati a rigore ed integrità, ha adottato il Codice Etico e la Policy Anticorruzione.

Il Codice Etico contiene le regole che tutti i dipendenti devono adottare per garantire che i comportamenti siano sempre ispirati a criteri di correttezza, collaborazione, lealtà, trasparenza e reciproco rispetto, nonché per evitare che vengano poste in essere condotte idonee ad integrare le fattispecie di reato e gli illeciti inclusi nel D.Lgs.231/2001. Il Codice Etico individua, pertanto, i valori essenziali che caratterizzano il modo di operare della Cassa di Risparmio di Fermo S.p.a. ed ispirano il comportamento di tutti coloro che operano in nome e per conto della Banca, fissando standard di riferimento e norme di condotta tesi ad avvalorare i processi decisionali aziendali ed orientare i comportamenti della Banca. Contiene la mission, i valori aziendali e i principi che regolano le relazioni con gli stakeholder.

La Policy Anticorruzione individua i principi, identifica le aree sensibili ("a maggior rischio"), evidenzia le modalità di segnalazione e definisce i ruoli e le responsabilità ed i macro processi per la gestione del rischio di corruzione da parte della Banca. Il Consiglio di Amministrazione, il Direttore Generale e tutta l'Alta Direzione della Banca hanno la responsabilità di creare e diffondere la cultura della gestione del rischio all'interno dell'organizzazione e di assicurare la supervisione della condotta richiesta. Tali soggetti, nell'ambito della generale responsabilità di governo del rischio, stabiliscono univoci indirizzi e adempimenti affinché le relazioni d'affari siano improntate alla sana e prudente gestione nonché a criteri di buona fede e correttezza. Essi pertanto ricoprono un ruolo attivo nel far rispettare gli standard di comportamento descritti nella policy adottata dalla Banca.

La Policy, inoltre, affida alla Funzione di Internal Audit e all'Organismo di Vigilanza la gestione delle segnalazioni in materia secondo le modalità indicate nel seguito e/o nella normativa interna.

2.4 Il Sistema dei Controlli Interni – caratteristiche principali

Il Sistema dei Controlli Interni (SCI) è un elemento fondamentale del complessivo sistema di governo della Banca.

La Banca, in linea con la normativa di legge e di vigilanza si è dotata di un sistema di controllo interno idoneo a rilevare, misurare e verificare nel continuo i rischi tipici dell'attività aziendale. Esso rappresenta un elemento fondamentale del complessivo sistema di governo della Banca, assicura che l'attività aziendale sia in linea con le strategie e le politiche aziendali e sia improntata a canoni di sana e prudente gestione.

Il Sistema dei Controlli Interni è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare il conseguimento delle seguenti finalità:

- Verifica dell'attuazione delle strategie e delle politiche aziendali;

- Contenimento del rischio entro i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio della Banca (Risk Appetite Framework – "RAF");

- Salvaguardia del valore delle attività e protezione dalle perdite;

- Efficacia ed efficienza dei processi aziendali;
- Affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche;
- Prevenzione del rischio che la Banca sia coinvolta, anche involontariamente, in attività illecite;
- Conformità delle operazioni con la legge e la normativa di vigilanza, nonché con le politiche, i regolamenti e le procedure interne.

Il presupposto di un sistema di controllo interno completo e funzionale è l'esistenza di una organizzazione aziendale adeguata ad assicurare una sana e prudente gestione e l'osservanza delle disposizioni normative. Il corretto funzionamento del governo societario, nel rispetto delle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche, è costituito dallo Statuto e dai documenti di Corporate Governance della Banca. Nel dettaglio i principi generali di organizzazione:

- Assicurano una necessaria separatezza tra le funzioni operative e quelle di controllo ed evitano situazioni di conflitto di interesse nell'assegnazione delle competenze;
- Assicurano che il personale sia provvisto delle competenze e della professionalità necessarie per l'esercizio delle responsabilità a esso attribuite;
- Sono in grado di identificare, misurare e monitorare adeguatamente tutti i principali rischi assunti o assumibili nei diversi segmenti operativi;
- Sono in grado di stabilire attività di controllo ad ogni livello operativo;
- Assicurano sistemi informativi affidabili ed idonei ad evidenziare tempestivamente le anomalie riscontrate nell'attività di controllo;
- Consentono la registrazione di ogni fatto di gestione e di ogni operazione con adeguato grado di dettaglio.

La Banca, in coerenza con le indicazioni delle Autorità di Vigilanza, ha individuato le seguenti tipologie di controllo descritte nel dettaglio nel documento "Sistemi dei Controlli Interni":

- ***Controlli di primo livello*** - o controlli di linea - diretti ad assicurare il corretto svolgimento delle operazioni. I controlli sono effettuati dalle stesse unità organizzative, o da unità diverse secondo la logica di "maker/checker", o incorporati dalle procedure;
- ***Controlli di secondo livello*** - o controlli sui rischi e sulla conformità - affidati a unità diverse da quelle produttive, volti ad assicurare la corretta attuazione del processo di gestione dei rischi, il rispetto dei limiti operativi, la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione. I controlli di 2° livello sono effettuati dalla Funzione di Compliance, dalla Funzione Risk Management e dalla Funzione Antiriciclaggio;
- ***Controlli di terzo livello****,* finalizzati ad individuare violazioni delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni e del sistema informativo, con

cadenza prefissata in relazione alla natura e all'intensità dei rischi. Nella Carifermo l'attività è condotta dalla Funzione Internal Audit.

Il Sistema dei Controlli Interni ha consentito alle banche di dotarsi di standard organizzativi adeguati, che costituiscono, seppure in una accezione più ampia, ciò che sostanzialmente il Decreto intende affermare nell'ordinamento.

La Banca assicura la necessaria separatezza tra le funzioni operative e quelle di controllo ed evita situazioni di conflitto di interesse nell'assegnazione delle competenze; identifica, misura e monitora adeguatamente tutti i rischi assunti o assumibili nei diversi segmenti operativi; stabilisce attività di controllo ad ogni livello operativo; assicura sistemi informativi affidabili e idonei ad evidenziare tempestivamente le anomalie riscontrate nell'attività di controllo; consente la registrazione di ogni fatto di gestione con adeguato grado di dettaglio.

Ogni banca effettua un monitoraggio finalizzato alla prevenzione dei rischi connessi con frodi e infedeltà dei dipendenti e di quelli derivanti dall'eventuale coinvolgimento della banca in operazioni di riciclaggio di denaro sporco; un monitoraggio sulle attività che possono determinare rischi di perdite risultanti da errori o inadeguatezza dei processi interni, delle risorse umane e dei sistemi oppure derivanti da eventi esterni.

I detti principi pervadono tutta l'attività aziendale e riguardano la redazione dei bilanci, i capitoli di spesa, i flussi finanziari in entrata e in uscita, l'affidabilità di tutte le informazioni finanziarie e gestionali, affinché il complesso delle attività sia conforme ai principi contabili di riferimento, alle leggi, ai regolamenti, alle norme di vigilanza nonché a quelle statutarie.

La Banca è dotata di complessi sistemi di regole interne che assolvono la funzione di:

a) Organizzare il sistema dei poteri e delle deleghe;
b) Regolamentare e documentare le attività svolte;
c) Gestire i rapporti tra i vari attori del sistema dei controlli interni;
d) Disciplinare i flussi informativi fra le diverse funzioni aziendali.

Tali regole e procedure - contenute in disposizioni interne, nella normativa aziendale, in codici etici, etc. - costituiscono già di per sé modelli organizzativi o quanto meno la base precettiva di ciò che è richiesto ad un modello organizzativo secondo il Decreto.

2.5 Il Sistema di deleghe e poteri

A norma di Statuto, al Consiglio di Amministrazione spettano tutti i poteri di ordinaria e straordinaria amministrazione della Banca. Al fine di assicurare la corretta ed ordinata gestione della Banca, è in essere un sistema di deleghe e poteri.

Il Consiglio di Amministrazione ha delegato alcune delle proprie attribuzioni al fine di assicurare unitarietà nella gestione corrente e nell'erogazione del credito.

In particolare, il Consiglio di Amministrazione per la gestione corrente ha delegato alcune delle proprie attribuzioni al Comitato Esecutivo, al Presidente, al Direttore Generale e al Vice Direttore Generale (qualora nominato), delegando i poteri e le funzioni al Dirigente in caso di contemporanea

assenza o impedimento del Direttore Generale e del Vice Direttore Generale. I poteri e le funzioni sono esercitati dal Dirigente, fatto salvo quanto previsto per la concessione del credito, definendo altresì l'ambito dei poteri deliberativi e di spesa conferiti agli altri Responsabili di Area/Direzione.

Il Consiglio di Amministrazione ha altresì delegato, nell'ambito dell'erogazione del credito, poteri entro limiti di importo predeterminati ed in relazione all'intensità del rischio a dipendenti della Società, al fine di rispondere con immediatezza alle richieste di credito avanzate dalla clientela ordinaria. Per la corretta erogazione del credito la Banca ha individuato criteri determinati per ponderare i rischi. Il Consiglio di amministrazione, nell'ambito della gestione dei rischi finanziari, ha altresì attribuito deleghe in materia finanziaria e in materia di operazioni su cambi.

In ogni caso, in materia si intendono qui integralmente richiamati il Testo coordinato dei "Poteri Delegati" e la "Policy per la gestione dei rischi finanziari".

2.6 Finalità del modello

La Banca, al fine di assicurare sempre più condizioni di correttezza e trasparenza nella conduzione delle attività aziendali, ha ritenuto opportuno adottare un Modello di Organizzazione, Gestione e Controllo in linea con le prescrizioni del Decreto, pur ritenendo gli strumenti aziendali illustrati nei paragrafi precedenti già di per sé idonei anche a prevenire i reati contemplati nel D.Lgs.231/2001.

Tale iniziativa è stata assunta nella convinzione che l'adozione del Modello costituisca un valido strumento di sensibilizzazione di tutti coloro che operano per conto della Banca affinché tengano, nell'espletamento della propria attività, comportamenti corretti e rispettosi delle norme vigenti e dei fondamentali principi di etica professionale, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

2.7 Scopo e principi del modello

Il Modello si inserisce nel più ampio sistema di controllo interno della Carifermo, di cui si è tenuto conto nella predisposizione del Modello stesso, in quanto misura di prevenzione dei reati e di controllo sui processi operativi relativi alle aree a rischio.

I principi cardine del Modello, oltre all'esistente sistema di controllo interno, sono:

- le Linee Guida dell'Associazione Bancaria Italiana (ABI);
- i requisiti indicati dal Decreto ed in particolare:
    - la costituzione di un Organismo di Vigilanza che ha il compito di verificare l'effettiva e corretta attuazione del Modello anche mediante il monitoraggio dei comportamenti aziendali ed il diritto ad una informazione costante sulle attività rilevanti ai fini del Decreto;
    - la verifica del funzionamento e dell'osservanza del Modello ed il periodico aggiornamento dello stesso;
    - la comunicazione e diffusione a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
- principi generali di un adeguato sistema di controllo interno, quali:

- rispetto del principio di separazione di compiti e funzioni;
- definizione di poteri delegati coerenti con le responsabilità assegnate;
- definizione di un efficace sistema di flussi informativi;
- documentabilità dei controlli svolti.

Scopo del Modello, pertanto, è la realizzazione di un sistema organico di prevenzione e controllo finalizzato particolarmente alla riduzione del rischio di commissione delle fattispecie criminose previste dal Decreto mediante l'individuazione delle attività a rischio e, ove necessario, l'integrazione della relativa regolamentazione.

In particolare, mediante l'individuazione delle attività / processi 'sensibili', ai fini dei reati previsti dal Decreto, il Modello si propone di:

- determinare in tutti coloro che operano in nome e per conto della Banca, in particolare nelle aree in cui si svolgono le attività / i processi 'sensibili', una piena consapevolezza di poter incorrere in caso di violazione delle disposizioni aziendali e di quelle previste dal D.Lgs.231/2001 e riportate nel Modello, in un reato passibile di sanzioni penali e amministrative, la cui commissione è fortemente censurata dalla Banca, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, potrebbe trarne un vantaggio economico immediato;
- ribadire che la Banca non tollera comportamenti illeciti, di ogni tipo ed indipendentemente da qualsiasi finalità, in quanto gli stessi, oltre a trasgredire le leggi vigenti, sono comunque contrari ai principi etici ai quali la Banca si ispira;
- consentire alla Banca di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi, attraverso un monitoraggio costante dell'attività.

2.8 Costruzione e componenti del Modello

A seguito dell'emanazione del Decreto, la Carifermo ha definito il proprio Modello, la cui realizzazione è stata preceduta dalle seguenti attività:

a) identificazione delle attività a rischio di reato. In tale fase si è provveduto ad individuare: le attività / i processi a rischio di reato; le più significative fattispecie di rischio/reato e le possibili modalità di realizzazione delle stesse per ciascuna attività oggetto di analisi; i punti di controllo esistenti volti a mitigare il rischio di commissione delle fattispecie di reato individuate;

b) individuazione delle eventuali azioni di miglioramento. Sulla base della situazione esistente (controlli e procedure già attivi con riferimento alle aree a rischio di reato) e delle previsioni e finalità del Decreto, sono state individuate le azioni da intraprendere per l'implementazione di un efficace sistema di controllo interno e per la conformità ai requisiti organizzativi del Modello;

c) definizione della struttura del Modello.

Il Modello della Banca si compone delle seguenti parti:

- una Parte Generale, che rappresenta il corpo centrale del documento e illustra, sinteticamente il Modello di Organizzazione, gestione e controllo e i meccanismi di concreta attuazione del Modello;

- una Parte Speciale, nella quale sono individuate le fattispecie di reato e le diverse attività aziendali sensibili della Banca che presentano un potenziale rischio di commissione delle fattispecie di reato contemplate nel Decreto e sono rappresentati i principi generali di controllo e i principi di comportamento atti a prevenire il compimento di tali reati, nel rispetto della normativa interna esistente, che ne costituisce parte integrante e sostanziale;

- un Elenco dei reati presupposto ai sensi del D.Lgs.231/2001, in cui sono rappresentate le fattispecie di reato rilevanti ai sensi del Decreto;

- un Risk Assessment, nel quale sono individuate le attività a rischio di commissione reati, avuto riguardo dell'analisi dei reati stessi e del loro profilo di rischiosità ("fattore di rischio totale" – FRT) in funzione della frequenza e della rilevabilità delle singole attività sensibili individuate.

Costituiscono, inoltre, parte integrante del Modello della Banca i seguenti documenti:

- Codice Etico, nel quale sono sanciti i principi etici ai quali la Banca orienta la propria attività;
- Regolamentazione interna rilevante (policy, regolamenti, manuali etc.).

2.9 Destinatari del Modello

Il Modello e le disposizioni ivi contenute e richiamate devono essere rispettate dagli esponenti aziendali e da tutto il personale di Carifermo e, in particolare, da parte di coloro che si trovino a svolgere le attività sensibili.

Al fine di garantire l'efficace ed effettiva prevenzione dei reati, il Modello è destinato anche ai soggetti esterni (intendendosi per tali i fornitori, gli agenti, i consulenti, i professionisti, i lavoratori autonomi o parasubordinati, i partner commerciali, o altri soggetti) che, in forza di rapporti contrattuali, prestino la loro collaborazione a Carifermo per la realizzazione delle sue attività.

La Banca richiede ai soggetti esterni il rispetto del Modello, anche mediante l'apposizione di una clausola contrattuale che impegni il contraente ad attenersi ai principi del Modello, prevedendosi che la violazione degli impegni o, comunque, eventuali condotte illecite poste in essere in occasione o comunque in relazione all'esecuzione degli incarichi costituiranno a tutti gli effetti grave inadempimento ai sensi dell'art. 1455 cod. civ. e ss. ai fini della risoluzione del contratto.

L'insieme dei soggetti interni ed esterni della Banca che devono attenersi al rispetto di quanto prescritto nel presente Modello costituiscono i Destinatari del Modello.

2.10 Adozione, efficace attuazione e modificazione del modello – ruoli e responsabilità

Adozione del Modello

L'adozione e l'efficace attuazione del "*Modello di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231*" costituiscono, ai sensi dell'art. 6, comma I, lett. a) del D.Lgs. n. 231/01, atti di competenza e di emanazione del Consiglio di Amministrazione che approva mediante apposita delibera il Modello.

Efficace attuazione e modificazione del Modello

E' cura del Consiglio di Amministrazione provvedere all'efficace attuazione del Modello, mediante valutazione e approvazione delle azioni necessarie per implementarlo o modificarlo. Per l'individuazione di tali azioni, l'organo amministrativo si avvale del supporto dell'Organismo di vigilanza. Il Consiglio di Amministrazione delega le singole strutture a dare attuazione ai contenuti del Modello e a curare il costante aggiornamento e l'implementazione della normativa interna e dei processi aziendali, che costituiscono parte integrante del Modello, nel rispetto dei principi generali di controllo e di comportamento definiti in relazione ad ogni attività sensibile. L'efficace e concreta attuazione del Modello è garantita altresì:

- dall'Organismo di vigilanza, nell'esercizio dei poteri di iniziativa e di controllo allo stesso conferiti sulle attività svolte dalle singole unità organizzative nelle aree sensibili;

- dai responsabili delle varie unità organizzative (Aree di Governo, Direzioni e Unità Organizzative) di Carifermo in relazione alle attività a rischio dalle stesse svolte.

Il Consiglio di Amministrazione deve inoltre garantire, anche attraverso l'intervento dell'Organismo di vigilanza, l'aggiornamento delle aree sensibili e del Modello, in relazione alle esigenze di adeguamento che si rendono necessarie.

Specifici ruoli e responsabilità nella gestione del Modello sono inoltre attribuiti alle funzioni di seguito indicate.

Struttura organizzativa della Cassa di Risparmio di Fermo S.p.a.

L'organizzazione della Banca è di tipo gerarchico-funzionale e al suo vertice è posto il Direttore Generale che svolge le funzioni attribuitegli dallo Statuto e dall'Organo con funzione di Supervisione Strategica – il Consiglio di Amministrazione.

La Direzione Generale è composta dal Direttore Generale, dal Vice Direttore Generale e dal Direttore Centrale, ad essa sono attribuite funzioni di pianificazione, di organizzazione, di rilevazione e controllo, nonché di coordinamento funzionale delle attività svolte a livello centrale e periferico.

L'Area Amministrazione Controllo e Finanza e le Direzioni rappresentano aggregazioni di Uffici o Funzioni in relazione ai compiti da espletare.

Gli Uffici, che possono essere articolati anche in Funzioni, rappresentano la suddivisione e ripartizione settoriale delle attività relative ai processi o parte di essi e concorrono a formare l'organizzazione aziendale volta ad assicurare una sana e prudente gestione.

Le Filiali e le Agenzie costituiscono la "rete distributiva di servizio e gestione relazionale" con la clientela nelle diverse aree territoriali in cui opera la Banca.

Nella gestione del Modello sono coinvolte le funzioni aziendali di controllo e le strutture della Banca, di seguito individuate, alle quali sono affidati specifici ruoli e responsabilità.

Si precisa che nel prosieguo del presente documento sarà utilizzato il termine “struttura” per indicare indistintamente le strutture aziendali previste dal funzionigramma aziendale, ossia Aree, Direzioni, Uffici.

Direttore Generale

Il Direttore Generale svolge funzioni di direzione e sovrintendenza di tutte le aree operative della Banca di cui indirizza, coordina e sorveglia l’attività secondo le direttive dell’Organo con Funzioni di Supervisione Strategica – Consiglio di Amministrazione -.

Il Direttore Generale cura l’attuazione degli indirizzi strategici, del RAF e delle politiche di governo dei rischi definiti dal Consiglio di Amministrazione ed è responsabile per l’adozione di tutti gli interventi necessari ad assicurare l’aderenza dell’organizzazione e del sistema dei controlli interni ai principi e requisiti disciplinati nelle Istruzioni di Vigilanza per le Banche emanate dalla Banca d’Italia.

In caso di assenza o impedimento le funzioni del Direttore Generale sono attribuite al Vice Direttore Generale (qualora nominato) o, in assenza di questo, al Dirigente con i limiti definiti dal documento “Poteri Delegati”, come sopra specificato.

Il Direttore Generale è il Capo del Personale e impartisce alla struttura ogni istruzione operativa per il raggiungimento degli scopi sociali e degli indirizzi dettati dal Consiglio di Amministrazione, al quale riferisce periodicamente.

Comitato di Direzione

Il Comitato di Direzione è un organo consultivo e di coordinamento per l’emanazione, diffusione uniforme e sistematica delle politiche strategiche e gestionali della Banca. I vertici della struttura esecutiva e i responsabili delle Funzioni di controllo prendono parte alla definizione delle strategie e, nell’ambito del loro ruolo nelle rispettive aree di competenza, sono responsabili della corretta e tempestiva attuazione delle stesse.

Comitato Crediti

Il Comitato Crediti è un organo tecnico costituito allo scopo di analizzare e condividere le politiche di credito e la gestione coordinata delle problematiche inerenti il credito. È responsabile della definizione delle politiche creditizie, dei processi del credito, dell’esame dell’andamento dei crediti anomali e della concentrazione di portafoglio.

Comitato Finanza

Il Comitato Finanza è un organo tecnico costituito allo scopo di assicurare la gestione coordinata del portafoglio di proprietà e delle problematiche inerenti i rischi di mercato, di tasso e di liquidità.

Responsabili delle Aree di Governo e delle Direzioni

I Responsabili delle Aree di Governo e delle Direzioni collaborano con il Direttore Generale per l’attuazione della politica aziendale definita dal Consiglio di Amministrazione, formulando proposte

per ogni opportuna innovazione normativa, tecnologica, organizzativa e strutturale. Costituiscono l'elemento cardine nella diffusione all'interno della Banca delle politiche gestionali e dello stile di direzione e rappresentano il primo livello di assegnazione e monitoraggio degli obiettivi gestionali di efficienza, economicità, efficacia, qualità del servizio.

Funzione Internal Audit

La funzione Internal Audit è volta a verificare il regolare andamento dell'operatività e l'evoluzione dei rischi, nonché la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del sistema di controlli interni, portando all'attenzione degli organi aziendali i possibili miglioramenti. In particolare assicura un costante e sistematico monitoraggio del Sistema di Controllo Interno e di Gestione dei Rischi (Regole, Politiche, Norme, Procedure, Strutture organizzative), inteso come processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi aziendali, al fine di verificare l'adeguatezza e l'effettiva operatività rispetto agli obiettivi fissati nel Piano Industriale e nel budget annuale. Il responsabile della revisione interna informa i responsabili delle altre funzioni aziendali di controllo delle eventuali inefficienze o irregolarità emerse nel corso delle attività di verifica di propria competenza e viene informato dalle funzioni di risk management, dalla funzione di conformità alle norme e dai responsabili delle unità organizzative delle criticità rilevate nelle proprie attività di controllo che possano essere di interesse per l'attività di audit.

La funzione Internal Auditi assicura in generale una costante ed indipendente azione di sorveglianza sul regolare andamento dell'operatività e dei processi al fine di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose, valutando la funzionalità del complessivo sistema dei controlli interni e la sua idoneità a garantire l'efficacia e l'efficienza dei processi aziendali.

La funzione Internal Audit, per quanto di propria competenza e di concerto con le altre funzioni aziendali di controllo, supporta l'Organismo di Vigilanza nel vigilare sul rispetto e sull'adeguatezza delle regole contenute nel Modello, attivando, a fronte delle eventuali criticità riscontrate nel corso della propria attività, le funzioni di volta in volta competenti per le opportune azioni di mitigazione.

Ufficio Compliance, Privacy e ICT Risk

La Funzione di Compliance è competente a garantire la presenza di regole, procedure e prassi operative all'interno della Banca che prevengano efficacemente comportamenti non conformi alla normativa di riferimento.

Nell'Ufficio Compliance, Privacy e ICT Risk sono ricomprese la funzione di Conformità alle norme (o Compliance) a cui fanno capo i controlli di secondo livello volti ad assicurare la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione e la Funzione di controllo dei Rischi ICT e di sicurezza [1] ;il Responsabile dell'Ufficio svolge inoltre il ruolo di Responsabile della Protezione Dati (RDP o DPO) cui sono assegnate funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione della normativa in materia di trattamento di dati personali e della loro protezione.

[1] Cfr. Circolare Banca d'Italia n.285/2023, Titolo IV, Capitolo 4, Sezione II

La Funzione di Compliance presiede, secondo un approccio risk based, alla gestione del rischio di non conformità con riguardo a tutta l'attività aziendale, verificando che le procedure interne siano adeguate a prevenire tale rischio;
La Funzione di Compliance, per quanto di propria competenza, supporta l'attività di controllo dell'Organismo di Vigilanza, monitorando nel tempo l'efficacia delle regole e dei principi di comportamento indicati nel Modello a prevenire i reati di cui al Decreto e collaborando, di concerto con le altre strutture della Banca, con le funzioni aziendali di controllo e con il Datore di Lavoro ai sensi del D.Lgs.81/2008, per quanto di loro competenza, all'aggiornamento del Modello in coerenza con l'evoluzione della normativa di riferimento e con le modifiche della struttura organizzativa aziendale.

La Funzione di Compliance partecipa, inoltre, di concerto con la struttura competente in materia di formazione, alla predisposizione di un adeguato piano di formazione.

La Funzione di Controllo dei rischi ICT e di sicurezza è volta a verificare in un'ottica di controlli di secondo livello il processo di gestione dei rischi ICT e di sicurezza; tramite un'attività di *assessment* si assicura che i rischi siano individuati, misurati, valutati, gestiti, monitorati nonché ripartiti e manutenuti entro i limiti della propensione al rischio della Banca.

Il Responsabile della protezione dei dati personali (RDP o DPO) svolge funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento Europeo 679/2016. Coopera con l'Autorità e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

Ufficio Risk Governance – Funzione Risk Management e Funzione Antiriciclaggio

Nell'Ufficio Risk Governance sono ricomprese due funzioni aziendali a cui fanno capo parte dei controlli di secondo livello, volti ad assicurare la corretta attuazione del processo di gestione dei rischi e della normativa interna ed esterna di competenza.

All'interno dell'Ufficio sono svolte le Funzioni di:

- Risk Management (funzione di controllo dei rischi) che ha la finalità di collaborare alla definizione e all'attuazione del RAF (Risk Appetite Framework) e delle relative politiche di governo dei rischi, attraverso un adeguato processo di gestione e monitoraggio dei rischi; assicura che ogni rischio di rilievo per la Banca sia correttamente individuato ed efficacemente gestito e che siano fornite alle Funzioni aziendali competenti e a tutti gli Organi di Vertice, informazioni complete e flussi informativi integrati che permettano un'effettiva conoscenza del profilo di rischio della Banca.

- Antiriciclaggio, che sovrintende le attività di prevenzione e gestione del rischio di riciclaggio e di finanziamento al terrorismo, verificando nel continuo l'idoneità delle procedure interne in materia, anche per le finalità di cui al Decreto.

La Funzione Antiriciclaggio partecipa, inoltre, in raccordo con la struttura competente in materia di formazione, alla predisposizione di un adeguato piano di formazione in materia di contrasto al riciclaggio e al finanziamento del terrorismo.

Ufficio Risorse Umane

L'Ufficio Risorse Umane ha funzione di gestione e sviluppo del personale, coerentemente con le linee guida e le politiche strategiche definite dalla Banca. Promuove lo sviluppo professionale delle risorse umane, supportando il Direttore Generale e interagendo con i Responsabili delle Unità Centrali e Periferiche nella formulazione/gestione del budget del personale e assicura l'amministrazione dei rapporti di lavoro individuali del personale. Programma, con la collaborazione dei Responsabili delle Unità Organizzative, piani di formazione e interventi di sensibilizzazione rivolti al personale delle Unità Centrali e Periferiche competenti sull'importanza di un comportamento conforme alle regole aziendali, anche sulla comprensione dei contenuti del Modello e del Codice Etico e presidia, con il supporto delle funzioni Compliance, Internal Auditing, Antiriciclaggio e Legale e Contenzioso, il processo di rilevazione e gestione delle violazioni del Modello, nonché il conseguente processo sanzionatorio e, a sua volta, fornisce tutte le informazioni emerse in relazione ai fatti e/o ai comportamenti rilevanti ai fini del rispetto della normativa del D. Lgs. 231/2001 all'Organismo di Vigilanza, il quale le analizza al fine di prevenire future violazioni, nonché di monitorare l'adeguatezza del Modello.

Ufficio Legale e Contenzioso

L'Ufficio Legale e Contenzioso garantisce l'attività legale di supporto alla Presidenza/Direzione, agli Uffici Interni ed alle Filiali/Agenzie, con pareri scritti e verbali, su pratiche e atti a rilevanza interna ed esterna. Formula pareri legali, ove necessario anche con il supporto di legali esterni. Svolge, ove richiesta, attività di assistenza consultiva e di supporto al fine di fornire soluzioni su questioni giuridiche ed interpretative di norme legislative, idonea ad indirizzare il corretto svolgimento dell'attività bancaria. Svolge, in favore della Banca, attività di consulenza ed assistenza per tutta la contrattualistica aziendale, sia nei rapporti con i fornitori di servizi che in relazione alle modifiche da apportare alla modulistica contrattuale, la quale necessita di costanti adeguamenti alle statuizioni della normativa di settore, prevenendo, per quanto possibile, il contenzioso, nonché eventuali rilievi da parte degli Organi di Vigilanza e/o Ispettivi. Svolge attività di studio e di istruttoria funzionali al conferimento di incarichi a legali esterni per il recupero dei crediti insoluti e la difesa della Banca, compiendo, all'uopo, ogni atto necessario ad assicurare il buon esito del giudizio. Ha la responsabilità della gestione dei crediti scritturati a Sofferenza, delle insolvenze, del contenzioso promosso da o nei confronti della Banca (sia in fase extra-giudiziale che giudiziale) e la formulazione di pareri legali. La funzione Legale e Contenzioso, per il perseguimento delle finalità di cui al D. Lgs. 231/2001, assicura assistenza e consulenza legale alla Banca, seguendo l'evolversi della normativa specifica e degli orientamenti giurisprudenziali in materia. Spetta altresì alla funzione Legale e Contenzioso l'interpretazione della normativa, la risoluzione di questioni di diritto e l'identificazione delle condotte che possono configurare ipotesi di reato.

Direzione Commerciale

La Direzione Commerciale ha funzione di supervisione e governo diretto del sistema distributivo della Banca, rappresentato dalle Filiali/Agenzie, di cui sovraintende le attività per il raggiungimento degli obiettivi fissati dal budget aziendale. Si attiva al fine di integrare la visione commerciale con

tutte le Direzioni e dialoga trasversalmente con le stesse al fine di indirizzare e gestire correttamente l'attività della rete con l'obiettivo di rafforzare l'integrazione tra Rete e Sede. Presiede al regolare funzionamento degli Uffici in carico, orientandone e coordinandone l'attività in conformità alle norme vigenti ed in armonia con i criteri stabiliti dall'Organo con Funzione di Supervisione Strategica e dal Direttore Generale. Orienta l'attività della Rete ai principi e valori del Codice Etico della Banca e ne verifica il rispetto. Gestisce il processo di definizione degli obiettivi facendosi parte attiva nella definizione di metodi e azioni volti al raggiungimento degli obiettivi specifici per area di business e Filiale, coordinandosi con le Funzioni Marketing, con i Direttori/Titolari di Filiale e con i Coordinatori.

Direzione Amministrazione

La Direzione Amministrazione coordina le attività contabili, amministrative, di bilancio, del sistema dei pagamenti, dei servizi di tesoreria e di cassa, di gestione del contante, dell'Ufficio IT, oltre alla gestione dell'aspetto fiscale, in conformità alle norme vigenti e di concerto con il Responsabile dell'Area Amministrazione, Controllo e Finanza. Cura il raggiungimento degli obiettivi fissati dagli organi aziendali, relativamente agli uffici assegnati e verifica i risultati conseguiti. Esercita le deleghe attribuite dall'Organo con Funzione di Supervisione Strategica e propone soluzioni per migliorare l'efficienza degli uffici assegnati. Comunica mensilmente i report contabili al Responsabile Area Amministrazione, Controllo e Finanza e tiene informati i Responsabili degli uffici sulle normative aziendali, civilistiche, fiscali e di bilancio inerenti ai servizi assegnati. Gestisce l'attività fiscale, le attività contabili e amministrative, le attività connesse con l'Ufficio Estero, le attività di autorizzazione reti interbancarie, le attività di gestione dei rapporti con gli Organi dell'Amministrazione dello Stato e le attività relative agli immobili.

Direzione Finanza

La Direzione Finanza è responsabile della corretta gestione dei sistemi e delle risorse finanziarie al fine di garantire un'adeguata gestione finanziaria della Banca. Coordina la gestione del portafoglio titoli di proprietà, la gestione della liquidità della Banca, i cambi e le attività dell'Ufficio Estero. Fornisce supporto consulenziale alle strutture della Banca per la definizione delle politiche dei servizi di investimento forniti alla clientela e di concerto con il Responsabile dell'Ufficio Estero propone all'Ufficio Crediti gli affidamenti a banche estere funzionali alle operazioni da eseguire per proprio conto o per conto della clientela. Gestisce i rapporti con le controparti di mercato, gestisce e controlla la situazione tesoreria, gestisce e controlla il portafoglio titoli, predispone le relazioni e le delibere sulla gestione della liquidità e del portafoglio titoli in collaborazione con la Direzione Generale, assicura assistenza alle eventuali controversie legali riguardanti i servizi di investimento forniti alla clientela in collaborazione con la Direzione Generale e con l'Ufficio Legale e Contenzioso, gestisce e fornisce i report dell'attività sul portafoglio titoli della Banca per la Direzione Generale e predispone i dati settoriali per l'Ufficio Contabilità.

Direzione Organizzazione e IT

La Direzione Organizzazione e IT coordina gli interventi necessari ad aggiornare i processi organizzativi derivanti dalle novità normative e regolamentari e le attività propedeutiche all'innovazione dell'organizzazione aziendale (strutture, responsabilità, processi) al fine di ottimizzare l'efficacia, l'efficienza e il controllo. In qualità di Funzione ICT è responsabile dello svolgimento dei processi operativi del sistema informativo. La Direzione è responsabile di garantire

la sicurezza dei dati e delle informazioni sensibili dei clienti. In caso di risorse esternalizzate si traduce nell'implementazione e nella verifica dell'adeguatezza di sistemi e protocolli di sicurezza avanzati per prevenire l'accesso non autorizzato, il furto di dati o altre minacce informatiche. La Direzione ha la responsabilità di gestire e coordinare il portafoglio delle progettualità ICT della Banca interne ed esternalizzate. Governa l'evoluzione dell'architettura e dell'innovazione tecnologica. Si coordina con le linee di business con particolare riguardo alle attività di individuazione e pianificazione delle iniziative ICT. Svolge attività di coordinamento in caso di incidenti di sicurezza informatica. A garanzia dell'unitarietà della visione gestionale e del rischio ICT e di sicurezza, nonché dell'uniformità di applicazione delle norme riguardanti il sistema informativo, riferisce direttamente all'Organo con Funzione di Gestione. Nell'ambito della continuità operativa, la Direzione fornisce supporto al Business Continuity Manager per la definizione e l'aggiornamento del BIA ("Business Impact Analysis") e BCP ("Business Continuity Plan"). ADalla direzione dipendono l'Ufficio Organizzazione e l'Ufficio IT.

Direzione Crediti

La Direzione Crediti coordina l'attuazione degli indirizzi e delle strategie in materia di credito. Partecipa, in coerenza con le strategie e gli obiettivi aziendali, alla definizione degli indirizzi di strategia creditizia e delle linee guida in materia di assunzione e gestione dei rischi di credito della Banca. Garantisce la qualità del credito erogato indirizzando, autorizzando – per quanto di competenza – e monitorando l'assunzione e la gestione dei rischi di credito della Banca. Monitora l'evoluzione della qualità del portafoglio crediti della Banca, promuove la realizzazione degli interventi correttivi a garanzia della qualità del credito. Assume, direttamente o sottoponendole agli Organi competenti, le decisioni creditizie e garantisce il presidio del credito problematico, supervisiona le attività di credito della Banca, ivi compreso il credito su pegno ed è responsabile di tutte le figure di Rete dedicate al credito e della individuazione e valorizzazione di eventuali errori affinché gli stessi siano utilizzati per definire le migliori best practice. Il Responsabile della Direzione Crediti è inoltre il "Referente per l'attività esternalizzata".

Unità organizzative

Alle unità organizzative è assegnata la responsabilità dell'esecuzione, del buon funzionamento e dell'efficace applicazione nel tempo dei processi. La normativa interna individua le unità organizzative cui è assegnata la responsabilità della progettazione dei processi.

Le unità organizzative hanno la responsabilità di:

- suggerire, alla luce dei principi di comportamento e di controllo prescritti per la disciplina delle attività sensibili, possibili migliorie alle prassi e i processi di propria competenza, al fine di renderli adeguati a prevenire comportamenti illeciti;

- segnalare all'Organismo di Vigilanza eventuali situazioni di irregolarità o comportamenti anomali.

In particolare, le predette unità organizzative per le attività aziendali sensibili devono prestare la massima e costante cura nel verificare l'esistenza e nel porre rimedio ad eventuali carenze di normative o di procedure che potrebbero dar luogo a prevedibili rischi di commissione di illeciti presupposto nell'ambito delle attività di propria competenza.

Datore di lavoro ai sensi del D.Lgs. n. 81/2001

Il soggetto individuato quale Datore di Lavoro ai sensi del D.Lgs.81/2008, limitatamente all'ambito di competenza per la gestione dei rischi in materia di salute e sicurezza sui luoghi di lavoro, individua e valuta l'insorgenza di fattori di rischio dai quali possa derivare la commissione di reati di cui al Decreto e promuove eventuali modifiche organizzative volte a garantire un presidio dei rischi individuati. Per gli ambiti di propria competenza, il Datore di Lavoro ai sensi del D.Lgs.81/2008 partecipa, di concerto con le altre strutture interessate e le funzioni aziendali di controllo, alla definizione della struttura del Modello e all'aggiornamento dello stesso, nonché alla predisposizione del piano di formazione.

Attività oggetto di esternalizzazione

La Banca esternalizza alcune attività, o parte di esse, a soggetti terzi.

L'affidamento delle attività agli outsourcer è realizzato in conformità alle prescrizioni delle Autorità di Vigilanza ed è formalizzato attraverso la stipula di specifici contratti che consentono alla Banca:

- di assumere ogni decisione nell'esercizio della propria autonomia, conservando le necessarie competenze e responsabilità sulle attività relative ai servizi esternalizzati (con particolare riferimento alla gestione dei rischi connessi e dei conflitti di interesse);

- di mantenere conseguentemente i poteri di indirizzo e controllo sulle attività esternalizzate.

Ogni contratto di esternalizzazione di funzioni aziendali deve avere almeno i seguenti contenuti:

- una descrizione chiara dell'attività esternalizzata;

- le date di inizio e, ove applicabile, di fine dell'accordo ed i termini di preavviso;

- la normativa che disciplina il contratto;

- nel caso di esternalizzazioni che comportano il trasferimento di dati, clausole che regolano la comunicazione di eventuali violazioni di integrità o riservatezza degli stessi; nel caso di trattamenti di dati personali, la garanzia che questi vengano trattati in conformità al Regolamento UE 2016/679, comprese le procedure per la gestione dei diritti degli interessati e dei c.d. "data breach"; l'indicazione dei paesi dove i dati saranno trattati o conservati, compreso l'obbligo di informare il committente in caso di successive variazioni;

- i livelli di servizio attesi (SLA), espressi in termini oggettivi e misurabili, nonché flussi di informazione necessari al committente per la verifica, nel continuo, del loro rispetto;

- il diritto del committente e delle Autorità competenti di ispezionare e sottoporre il fornitore ad attività di audit, previo ragionevole preavviso, per consentire il monitoraggio dell'accordo; tali diritti possono essere graduati in funzione del rischio stimato per l'attività in fase istruttoria, salvo le più strette prescrizioni previste per l'esternalizzazione di FOI (Funzioni operative importanti);

- l'indicazione della presenza di eventuali conflitti di interesse e le opportune misure per prevenirli o, se non possibile, attenuarli.

- la facoltà della Banca di risolvere il contratto in caso di violazione da parte dell'outsourcer, nell'esecuzione delle attività esternalizzate: i) di norme di legge e altre disposizioni regolamentari che possono comportare sanzioni a carico del Committente; ii) dei principi contenuti nel Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs.231/2001 adottato dalla Banca, nonché del Codice Etico.

Ogni contratto viene sottoposto alla verifica della Funzione Compliance, della Funzione Antiriciclaggio e della Funzione Legale che verificano, sulla base delle proprie competenze, il rispetto di tutti i requisiti necessari per l'esternalizzazione. Possono essere coinvolte, inoltre, a vario titolo altre Funzioni della Banca su diversi aspetti di competenza connessi all'esternalizzazione (es. Risk Management, Ufficio IT, Ufficio Organizzazione, Responsabile della Protezione dei Dati). Apposite Funzione della Banca verificano nel continuo la rispondenza del servizio prestato dall'outsourcer ai termini stabiliti contrattualmente.

Carifermo si è dotata di una "Politica delle esternalizzazioni" per un'adeguata gestione normativa delle esternalizzazioni delle funzioni aziendali della Banca. All'interno della policy viene definito un sistema di regole di riferimento affinché i processi di selezione, controllo e mitigazione dei rischi connessi all'attività svolta dagli outsourcer si espletino nel pieno rispetto di specifici principi di controllo e responsabilità.

3 ORGANISMO DI VIGILANZA

3.1 Natura e composizione

Il compito di vigilare continuativamente sull'efficace attuazione, sul funzionamento, sull'osservanza del Modello e di proporne l'aggiornamento al fine di migliorarne l'efficacia nella prevenzione dei reati e degli illeciti, in conformità all'art.6 del D.Lgs.231/2001, è affidato all'Organismo di Vigilanza, dotato di autonomi poteri di iniziativa e controllo.

Le Istruzioni di Vigilanza prudenziale delle Banche, circolare 285 di Banca d'Italia, Titolo V, capitolo 7, prevedono espressamente che: *"L'Organo con funzioni di controllo svolge di norma le funzioni dell'organismo di vigilanza – eventualmente istituito ai sensi del D.Lgs.231/2001, in materia di responsabilità degli enti – che vigila sul funzionamento e l'osservanza dei modelli di organizzazione e di gestione di cui si dota la banca per prevenire i reati rilevanti ai fini del medesimo decreto legislativo. Le banche possono affidare tali funzioni a un organismo appositamente istituito dandone adeguata motivazione".*

In conformità al suddetto disposto regolamentare ed allo scopo di migliorare, anche in termini di standard professionali, autonomia ed indipendenza, l'efficienza e l'efficacia dei presidi a fronte dei rischi di violazione del Modello, la Banca ha deciso di attribuire le funzioni di Organismo di Vigilanza ai componenti effettivi del Collegio Sindacale. Dell'avvenuto affidamento di tali funzioni al Collegio Sindacale è data formale comunicazione a tutti i livelli aziendali.

Il Collegio Sindacale nello svolgimento di dette funzioni opera sulla base di uno specifico Regolamento approvato dal medesimo, mantenendo distinte e separate le attività svolte quale Organismo da quelle svolte nelle sue qualità di Organo con funzione di controllo della Banca.

Al fine di svolgere le attività previste dall'art.6 comma 1 del D.Lgs.231/2001, l'Organismo di Vigilanza (nel prosieguo anche "OdV") si avvale della collaborazione delle funzioni aziendali di controllo della Banca (Internal Audit, Risk Management, Compliance e Antiriciclaggio), così da poter ricevere il più adeguato flusso di informazioni (campionamenti statistici, analisi e valutazione dei rischi, consulenza nell'individuazione delle regole di prevenzione dei rischi o nella predisposizione dei meccanismi burocratici di contrapposizione dei compiti, ecc.) ed il supporto necessario per l'analisi e valutazione periodica del rischio effettuato dalle stesse funzioni aziendali.

La partecipazione al Collegio Sindacale è presupposto di quella all'Organismo di Vigilanza, di conseguenza al venire meno del primo incarico cessa automaticamente il secondo.

Laddove ne ravvisi la necessità in funzione della specificità degli argomenti trattati, l'Organismo di Vigilanza può avvalersi di altre strutture aziendali ovvero di consulenti esterni.

3.2 Cause di ineleggibilità e decadenza

I componenti dell'Organismo di Vigilanza devono possedere i requisiti di professionalità, indipendenza e onorabilità.

Fermi restando tali requisiti, costituiscono cause di ineleggibilità e decadenza da membro dell'OdV:

- essere stata esercitata l'azione penale, nelle forme previste dal codice di procedura penale, in relazione ad uno dei reati (consumati o tentati) previsti dal D.Lgs.231/2001; a questo fine, sono immediatamente ed automaticamente recepite nel presente Modello eventuali modificazioni e/o integrazioni delle fattispecie di reato previste dal D.Lgs.231/2001;

- essere destinatario di misure cautelari personali, coercitive o interdittive, per uno dei reati (consumati o tentati) previsti dal D.Lgs.231/2001;

- aver riportato condanna, con sentenza passata in giudicato, ad una pena che comporta l'interdizione, anche temporanea, dai pubblici uffici o l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese; la sentenza di patteggiamento viene considerata equivalente ad una sentenza di condanna;

- aver rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, anche con provvedimento non definitivo, le sanzioni previste dall'art.9 del medesimo Decreto, per illeciti commessi durante la loro carica;

- incorrere nella revoca o decadenza della carica di sindaco, anche in conseguenza del venir meno dei requisiti di professionalità, onorabilità e indipendenza prescritti dalla Legge o dallo Statuto;

- essere coniuge, ovvero parente o affine entro il 3° grado di dipendenti o collaboratori, a qualsiasi titolo, dirigenti (con contratto di lavoro subordinato e/o di consulenza), amministratori e sindaci della società;

- essere socio della società, anche indirettamente, con una partecipazione superiore allo 0,10% del capitale sociale;
- essere stato interdetto, inabilitato, affiancato da un amministratore di sostegno;
- aver violato il Codice Etico, ovvero i principi che lo informano.

Il membro dell'OdV che versi in una condizione di ineleggibilità o decadenza, deve darne immediata comunicazione al Consiglio di Amministrazione. L'omessa comunicazione da parte del componente dell'Organismo ne determina l'immediata decadenza da tale funzione.

Fuori dai casi precedenti, il Consiglio di Amministrazione può comunque ritenere ineleggibile o revocare dall'incarico colui nei cui confronti sia stato iniziato un procedimento penale per i reati, consumati o tentati, previsti dal D.Lgs.231/2001, nonché per delitti dolosi, consumati o tentati, commessi con violenza o minaccia alle persone o per delitti, consumati o tentati, contro il patrimonio, mediante violenza o frode.

L'OdV o uno dei suoi membri può essere inoltre revocato, con delibera del Consiglio di Amministrazione, per inadempienza agli obblighi/funzioni, di seguito stabiliti, o comunque per comportamenti gravemente lesivi dei principi di imparzialità, correttezza e trasparenza connessi allo svolgimento dell'incarico o legati all'attività della Banca, ovvero per la perdita dei c.d. requisiti di onorabilità.

In caso di revoca o recesso, il CdA provvede alla nomina contestuale di un nuovo membro.

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea, ad un componente effettivo dell'Organismo di Vigilanza di svolgere le proprie funzioni ovvero di svolgerle con la necessaria indipendenza ed autonomia di giudizio, questi è tenuto a dichiarare la sussistenza del legittimo impedimento e, qualora esso sia dovuto ad un potenziale conflitto di interessi, la causa da cui il medesimo deriva astenendosi dal partecipare alle sedute dell'Organismo stesso o alla specifica delibera cui si riferisca il conflitto stesso, sino a che il predetto impedimento perduri o sia rimosso.

3.3 Autonomia dell'Organismo di Vigilanza

L'Organismo di Vigilanza è dotato di autonomi poteri di iniziativa e di controllo sull'attività della Banca. Non gli sono attribuiti poteri di gestione. Al fine di svolgere, in completa indipendenza, le proprie funzioni, l'Organismo di Vigilanza dispone di autonomi poteri di spesa sulla base di un budget annuale approvato dal Consiglio di Amministrazione.

3.4 Funzione e Poteri

All'Organismo di Vigilanza è affidato il compito di vigilare:

- sull'effettività del Modello, ossia vigilare affinché i comportamenti posti in essere all'interno della Banca corrispondano al Modello adottato;

- sull'efficacia del Modello, ossia verificare che il Modello predisposto sia concretamente idoneo a prevenire il verificarsi dei reati previsti dalla Legge e dai successivi provvedimenti che ne modifichino il campo di applicazione;
- sull'osservanza delle prescrizioni contenute nel Modello e delle disposizioni in esso richiamate da parte dei destinatari (dipendenti, soggetti apicali, soggetti terzi e in generale tutti coloro che operano in nome e per conto della Banca);
- sull'opportunità di aggiornamento del Modello, al fine di adeguarlo alle modifiche legislative ed alle modifiche della struttura aziendale.

Al fine dell'assolvimento dei compiti sopra indicati, l'Organismo di Vigilanza dovrà:

- predisporre, all'inizio di ciascun esercizio, un piano di attività;
- procedere alla formazione di un Regolamento di funzionamento interno, da sottoporre al Consiglio di Amministrazione;
- determinare il budget annuale che si dovesse rendere necessario per lo svolgimento delle attività, da sottoporre al vaglio del Consiglio di Amministrazione per il relativo stanziamento; eventuali integrazioni al budget, che si dovessero rendere necessarie, saranno comunicate al Consiglio di Amministrazione;

Inoltre, l'Organismo di Vigilanza può:

- avvalersi, sotto la propria sorveglianza, dell'ausilio delle strutture della Banca e/o di consulenti esterni;
- effettuare verifiche e ispezioni mirate su determinate operazioni o atti specifici, posti in essere nell'ambito delle attività a rischio-reato, per come individuate nella parte speciale;
- raccogliere, elaborare e conservare le informazioni rilevanti ai fini dell'attuazione del Modello e in vista di un suo eventuale adattamento;
- condurre indagini interne per l'accertamento di eventuali violazioni delle prescrizioni del Modello e per l'esercizio dell'azione disciplinare;

Ai fini dello svolgimento e della realizzazione delle proprie funzioni, l'OdV:

- è dotato di autonomi poteri di iniziativa e di controllo e la sua attività non può essere sindacata da alcun altro organismo o struttura della Banca, fatte salve le ipotesi di inadempienza agli obblighi;
- si colloca, nell'organigramma aziendale, al di fuori di qualsiasi autorità gerarchica di line, come organo indipendente;
- dovrà essere munito di un'adeguata dotazione di risorse finanziarie per l'efficace svolgimento dei suoi compiti, nonché di una casella di posta elettronica, che saranno comunicate a tutti i dipendenti;
- ha libero accesso a tutte le funzioni e le strutture della Banca, nonché ad ogni documentazione ed archivio, senza necessità di alcuna autorizzazione preventiva, per ottenere ogni informazione o dato reputato rilevante per lo svolgimento dei compiti previsti dal D.Lgs.231/2001.

L'OdV svolge le proprie funzioni con imparzialità, correttezza e trasparenza. In particolare:

- non svolge alcun ruolo operativo, che ne minerebbe l'autonomia e l'obiettività di giudizio al momento delle verifiche, né esercita alcun potere di ingerenza nella gestione aziendale e, quanto alla vigilanza sull'effettività e l'adeguatezza del modello, è gravato dal dovere di evidenziarne la idoneità e la congruità nel tempo, suggerendo le opportune e necessarie modifiche ed integrazioni, in dipendenza di significative violazioni del modello, ovvero del Codice Etico, di modificazioni dell'assetto societario o dell'attività di impresa, nonché di variazioni del quadro normativo;
- deve di riferire annualmente, con relazione scritta, al Consiglio di Amministrazione sullo stato di attuazione e di effettività del Modello, proponendo, ove necessario, modificazioni, adattamenti ed integrazioni;
- cura l'archiviazione e la conservazione, di ogni documento relativo all'attività espletata ed alla corrispondenza ricevuta ed inviata;

All'OdV (e ai suoi eventuali collaboratori, esterni o interni) è fatto divieto di rivelare a terzi estranei alla Banca tutte le notizie, le informazioni e le decisioni, concernenti l'attività della Banca, di cui venga a conoscenza nell'esercizio delle sue funzioni.

Inoltre, al fine di garantire l'assoluta autonomia e indipendenza dell'OdV, è fatto divieto ai suoi membri di intrattenere con la Banca, anche per interposta persona, rapporti di carattere economico, fatti salvi quelli intrattenuti a condizioni praticate in via ordinaria.

3.5 Regole di funzionamento dell'OdV

Le regole di funzionamento dell'OdV, coerenti con le disposizioni interne della Carifermo e conformi alle Linee Guida, sono illustrate nei paragrafi successivi.

3.6 Flussi informativi e reporting

Al fine di garantire l'autonomia e l'indipendenza necessarie allo svolgimento dei compiti affidati, l'OdV riporta direttamente al Consiglio di Amministrazione.

In particolare, l'OdV è tenuto a presentare una *relazione scritta* sugli esiti delle proprie attività al Consiglio di Amministrazione con periodicità almeno annuale e comunque ogni volta che risulti essere necessario a seguito di interventi normativi o al manifestarsi di segnali di criticità che potrebbero dar luogo ad infrazioni della normativa di riferimento.

Nella relazione periodica devono essere descritti:

- l'attività svolta, indicando in particolare i controlli effettuati, l'esito degli stessi e l'eventuale aggiornamento dei 'processi sensibili' e dei reati;
- le eventuali criticità emerse sia in termini di comportamenti o eventi interni, sia in termini di efficacia del Modello;
- gli interventi correttivi e migliorativi da attuare;
- la verifica della rimozione delle anomalie segnalate in precedenza e la realizzazione degli interventi richiesti;
- il piano annuale delle attività di controllo.

Infine, l'OdV provvede a segnalare tempestivamente al Consiglio di Amministrazione eventuali violazioni del Modello da parte di soggetti apicali, dipendenti della Banca e soggetti terzi (collaboratori e fornitori) che interagiscono con la stessa.

L'OdV deve essere tempestivamente e periodicamente informato, mediante apposite segnalazioni, da parte dei soggetti apicali, dei dipendenti e dei soggetti terzi in merito a quegli atti, comportamenti od eventi che possano determinare una violazione del Modello o che, più in generale, sono rilevanti ai fini del Decreto.

FLUSSI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Flussi informativi in caso di segnalazioni - Whistleblowing

Il D.Lgs 24/2023, emanato in attuazione della Direttiva (UE) 2019/1937, ha disciplinato in modo organico la materia dei sistemi di segnalazione e in particolare ha modificato il D.Lgs. 231/2001 sostituendo i commi 2-bis, 2-ter e 2-quater dell'art. 6, che disciplinavano tali sistemi, con un nuovo comma 2-bis il quale dispone che i modelli di organizzazione e gestione prevedano i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare ai sensi del D.Lgs. 24/2023, di fatto rinviando a quest'ultimo per la relativa disciplina. I riferimenti dei canali interni sono pubblicizzati sia nella intranet aziendale sia sul sito internet della Banca nelle sezioni dedicate.

In base a quanto previsto D.Lgs 24/2023, le segnalazioni possono essere effettuate da: lavoratori dipendenti e i lavoratori autonomi che svolgono o hanno svolto la propria attività lavorativa presso la Banca, titolari di un rapporto di collaborazione professionale, lavoratori o collaboratori che forniscono beni o servizi o che realizzano opere in favore di terzi e svolgono o hanno svolto la propria attività lavorativa presso la Banca, liberi professionisti e i consulenti che svolgono o hanno svolto la propria attività lavorativa presso la Banca, volontari e i tirocinanti (retribuiti e non retribuiti), gli azionisti (persone fisiche), le persone con funzione di amministrazione, controllo, vigilanza o rappresentanza.

L'Organismo di Vigilanza deve essere informato, mediante apposite segnalazioni da parte del personale interno della Banca (Organi e Dirigenti, Funzioni di Controllo, Responsabili di Funzione, Dipendenti) e dei soggetti esterni (intendendosi per tali i fornitori, i consulenti, i professionisti, i lavoratori autonomi o parasubordinati, i partner commerciali o altri soggetti) in merito ad eventi o situazioni che potrebbero ingenerare una responsabilità di Carifermo, ai sensi del D.Lgs. 231/2001.

Devono essere segnalate senza ritardo le notizie circostanziate, fondate su elementi di fatto precisi e concordanti, concernenti:

- la commissione, ovvero la potenziale commissione, di illeciti per i quali è applicabile il D.Lgs.231/2001;

- le violazioni delle regole di comportamento o procedurali contenute nel presente Modello e nella normativa in esso richiamata.

Con riferimento al sistema di gestione Whistleblowing, Carifermo ha definito specifici canali interni di segnalazione:

- E-mail allo specifico indirizzo whistleblowing@carifermo.it;

- Comunicazione scritta indirizzata al “Responsabile whistleblowing” c/o Cassa di Risparmio di Fermo S.p.A., Via Don Ernesto Ricci 1, 63900 Fermo;

- Comunicazione orale, su richiesta del soggetto segnalante, mediante un incontro diretto con il Responsabile Whistleblowing, da richiedere alla Cassa di Risparmio di Fermo (+39 0734 2861).

La Banca, inoltre, ha istituito un canale di comunicazione specifico, autonomo e indipendente dalle ordinarie linee di reporting, volto alla raccolta delle segnalazioni e alla corretta gestione dei flussi informativi ad essa collegati. In particolare è disponibile una procedura informatica finalizzata alla gestione dei sistemi di whistleblowing individuata nell’applicativo “Comunica Whistleblowing”, volto alla gestione delle attività legate all’intero processo di segnalazione che garantisce la riservatezza del soggetto segnalante.

La Banca ha individuato nel Responsabile della Funzione di Revisione Interna (Internal Audit) e nel Responsabile della Funzione Antiriciclaggio (per le segnalazioni relative alla specifica materia AML) i soggetti preposti all’attività di ricezione, analisi e valutazione delle segnalazioni (comprese le segnalazioni inerenti presunti illeciti, tra quelli previsti dal Modello 231 della Cassa di Risparmio di Fermo S.p.a., da parte di esponenti aziendali nell’interesse o a vantaggio della società) definendoli soggetti Responsabili dei sistemi interni di segnalazione delle violazioni.

L’Organismo di Vigilanza viene informato circa le segnalazioni effettuate nel caso in cui le stesse siano relative a fatti/comportamenti che possano comportare la responsabilità della Banca e presentino elementi di fondatezza.

Per le modalità di gestione e rendicontazione delle segnalazioni pervenute attraverso gli specifici canali predisposti dalla Banca ai sensi del D.Lgs. 24/2023, si rinvia a quanto previsto dalla “Policy Whistleblowing” adottata dalla Banca.

Carifermo garantisce misure di protezione per i segnalanti, qualunque sia il canale utilizzato, da qualsiasi forma di ritorsione, discriminazione o penalizzazione e assicura in ogni caso la massima riservatezza circa la loro identità, fatti salvi gli obblighi di legge. Tali misure sono estese anche alle persone collegate (es. parenti del segnalante che hanno rapporti lavorativi con la società e ‘facilitatori’). Il sistema disciplinare previsto dal Decreto, in attuazione del quale sono stabilite le sanzioni indicate nel Capitolo 5 che segue, si applica anche a chi:

- viola gli obblighi di riservatezza sull’identità del segnalante o i divieti di atti discriminatori o ritorsivi;

- effettua con dolo o colpa grave segnalazioni di fatti che risultino infondati.

Flussi informativi periodici

Il D.Lgs.231/2001 prevede l’obbligo di stabilire appositi flussi informativi nei confronti dell’Organismo di Vigilanza, relativi all’esecuzione delle attività sensibili. I flussi informativi hanno ad oggetto tutte le informazioni e tutti i documenti che devono pervenire all’Organismo di Vigilanza al fine di consentire a quest’ultimo di aumentare il livello di conoscenza della Banca, di acquisire informazioni atte a

valutare la rischiosità insita in taluni processi sensibili, nonché di svolgere le proprie attività di verifica e di vigilanza in merito all'efficacia e all'osservanza del Modello.

L'Organismo di Vigilanza esercita le proprie attività di vigilanza e controllo anche mediante l'analisi di flussi informativi periodici trasmessi dalle funzioni che svolgono attività di controllo di primo livello (Unità operative), dalle funzioni che svolgono attività di controllo di secondo livello (Funzione Compliance, Risk Management e Antiriciclaggio), dalle funzioni che svolgono controllo di terzo livello (Funzione Internal Audit) e per quanto concerne gli ambiti normativi specialistici, dalle strutture interne funzionalmente competenti e dai ruoli aziendali istituiti ai sensi delle specifiche normative di settore.

Flussi informativi provenienti dalle Unità Organizzative

I responsabili delle Unità Organizzative coinvolte nei processi sensibili ai sensi del D.Lgs.231/01, laddove richiesto dall'Organismo di Vigilanza, attestano il livello di attuazione del Modello con particolare attenzione al rispetto dei principi di controllo e comportamento e delle norme operative, evidenziando le eventuali criticità nei processi gestiti e agli scostamenti rispetto al Modello. Tali attestazioni sono inviate al Direttore Generale, il quale archivierà la documentazione, tenendola a disposizione dell'Organismo di Vigilanza, per il quale produrrà una relazione sulle risultanze.

Flussi informativi provenienti dalla Funzione di Compliance

La funzione di Conformità, nelle verifiche condotte e nelle relazioni prodotte per gli Organi Aziendali, tiene conto anche dei rischi di non conformità alla normativa sulla responsabilità amministrativa degli enti, derivanti da carenze nei processi. Nella relazione annuale prodotta dalla Funzione per l'OFSS, che viene condivisa anche con l'OdV, vengono comunicate le attività svolte e l'esito delle stesse, gli interventi correttivi e migliorativi pianificati (inclusi quelli formativi) e il loro stato di realizzazione, nonché le principali variazioni intervenute nei processi, nelle policy e nei regolamenti.

Flussi informativi provenienti dalla Funzione Internal Audit

Il flusso di rendicontazione della Funzione Internal Audit verso l'Organismo di Vigilanza consiste in relazioni annuali, con le quali quest'ultimo è informato sulle verifiche svolte, sulle principali risultanze, sulle azioni riparatrici poste in essere, sugli ulteriori interventi di controllo in programma, nel rispetto del Piano di Audit. Nell'ambito di tale rendicontazione è data evidenza delle segnalazioni i cui approfondimenti hanno evidenziato tematiche sensibili ai fini del D.Lgs.231/2001. Laddove ne ravvisi la necessità, l'Organismo di Vigilanza richiede alla Funzione Internal Audit copia dei report di dettaglio per i punti specifici che ritiene di voler meglio approfondire.

Flussi informativi provenienti dalla Funzione Antiriciclaggio

I flussi di rendicontazione della Funzione Antiriciclaggio verso l'Organismo di Vigilanza consistono, con cadenza semestrale, nel "Report periodico operatività antiriciclaggio" prodotto dalla Funzione con cadenza trimestrale e già destinato al Comitato Esecutivo e Direttore Generale, che espone un quadro sintetico dell'attività periodica della Funzione, dei controlli antiriciclaggio predisposti e dell'attività in segnalazioni di operazioni sospette e, con cadenza annuale, nella Relazione Antiriciclaggio comprensiva dell'esercizio di autovalutazione del rischio di riciclaggio e finanziamento del terrorismo.

Flussi informativi da parte del Datore di Lavoro ai sensi del D.Lgs.81/08

Il flusso di rendicontazione del Datore di Lavoro ai sensi del D.Lgs.81/08 verso l'Organismo di Vigilanza è incentrato su relazioni annuali, con le quali vengono comunicati gli esiti delle attività svolte in relazione all'organizzazione e al controllo effettuato sul sistema di gestione aziendale della salute e sicurezza.

Flussi informativi da parte dell'Ufficio Risorse Umane

Il flusso di rendicontazione dell'Ufficio Risorse Umane verso l'Organismo di Vigilanza consiste in un'informativa trimestrale prodotta dall'Ufficio per l'OFSS sui provvedimenti disciplinari comminati al personale nel periodo di riferimento. Laddove ne ravvisi la necessità l'Organismo di Vigilanza richiede all'Ufficio Risorse Umane un'informativa di dettaglio con evidenza degli eventuali eventi collegati direttamente o indirettamente a segnalazioni di condotte illecite previste nel Decreto ovvero violazioni del Modello.

Altri flussi informativi

In aggiunta ai flussi di cui sopra, sarà cura dell'Organismo di Vigilanza richiedere eventualmente ulteriori flussi informativi a supporto delle proprie attività di vigilanza sul funzionamento e l'osservanza del Modello, definendo le relative modalità e tempistiche di trasmissione.

3.7 Verifiche dell'adeguatezza del Modello

L'OdV effettua periodicamente specifiche verifiche dell'adeguatezza del Modello ovvero della sua reale capacità di prevenire i reati.

Tali attività di verifica si concretizzano nello svolgimento di controlli a campione sui principali processi sensibili, e sui contratti di maggior rilevanza conclusi dalla Banca, nel rispetto di quanto previsto nel piano annuale delle attività.

Inoltre, da parte dell'OdV deve essere svolta un'attività di analisi delle segnalazioni ricevute e delle eventuali azioni intraprese, e deve essere effettuata una verifica sull'effettiva e corretta attuazione, da parte delle strutture aziendali interessate, di eventuali soluzioni proposte per l'incremento dell'efficacia del Modello.

4 DIFFUSIONE E FORMAZIONE SUL MODELLO

Il regime della responsabilità amministrativa previsto dalla normativa di legge e l'adozione del Modello di organizzazione, gestione e controllo da parte della Banca formano un sistema che deve trovare nei comportamenti operativi del personale una coerente ed efficace risposta.

L'adeguata formazione e la costante informazione dei Dipendenti, Collaboratori in ordine ai principi ed alle prescrizioni contenute nel Modello rappresentano fattori di grande importanza per la corretta ed efficace attuazione del sistema di prevenzione aziendale.

Tutto il personale della Banca è tenuto ad avere piena conoscenza degli obiettivi di correttezza e trasparenza che si intendono perseguire con il Modello e delle modalità attraverso le quali la Banca ha inteso perseguirli, apportando un sistema di procedure e controlli.

Al riguardo è pertanto fondamentale un'attività di comunicazione e di formazione finalizzata a favorire la diffusione di quanto stabilito dal Decreto e dal Modello adottato nelle sue diverse componenti (gli strumenti aziendali presupposto del Modello, le finalità del medesimo, la sua struttura e i suoi elementi fondamentali, il sistema dei poteri e delle deleghe, l'individuazione dell'Organismo di Vigilanza, i flussi informativi verso quest'ultimo, le tutele previste per chi segnala fatti illeciti, ecc.). Ciò affinché la conoscenza della materia e il rispetto delle regole che dalla stessa discendono costituiscano parte integrante della cultura professionale di ciascun collaboratore.

Con questa consapevolezza, le attività di formazione e comunicazione interna - rivolte a tutto il personale - hanno il costante obiettivo, anche in funzione degli specifici ruoli assegnati, di creare una conoscenza diffusa e una cultura aziendale adeguata alle tematiche in questione, mitigando così il rischio della commissione di illeciti.

4.1 Formazione e informazione dei Dipendenti

Ai fini dell'efficacia del presente Modello, la Carifermo garantisce la conoscenza e la divulgazione presso i Dipendenti del Decreto, del Modello, del Codice Etico, di tutti i regolamenti e disposizioni interne.

Ai fini dell'attuazione del Modello, il sistema di formazione ed informazione verso il Personale è supervisionato e coordinato dall'Ufficio Risorse Umane, con la collaborazione dell'Organismo di Vigilanza.

Con riguardo all'attività formativa, la stessa sarà effettuata mediante corsi specifici sulla base delle necessità intervenute e potrà risultare differenziata nei contenuti e nelle modalità di erogazione.

L' OdV si coordina con la Funzione di Conformità per definire contenuti formativi da pubblicare sulle piattaforme aziendali dedicate alla formazione.

Le modifiche sono rese note al personale tramite disposizioni interne.

4.2 Informazione ai soggetti terzi

Con riguardo all'attività informativa, ai soggetti terzi che instaurano rapporti di collaborazione / fornitura con la Carifermo sarà messo a disposizione il Modello di Organizzazione, Gestione e Controllo adottato dalla Banca e il Codice Etico e sarà fornita idonea informativa sulle conseguenze del mancato rispetto dei principi del medesimo e delle regole di condotta, anche mediante l'inserimento nei contratti di apposite clausole contrattuali inerenti il rispetto del D.Lgs.231/2001.

5 SISTEMA DISCIPLINARE

5.1 Funzione del sistema sanzionatorio

La definizione di un sistema di sanzioni (commisurate alla gravità della violazione e dotate di deterrenza), applicabili in caso di mancato rispetto delle regole di cui al presente Modello, rende più efficace la prevenzione dei reati agevolando l'attività di vigilanza dell'OdV e l'osservanza del Modello stesso.

La definizione di tale sistema sanzionatorio costituisce, infatti, ai sensi dell'art. 6, comma 1, lettera e) del Decreto, un requisito essenziale del Modello ai fini dell'esimente rispetto alla responsabilità dell'Ente.

Le sanzioni previste dal sistema sanzionatorio sono da attivare indipendentemente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria, nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del Decreto.

5.2 Sistema sanzionatorio per il Personale dipendente

La violazione, da parte dei Dipendenti soggetti al CCNL, delle singole regole comportamentali contenute nel Modello organizzativo costituisce illecito disciplinare.

Sono altresì previste sanzioni connesse alla violazione del divieto di atti di ritorsione nei confronti dei segnalanti e all'utilizzo abusivo dei canali di segnalazione ("whistleblowing").

5.2.1 Dipendenti inquadrati nella categoria dei dirigenti

In caso di violazione, da parte dei Dirigenti, delle prescrizioni del Modello organizzativo o di adozione, nell'espletamento delle attività a rischio reato, di un comportamento non conforme alle disposizioni del Modello, Carifermo applica, nei confronti degli stessi, le misure più idonee in conformità con quanto normativamente previsto.

Fermi restando gli obblighi per l'Ente, nascenti dallo Statuto dei Lavoratori e dal Contratto Collettivo e dai regolamenti interni applicabili, i comportamenti sanzionabili che costituiscono violazione del Modello organizzativo sono i seguenti:

- violazione di procedure interne previste dal Modello (ad esempio non osservanza delle procedure prescritte, omissione di comunicazioni all'OdV, omissione di controlli, etc.);
- adozione, nell'espletamento delle attività a rischio reato, di comportamenti non conformi alle prescrizioni del Modello;
- violazione di procedure interne previste dal Modello o adozione, nell'espletamento delle attività a rischio reato, di comportamenti palesemente in violazione delle prescrizioni del Modello, che espongano la Banca ad una situazione oggettiva di rischio imminente di commissione di uno dei reati previsti.

Le sanzioni e l'eventuale richiesta di risarcimento dei danni verranno commisurate al livello di responsabilità del Dirigente, all'eventuale presenza di precedenti disciplinari a carico del Dirigente stesso, all'intenzionalità del comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Banca può ragionevolmente ritenersi esposta a seguito della condotta

censurata. Le sanzioni saranno applicate dalla funzione competente, anche su segnalazione motivata dell'OdV.

5.2.2 Dipendenti inquadrati nelle altre categorie

Con riguardo ai lavoratori dipendenti non dirigenti, il Decreto prevede che i provvedimenti disciplinari avverranno nei limiti imposti dall'art. 7 della legge n. 300/1970 (c.d. "Statuto dei Lavoratori") e dalla contrattazione collettiva di settore e aziendale e nel rispetto delle leggi vigenti in materia.

Il sistema disciplinare correntemente applicato dalla Carifermo ai Quadri direttivi e al Personale delle aree professionali (dalla 1° alla 3°), in linea con le disposizioni vigenti, prevede:

- rimprovero verbale;
- rimprovero scritto;
- sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni;
- licenziamento per giustificato motivo;
- licenziamento per giusta causa.

Restano ferme – e si intendono qui richiamate – tutte le disposizioni, previste dalla legge e dai Contratti Collettivi in vigore, relative agli obblighi da osservare nell'applicazione delle sanzioni.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri conferiti, nei limiti della rispettiva competenza, agli organi societari e alle funzioni aziendali competenti.

Fermi restando gli obblighi per la Banca, nascenti dallo Statuto dei Lavoratori e dal Contratto Collettivo e dai regolamenti interni applicabili, i comportamenti sanzionabili che costituiscono violazione del Modello sono i seguenti:

- adozione, nell'espletamento dei processi sensibili, di comportamenti non conformi alle prescrizioni del Modello e diretti in modo univoco al compimento di uno o più reati nell'interesse ed a vantaggio della Banca;
- adozione, nell'espletamento dei processi sensibili, di comportamenti in palese violazione delle prescrizioni del Modello, tali da determinare la concreta applicazione a carico della Banca di sanzioni previste dal Decreto.

Le sanzioni e l'eventuale richiesta di risarcimento dei danni verranno commisurate al livello di responsabilità e autonomia del Dipendente, all'eventuale presenza di precedenti disciplinari a carico dello stesso, all'intenzionalità del comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Banca può ragionevolmente ritenersi esposta a seguito della condotta censurata. Le sanzioni saranno applicate dalla funzione competente, anche su segnalazione motivata dell'OdV, sentito il superiore gerarchico dell'autore della condotta censurata.

Per quanto riguarda l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, alle funzioni preposte all'interno della Banca.

5.3 Misure nei confronti degli Amministratori e dei Sindaci

In caso di violazione del presente Modello da parte di soggetti che ricoprono la funzione di componenti del Consiglio di Amministrazione della Banca o Sindaci della Carifermo, l'OdV informerà l'intero Consiglio d'Amministrazione, il quale prenderà gli opportuni provvedimenti, con riferimento a quanto disposto dalle norme di legge in vigore e con obbligo di informazione alla prima Assemblea dei Soci.

5.4 Misure nei confronti di soggetti terzi

Con riguardo a soggetti terzi, quali collaboratori esterni e fornitori con cui la Società entri in contatto nello svolgimento di relazione d'affari, l'informativa in merito alle conseguenze a fronte di eventuali comportamenti posti in essere in violazione del Modello e del Codice Etico (quali ad esempio l'immediata risoluzione del contratto o il mancato rinnovo dell'incarico/fornitura) viene data mediante apposita lettera che tali soggetti sono tenuti a sottoscrivere per presa conoscenza ed accettazione.

PARTE SPECIALE

6 GLI ILLECITI PRESUPPOSTO – AREE ED ATTIVITÀ SENSIBILI ED IL SISTEMA DI CONTROLLO

L'art. 6, comma 2, del D.Lgs. n. 231/01 prevede che il Modello debba "individuare le attività nel cui ambito possono essere commessi reati".

Nell'ambito della presente Parte Speciale del Modello vengono individuate le attività potenzialmente a rischio di commissione di un reato presupposto, già identificate in fase di risk assessment.

Sono state oggetto di analisi le singole fattispecie di reati presupposto per le quali trova applicazione il Decreto.

In relazione a ciascuna categoria dei medesimi sono state identificate in Carifermo le aree aziendali nell'ambito delle quali sussiste il rischio di commissione dei reati.

Per ciascuna di tali aree si sono quindi individuate le singole attività sensibili e qualificati i principi generali di controllo e di comportamento cui devono attenersi tutti coloro che vi operano.

Sulla base delle disposizioni di legge attualmente in vigore ed il sistema organizzativo interno, le aree sensibili identificate dal Modello di Carifermo riguardano in via generale le seguenti fattispecie di reato previste dal Decreto:

1) Reati contro la pubblica amministrazione (artt.24 e 25 d.lgs.231/2001);

2) I reati di falsità in moneta (e valori) (art.25-bis d.lgs.231/2001);

3) I reati societari (art.25-ter d.lgs.231/2001);

4) I reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché di autoriciclaggio (art.25-octies d.lgs.231/2001);

5) I delitti in materia di strumenti di pagamento diversi dai contanti (art.25-octies.1 d.lgs.231/2001);

6) I reati e illeciti amministrativi riconducibili ad abusi di mercato (art.25-sexies d.lgs.231/2001);

7) I reati in tema di salute e sicurezza sul lavoro (art.25-septies d.lgs.231/2001);

8) I reati informatici (art.24-bis d.lgs.231/2001);

9) I reati contro l'industria e il commercio (art.25-quater d.lgs.231/2001);

10) I reati in materia di violazione del diritto d'autore (25-novies d.lgs.231/2001);

11) I reati ambientali (art.25-undecies d.lgs.231/2001);

12) I reati tributari (art.25-quinquiesdecies d.lgs.231/2001).

7 REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (ART.24 E 25 D.LGS.231/2001)

7.1 Fattispecie di reato

Premessa

La presente Parte Speciale è volta a presidiare il rischio di commissione reati realizzabili nei rapporti tra la Banca e la Pubblica Amministrazione.

Con specifico riferimento ai reati di cui agli artt. 24 e 25 del Decreto, si elencano di seguito le fattispecie del Decreto identificate quali rilevanti, in relazione all'operatività della Banca, nell'ambito della presente Parte Speciale:

- Malversazione di erogazioni pubbliche (art. 316 bis c.p.) – art. 24 Decreto;
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.) – art. 24 Decreto;
- Indebita percezione di erogazioni pubbliche (art. 316 ter c.p.) – art. 24 Decreto;
- Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640, comma 2 n.1 c.p.) – art. 24 Decreto;
- Frode informatica in danno dello Stato o di altro ente pubblico (art. 640 ter c.p.) – art. 24 Decreto;
- Concussione (art. 317 c.p.) – art. 25 Decreto;
- Corruzione per l'esercizio della funzione (artt. 318, 320 c.p.) – art. 25 Decreto;
- Corruzione per un atto contrario ai doveri d'ufficio (artt. 319, 319 bis, 320 c.p.) – art. 25 Decreto;
- Corruzione in atti giudiziari (art. 319 ter c.p.) – art. 25 Decreto;
- Pene per il corruttore (art. 321 c.p.) – art. 25 Decreto;
- Istigazione alla corruzione (art. 322 c.p.) – art. 25 Decreto;
- Induzione indebita a dare o promettere utilità (art. 319 quater c.p.) – art. 25 Decreto;
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis c.p.) – art. 25 Decreto;

- Traffico di influenze illecite (art.346-bis c.p.) – art. 25 Decreto;
- Peculato (art.314, comma 1 c.p.) – art.25 Decreto;
- Peculato mediante profitto dell'errore altrui (art.316 c.p.) – art.25 Decreto;
- Abuso d'ufficio (art.323 c.p.) – art. 25 Decreto;
- Frodi nelle pubbliche forniture (art.356 c.p.) – art.24 Decreto;
- Frode ai danni del Fondo Europeo Agricolo – art.24 Decreto;
- Turbata libertà degli incanti (art.353 c.p.) – art.24 Decreto;
- Turbata libertà del procedimento di scelta del contraente (art.353-bis c.p.) – art. 24 Decreto.

Circa il dettaglio delle fattispecie delittuose previste dagli artt. 24 e 25 del Decreto si rimanda all'allegato "Elenco Reati".

Le fattispecie di reato di cui agli artt. 24 e 25 considerate ai fini della presente Parte Speciale possono essere commesse nei confronti di soggetti pubblici, ivi inclusi i pubblici ufficiali, gli incaricati di pubblico servizio e le Autorità di Vigilanza (di seguito "Pubblica Amministrazione").

Pertanto, ai fini del presente documento, per Pubblica Amministrazione si intende qualsiasi persona fisica o giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa, in forza di norme di diritto pubblico e di atti autoritativi. In particolare, a titolo esemplificativo, per Pubblica Amministrazione si intendono:

- *i soggetti pubblici*, ossia, principalmente, membri del Parlamento della Repubblica Italiana, le amministrazioni pubbliche, quali le amministrazioni dello Stato, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le regioni, le province, i comuni e loro consorzi e associazioni, le istituzioni scolastiche di qualsivoglia ordine e grado, le camere di commercio, industria, artigianato e agricoltura, gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del servizio sanitario nazionale;
- *i Pubblici Ufficiali*[2] ossia coloro che, pubblici dipendenti o privati, possano o debbano formare e manifestare la volontà della Pubblica Amministrazione, ovvero esercitare poteri autoritativi o certificativi, nell'ambito di una potestà di diritto pubblico (a titolo esemplificativo e non esaustivo: ufficiali giudiziari, consiglieri comunali, ufficiali sanitari, dipendenti dell'INPS, consulente tecnico del giudice, insegnanti delle scuole pubbliche, etc.);

[2] Pubblico Ufficiale (art.357 c.p.) – "Agli effetti della legge penale, sono pubblici ufficiali, coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

- *gli Incaricati di Pubblico Servizio*[3], ossia coloro che prestano un servizio pubblico svolgendo attività di interesse pubblico, ma non sono dotati dei poteri del pubblico ufficiale ovvero che, pur agendo nell'ambito di un'attività disciplinata nelle forme della pubblica funzione, non esercitano i poteri tipici di questa e non svolgono semplici mansioni d'ordine né prestano opera meramente materiale (a titolo esemplificativo e non esaustivo: operatore della Banca incaricato dell'erogazione di un finanziamento agevolato; esattori dell'Enel, guardie giurate che conducono furgoni portavalori, dipendenti del Poligrafo di Stato, etc.);
- *le Autorità di Vigilanza*, ossia, quegli enti dotati di particolare autonomia e imparzialità il cui obiettivo è la tutela di alcuni interessi di rilievo costituzionale, quali il buon andamento della Pubblica Amministrazione, la libertà di concorrenza, la tutela della sfera di riservatezza professionale, ecc. (a titolo esemplificativo e non esaustivo: Banca d'Italia, Autorità Garante per la Privacy, Autorità Garante per la Concorrenza e il Mercato, etc.).

Tutto ciò premesso si deve tenere presente che la legge non richiede necessariamente, ai fini del riconoscimento in capo ad un determinato soggetto delle qualifiche pubbliche predette, la sussistenza di un rapporto di impiego con un ente pubblico: la pubblica funzione od il pubblico servizio possono essere esercitati, in casi particolari, anche da un privato.

In relazione all'operatività della Banca, a titolo esemplificativo e non esaustivo, si possono individuare quali soggetti appartenenti alla Pubblica Amministrazione i seguenti:

- Amministrazioni dello Stato, anche a ordinamento autonomo, Comuni, Regioni e Province;
- i Ministeri, i Dipartimenti e le Commissioni;
- Aziende municipalizzate e gli Enti pubblici trasformati in S.p.A. (ad es. Poste Italiane, FS, ecc.);
- Camere di commercio, industria, artigianato, agricoltura e l'Ufficio del Registro;
- gli enti pubblici economici e gli enti pubblici non economici nazionali, regionali e locali (INPS, ENASARCO, INAIL, ISTAT);
- le amministrazioni, le aziende e gli enti del Servizio Sanitario regionale;
- Banca d'Italia, Agenzia delle Entrate, AGCM, Autorità Garante della Privacy, etc.

Per le finalità previste dal presente documento, si considerano non solo i rapporti "diretti", ma anche quelli "indiretti" con soggetti che - notoriamente - intrattengono rapporti di qualsivoglia natura (parentela, affinità, coniugo, convivenza, ecc.) con Pubblici Ufficiali o Incaricati di Pubblico Servizio.

Pertanto, i dipendenti ed esponenti che, nell'esercizio delle predette attività di rilevanza pubblica, pongono in essere le condotte tipiche dei pubblici agenti descritte nei reati, ad esempio, di "corruzione", "concussione" e "induzione indebita a dare o promettere utilità", "traffico di influenze illecite" "truffa ai danni dello Stato o di altro Ente pubblico", sono puniti come tali e può inoltre scattare la responsabilità della Banca ai sensi del D.Lgs. n. 231/01.

---

[3] Incaricato di pubblico servizio (art.358 c.p.) – "Agli effetti della legge penale, sono incaricati di pubblico servizio coloro i quali, a qualunque titolo, prestano pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opere meramente materiale".

7.2 Attività aziendali sensibili

Carifermo ha identificato le seguenti attività sensibili nelle quali è rilevante il rischio che siano posti in essere comportamenti illeciti nei rapporti con la Pubblica Amministrazione.

Gestione dei rapporti con Enti pubblici e Pubblica Amministrazione:

- Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione;
- Gestione dei rapporti con le Autorità di Vigilanza e di controllo (Banca d'Italia, Consob, AGCM, Garante privacy etc.);
- Gestione degli interventi agevolativi;
- Gestione delle attività inerenti la richiesta di concessioni, autorizzazioni, licenze o l'esecuzione di adempimenti verso la Pubblica Amministrazione;
- Gestione dei contenziosi (in via stragiudiziale e in via giudiziale) e degli accordi transattivi;
- Gestione e utilizzo dei sistemi informativi della Banca;
- Gestione del processo di selezione, assunzione, amministrazione del personale;
- Gestione della formazione finanziata;
- Gestione degli acquisti di beni e dei servizi, degli incarichi professionali e delle consulenze;
- Gestione di omaggi, liberalità, spese di rappresentanza, beneficenze e sponsorizzazioni;
- Gestione delle valutazioni immobiliari.

Con specifico riferimento alla *"Gestione e utilizzo dei sistemi informativi della Banca"* si rimanda all'attività a rischio-reato oggetto di trattazione nella Parte Speciale "Reati informatici e trattamento illecito dei dati", ove sono individuati i principi generali di controllo e i principi di comportamento aventi efficacia anche a presidio dei reati di cui alla presente Parte Speciale.

Sono di seguito riepilogati e descritti, i protocolli che dettano i principi generali di controllo e i principi di comportamento applicabili alle attività sensibili sopra individuate, che si completano con le policy e i regolamenti della Banca già in essere a cui l'operatività aziendale deve uniformarsi.

Detti protocolli trovano applicazione anche in riferimento alle attività poste in essere, sulla base di appositi contratti di servizio, da consulenti esterni, outsourcer esterni e fornitori di qualsiasi genere che abbiano rapporti con la Banca.

7.2.1 Stipula e Gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), ivi inclusi gli Enti della Pubblica Amministrazione

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione di rapporti contrattuali con la clientela, inclusi gli Enti della Pubblica Amministrazione, ossia i clienti il cui capitale è di proprietà (anche solo parziale) dello Stato o di altri Enti pubblici (es. società municipalizzate) aventi ad oggetto operazioni quali, a titolo esemplificativo e non esaustivo:

- gestione contratti di concessione di finanziamento/credito ordinario;
- gestione finanziamenti diretti alla clientela o ad enti pubblici;
- stipula e gestione di rapporti contrattuali societari e di accordi connessi e funzionali all'instaurazione e alla gestione di rapporti partecipativi con enti pubblici;
- gestione contratti di tesoreria e servizi di gestione, di incasso e pagamento, contratti bancari e contratti per la prestazione di servizi di investimento, anche per conto di un ente pubblico;
- gestione contratti aventi ad oggetto strumenti finanziari;
- gestione contratti/convenzioni per l'erogazione, l'incasso e la gestione di operazioni di finanza agevolata e/o di contributi/agevolazioni a supporto di finanziamenti agevolati;
- stipula e gestione di convenzioni con enti pubblici per l'offerta rivolta ai dipendenti pubblici di prodotti e servizi bancari, di investimento e assicurativi;
- gestione delle imposte in qualità di sostituto di imposta e di delegato all'incasso e riversamento deleghe;
- gestione degli accordi e dei rapporti con SACE e SIMEST o altre entità di natura pubblica con finalità similari;
- gestione amministrativa delle obbligazioni emesse dagli enti locali e dallo Stato;
- supporto consulenziale propedeutico alla stipula di rapporti contrattuali con la Pubblica Amministrazione;
- pagamento delle pensioni in convenzione;

Ai sensi del D. Lgs n. 231/2001, i relativi processi potrebbero presentare ad esempio occasioni per la commissione dei reati di "corruzione", nelle loro varie tipologie, di "*Induzione indebita a dare o promettere utilità*", di "*Traffico di influenze illecite*", di "Concussione" e di "*Truffa ai danni dello Stato o di altro Ente pubblico*", "*Malversazione di erogazioni pubbliche", "Truffa aggravata per il conseguimento di erogazioni pubbliche" "Indebita percezione di erogazioni pubbliche", "Peculato" "Abuso d'ufficio", "Corruzione tra privati"* (e in concorso con la clientela).

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa, in particolare:
    - la gestione dei rapporti con la clientela in costanza di esecuzione degli obblighi di natura contrattuale è organizzativamente demandata a specifiche strutture/funzioni della Banca che si occupano della erogazione di prodotti / servizi oggetto del contratto. La stipula dei contratti per l'esecuzione di servizi nei confronti della Pubblica Amministrazione è effettuata nel rispetto dei principi di comportamento sanciti nel presente protocollo;
    - tutti gli atti che impegnano contrattualmente la Banca nei confronti di terzi devono essere sottoscritti soltanto da soggetti appositamente incaricati;
    - nell'ambito di ogni struttura/funzione, tutti i soggetti che esercitano poteri autorizzativi e/o negoziali nella gestione dei rapporti contrattuali con la clientela o nei confronti della Pubblica Amministrazione devono essere individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale, dal sistema dei poteri e delle deleghe ovvero dal Responsabile di riferimento tramite delega interna, da conservare a cura della Banca e operano esclusivamente nell'ambito del perimetro/portafoglio di clientela loro assegnato dal Responsabile di riferimento;
    - sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite; le abilitazioni sono concesse tenendo conto dei principi di minimizzazione e del "minimo privilegio" previsti dalla normativa in materia di protezione dei dati personali.
- Segregazione dei compiti tra i soggetti coinvolti nel processo di stipula e gestione dei rapporti contrattuali con la clientela e le controparti, ivi inclusi gli Enti della Pubblica Amministrazione, in particolare:
    - le attività di sviluppo commerciale sono svolte da strutture/funzioni diverse rispetto a quelle che gestiscono operativamente l'erogazione dei prodotti/servizi contrattualizzati;
    - i soggetti deputati alla predisposizione della documentazione per la presentazione dell'offerta tecnica ed economica, ovvero per la partecipazione alla presentazione di offerte a clienti/bandi di gara pubblica sono differenti da coloro che sottoscrivono la stessa;
    - la definizione dell'accordo è esclusivamente affidata al Responsabile della struttura aziendale competente in virtù dell'oggetto del contratto o a soggetti a ciò facoltizzati; l'atto formale della stipula del contratto avviene in base al sistema dei poteri e delle deleghe vigenti;

- relativamente al processo del credito, e tenuto conto delle specifiche differenze connesse alla clientela “Pubblica Amministrazione” e clientela “privata”, esiste una segregazione tra i soggetti incaricati della fase istruttoria rispetto ai soggetti facoltizzati alla delibera del finanziamento;

- Attività di controllo:
  - la documentazione relativa alla stipula dei rapporti contrattuali viene sottoposta per il controllo al Responsabile della struttura aziendale competente in virtù dell’oggetto del contratto o a soggetti a ciò facoltizzati che si avvalgono, per la definizione delle nuove tipologie contrattuali, del contributo consulenziale della competente struttura per quanto concerne gli aspetti di natura legale;
  - la normativa interna di riferimento identifica i controlli di linea che devono essere svolti a cura di ciascuna struttura/funzione interessata nello svolgimento delle attività di natura contabile/amministrativa inerenti all’esecuzione dei processi oggetto del presente protocollo. In particolare dovrà essere assicurata la verifica della regolarità delle operazioni nonché della completezza, della correttezza e della tempestività delle scritture contabili;
  - tutta la documentazione predisposta dalla Banca per rispondere ad inviti a presentare offerte a clienti/potenziali clienti, ovvero ai fini della partecipazione a bandi di gara indetti da clienti/potenziali clienti appartenenti alla Pubblica Amministrazione, deve essere verificata, in termini di veridicità e congruità sostanziale e formale, dal Responsabile della struttura aziendale competente in virtù dell’oggetto del contratto o da soggetti a ciò facoltizzati;

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - ciascuna fase rilevante degli accordi con la clientela, ivi inclusa la Pubblica Amministrazione, deve risultare da apposita documentazione scritta, debitamente firmata da soggetti muniti di idonei poteri in base al sistema di deleghe e poteri vigenti;
  - la realizzazione delle operazioni nella esecuzione degli adempimenti contrattuali prevede l’utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle informazioni elaborate. Le Funzioni provvedono alla archiviazione della documentazione cartacea inerente all’esecuzione degli adempimenti svolti;
  - ciascuna Funzione di volta in volta interessata, al fine di consentire la ricostruzione delle responsabilità, è responsabile dell’archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell’ambito delle attività proprie del processo della gestione dei rapporti con la clientela.

Principi di comportamento

Le Funzioni della Banca, a qualsiasi titolo coinvolte nella gestione dei rapporti con la clientela, ivi inclusa la Pubblica Amministrazione, derivanti da adempimenti di natura contrattuale con gli stessi, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;

- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla alla Funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;

- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/esecuzione dei rapporti contrattuali con la clientela, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;

- non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;

- in occasione di operazioni di Tesoreria verso Enti pubblici, ovvero di incassi effettuati agli sportelli di imposte, tasse e contributi a vario titolo, le operazioni dovranno essere svolte secondo le procedure stabilite internamente nel rispetto di quanto definito dagli accordi commerciali presi.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;

- tenere una condotta ingannevole che possa indurre la clientela in errore in ordine alla scelta di attribuzione di incarichi alla Banca;

- chiedere o indurre – anche a mezzo di intermediari - i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la decisione di stipulare accordi/convenzioni/contratti con la Banca;

- promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - a rappresentanti dei clienti[4] o a soggetti della Pubblica Amministrazione, anche a seguito di induzione da parte degli stessi, con la finalità di promuovere o favorire interessi della Banca. A titolo meramente esemplificativo e non esaustivo, tra i vantaggi che potrebbero essere accordati, si citano la promessa di assunzione per parenti ed affini, la sponsorizzazione

[4] Intendendosi per tali i soggetti che ricoprono specifici incarichi, ruoli o funzioni presso società (persone giuridiche) clienti e potenziali clienti aventi natura privatistica.

o la beneficenza a favore di soggetti collegati, l'erogazione di credito a condizioni non conformi ai principi di sana e prudente gestione previsti dalla normativa aziendale e, più in generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per i soggetti predetti;

- promettere versare/offrire somme di denaro non dovute, doni o gratuite prestazioni, vantaggi di qualsiasi natura, come descritti al punto precedente, a favore di esponenti apicali o di persone a loro subordinate appartenenti a società/enti partecipanti a gare pubbliche al fine di dissuaderli dalla partecipazione o per conoscere le loro offerte e formulare le proprie in modo tale da ottenere l'aggiudicazione della gara, oppure minacciarli di un danno ingiusto per le medesime motivazioni;

- ricevere danaro, doni o qualsiasi altra utilità ovvero accettarne la promessa, da chiunque voglia conseguire indebitamente un trattamento in violazione della normativa o delle disposizioni impartite dalla Banca o, comunque, un trattamento più favorevole di quello dovuto;

- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza.

  In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dalla Policy Anticorruzione ; ciò al fine di prevenire il rischio di commissione di reati di corruzione nelle loro varie tipologie, di "*Induzione indebita a dare o promettere utilità*" e di "*Traffico di influenze illecite*" che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare la gestione del rapporto negoziale con la Banca.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi generali di controllo e di comportamento descritti nel presente protocollo.

7.2.2 Gestione dei rapporti con le Autorità di Vigilanza e di controllo

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione dei rapporti con le Autorità di Vigilanza e di controllo e riguarda qualsiasi tipologia di attività posta in essere in occasione di segnalazioni, adempimenti, comunicazioni, richieste e visite ispettive, previste dalla normativa di riferimento.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti con le Autorità di Vigilanza. Tra le Autorità di Vigilanza con le quali la Banca può trovarsi ad intrattenere rapporti si indicano, a titolo esemplificativo e non esaustivo:

- Banca d'Italia;
- Consob;
- Unità di Informazione Finanziaria (U.I.F.);

- Istituto per la Vigilanza sulle Assicurazioni (IVASS);
- Autorità Garante per la protezione dei dati personali;
- Autorità Garante per la Concorrenza e il Mercato (AGCM);
- Autorità di Supervisione in materia fiscale (Agenzia delle Entrate).

Ai sensi del D. Lgs. n. 231/2001, le attività in oggetto potrebbero potenzialmente presentare ad esempio occasioni per la commissione dei reati di "corruzione", nelle loro varie tipologie, di "*Induzione indebita a dare o promettere utilità*", di "*Traffico di influenze illecite*" e di "*Ostacolo all'esercizio delle funzioni delle Autorità Pubbliche di Vigilanza*" (art. 2638 del codice civile).

I principi di comportamento contenuti nel presente protocollo si applicano, a livello d'indirizzo comportamentale, anche nei confronti delle Autorità di Vigilanza estere.

Principi generali di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa, in particolare:
  - i rapporti con le Autorità di Vigilanza sono intrattenuti dal Responsabile della struttura/funzione aziendale di riferimento o da soggetti dallo stesso appositamente incaricati tramite delega interna, da conservare a cura della Banca;
  - gli atti che impegnano contrattualmente la Banca devono essere sottoscritti soltanto da soggetti incaricati;
  - è individuato un Responsabile della raccolta e dell'elaborazione delle informazioni richieste e trasmesse alle Autorità di Vigilanza, in ottemperanza alle normative di settore;
  - il riscontro ai rilevi delle Autorità è sottoposto, laddove previsto, all'approvazione e/o esame del Consiglio di Amministrazione.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione dei rapporti con le Autorità di Vigilanza, in particolare:
  - con riferimento alla gestione dei rapporti non riconducibili alla ordinaria operatività delle Funzioni della Banca, tutta la corrispondenza inerente a rilievi o eccezioni relative alla sfera dell'operatività aziendale indirizzata alle Autorità di Vigilanza è redatta dalla Funzione competente;
  - con riferimento alle visite ispettive, la Funzione competente avuta notizia dell'ispezione avvisa la funzione Internal Audit e la Funzione Compliance ed i Responsabili delle Aree e Direzioni interessate dalla visita ispettiva che, dopo aver accertato l'oggetto dell'ispezione, individuano le risorse deputate a gestire i rapporti con i Funzionari pubblici durante la loro permanenza presso la Banca. L'Organismo di Vigilanza deve essere tempestivamente informato della visita ispettiva in atto e di eventuali prescrizioni o eccezioni rilevate dall'Autorità.
- Attività di controllo:

- controlli di completezza, correttezza ed accuratezza delle informazioni trasmesse alle Autorità di Vigilanza da parte della Banca per le attività di competenza;
- controlli di carattere giuridico sulla conformità alla normativa di riferimento della segnalazione/comunicazione richiesta;
- controlli automatici di sistema, con riferimento alle segnalazioni periodiche;
- il Responsabile della struttura/funzione di volta in volta interessata assicura la corretta e completa predisposizione dei contenuti delle comunicazioni ed il loro puntuale invio secondo le modalità e i tempi previsti dalla richiesta dell'Autorità;
- il Responsabile della struttura/funzione interessata dall'ispezione o il Responsabile incaricato del coordinamento redige un'apposita nota interna sull'indagine avviata dall'Autorità, con adeguata evidenza di tutte le fasi di raccolta ed elaborazione delle informazioni richieste e trasmesse, degli sviluppi dell'indagine e del suo esito;
- qualora necessario, nell'ambito della gestione di visite ispettive da parte delle Autorità di Vigilanza, la Banca individua il coordinatore dell'ispezione incaricato di assicurare il coordinamento tra i responsabili delle diverse strutture/funzioni aziendali interessate dall'ispezione, ovvero fare da punto di riferimento e coordinare tutte le richieste avanzate.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - è fatto obbligo a tutte le strutture/funzioni della Banca, a vario titolo coinvolte nella predisposizione e trasmissione di comunicazioni ed adempimenti alle Autorità di Vigilanza, di archiviare e conservare la documentazione di competenza prodotta nell'ambito della gestione dei rapporti con le Autorità, ivi inclusa quella trasmessa alle Autorità anche attraverso supporto elettronico.
  - ogni comunicazione nei confronti delle Autorità avente ad oggetto notizie e/o informazioni rilevanti sull'operatività della Banca è documentata/registrata in via informatica ed archiviata presso la Struttura di competenza;
  - fatte salve le situazioni in cui non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, il Responsabile della struttura/funzione interessata che ha presenziato alla visita ispettiva assiste il Funzionario pubblico nella stesura del verbale di accertamento ed eventuale prescrizione, riservandosi le eventuali controdeduzioni, firmando, per presa visione il verbale, comprensivo degli allegati, prodotto dal Funzionario stesso;
  - ad ogni visita ispettiva da parte di Funzionari rappresentanti delle Autorità di Vigilanza il Responsabile della Funzione interessata provvede a trasmettere alle strutture/funzioni competenti copia del verbale rilasciato dal Funzionario pubblico e degli annessi allegati. Qualora non sia previsto l'immediato rilascio di un verbale da parte dell'Autorità di Vigilanza, il Responsabile della struttura/funzione interessata dall'ispezione o un suo delegato provvede alla redazione di una nota di sintesi dell'accertamento effettuato e alla trasmissione della stessa alle strutture/funzioni competenti. La suddetta documentazione è archiviata dal Responsabile della struttura/funzione interessata dall'ispezione.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nel processo di gestione dei rapporti con le Autorità di Vigilanza, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione o induzione da parte di un soggetto dell'Autorità di Vigilanza di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla alla funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- devono essere puntualmente trasmesse le segnalazioni periodiche alle Autorità di Vigilanza e tempestivamente riscontrate le richieste/istanze pervenute dalle stesse Autorità;
- nell'ambito delle ispezioni effettuate da parte dei Funzionari delle Autorità di Vigilanza presso la sede della Banca, fatte salve le situazioni in cui i Funzionari richiedano colloqui diretti con personale della Banca specificamente individuato, partecipano agli incontri con i Funzionari stessi almeno due soggetti; laddove l'ispezione sia seguita da Strutture diverse da quella coinvolta dalla verifica è sufficiente la presenza di una sola persona della Struttura interessata, unitamente ad un'altra persona di una di dette Aree.
- nell'ambito delle ispezioni effettuate da parte dei Funzionari delle Autorità di Vigilanza è richiesta la massima collaborazione da parte di tutte le strutture/funzioni aziendali interessate dall'ispezione.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre le Autorità di Vigilanza in errore;
- chiedere o indurre – anche a mezzo di intermediari - i rappresentanti dell'Autorità di Vigilanza a trattamenti di favore ovvero omettere informazioni dovute al fine ostacolare l'esercizio delle funzioni di Vigilanza;
- promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - a rappresentanti dell'Autorità di Vigilanza con la finalità di promuovere o favorire interessi della Banca. A titolo meramente esemplificativo e non esaustivo, tra i vantaggi che potrebbero essere accordati, si citano la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, l'erogazione di credito a condizioni non conformi ai principi di sana e prudente gestione previsti dalla normativa aziendale e, più in generale, tutte le operazioni bancarie

o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per i soggetti predetti.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.3 Gestione degli interventi agevolativi

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione del processo di erogazione di agevolazioni pubbliche alle imprese e/o privati, (fondi regionali, nazionali e comunitari).

Il processo di gestione degli interventi agevolativi comprende le attività di istruttoria, gestione ed erogazione di tali interventi, che, a titolo esemplificativo e non esaustivo, possono riguardare:

- finanziamenti agevolati e contributi in conto capitale concessi dai Ministeri per agevolazioni a progetti di ricerca e sviluppo;
- finanziamenti garantiti dal Fondo Centrale di Garanzia istituito c/o Medio Credito Centrale S.p.A., ai sensi della L. n. 662/96;
- finanziamenti con contribuiti in conto interessi, finanziamenti con fondi di terzi, finanziamenti ordinari correlati ad erogazione di contributi in conto capitale o in conto interessi e mutui con ammortamento a carico dello Stato o con garanzia dello Stato;
- contributi in conto capitale a valere su strumenti quali quelli ex lege 488/92, di Programmazione Negoziata, strumenti regionali, ecc.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare ad esempio occasioni per la commissione dei reati di "Concussione", di "Corruzione", nelle loro varie tipologie, di "*Induzione indebita a dare o promettere utilità*", di "*Traffico di influenze illecite*"[11], di "*Truffa ai danni dello Stato o di altro Ente pubblico*", di "*Truffa aggravata per il conseguimento di erogazioni pubbliche*", di "*Malversazione*" e di "*Indebita percezione di erogazioni a danno dello Stato*".

Principi generali di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa, in particolare:
  - tutte le approvazioni per gli atti impegnativi e le autorizzazioni alle erogazioni dei fondi devono essere rilasciate da soggetti appositamente incaricati; la normativa interna illustra tali meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri di approvazione.
- Segregazione dei compiti tra i soggetti coinvolti in tutte le fasi del processo, in particolare:
  - nel caso in cui il finanziamento venga deliberato dalla Banca, la responsabilità dell'istruttoria compete ad un soggetto diverso da quello responsabile della delibera stessa, fatte salve le eccezioni espressamente previste dalla normativa interna tempo per tempo vigente.
- Attività di controllo:

- i controlli di linea che devono essere svolti a cura della Funzione competente per i finanziamenti a valere su fondi ministeriali per agevolazioni a progetti di ricerca e sviluppo, riguardano: i) la valutazione e approvazione, da parte dei responsabili degli uffici operativi delle relazioni istruttorie e di quelle di controllo sugli stati d'avanzamento degli investimenti, compreso quello finale; ii) l'utilizzo di sistemi informatici dedicati all'operatività, su cui sono implementati, ove possibile, idonei presidi di controllo automatizzato.
- per quanto riguarda, invece, la gestione delle altre agevolazioni, l'attività di controllo di linea preventiva riguarda in particolare: i) verifica, effettuata da parte degli istruttori degli uffici operativi, delle capacità economico patrimoniali dei soggetti richiedenti, sulla validità tecnica, economica e finanziaria dei progetti e delle modalità di copertura dei piani finanziari oggetto di valutazione; ii) utilizzo di sistemi informatici dedicati all'operatività, su cui sono implementati, ove possibile, attività di controllo automatico; iii) verifica, da parte dell'organo proponente, dei requisiti di ammissibilità, congruità della spesa e sostenibilità del piano finanziario; v) esistenza di verifiche finali sulla correttezza della documentazione allegata alla singola pratica, ad opera dell'ufficio di competenza; vi) accertamenti periodici, eventualmente derivanti da specifici obblighi di controllo e monitoraggio contenuti nel testo di convenzione con gli Enti.

Inoltre ciascuna Funzione interessata nello svolgimento delle attività di natura contabile/amministrativa inerenti all'esecuzione dei processi oggetto del presente protocollo deve assicurare il corretto espletamento dei controlli di linea, la verifica della regolarità delle operazioni nonché la completezza, la correttezza, e la tempestività delle scritture contabili che devono essere costantemente supportate da meccanismi di maker e checker.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo di gestione degli interventi agevolativi.

Principi di comportamento

Le Funzioni della Banca, a qualsiasi titolo coinvolte nella gestione degli interventi agevolativi sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione.

In particolare:

- tutti i soggetti che, in fase di richiesta e gestione di finanziamenti agevolati o contributi, intrattengono rapporti con la Pubblica Amministrazione per conto della Banca nonché coloro che hanno la responsabilità di firmare atti o documenti con rilevanza esterna alla Banca (es. pratiche di istruttoria, richieste fondi, ecc.) devono essere individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma, dal sistema di poteri e deleghe ovvero devono essere espressamente autorizzati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse

essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla alla funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;

- per ragioni di incompatibilità con il ruolo pubblicistico svolto dalla Banca, i finanziamenti agevolati/contributi in conto capitale e/o in conto interessi concessi alle imprese beneficiarie delle agevolazioni non possono essere oggetto di anticipazione ovvero di cessione alla Banca incaricata dell'istruttoria. Pertanto è tassativamente esclusa la possibilità di deliberare affidamenti/anticipazioni assistiti da mandato irrevocabile all'incasso o cessione di contributi spettanti alle imprese per le quali la Banca esegue l'istruttoria;
- i Responsabili delle Funzioni interessate devono garantire, nell'ambito delle attività di propria competenza, il costante aggiornamento e sensibilizzazione del personale sulla normativa esterna di riferimento;
- i rapporti e gli adempimenti nei confronti della Pubblica Amministrazione, ovvero nei confronti di suoi rappresentanti/esponenti, devono essere adempiuti con la massima trasparenza, diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere evitando e comunque segnalando nella forma e nei modi idonei, situazioni di conflitto di interesse;
- qualora sia previsto il coinvolgimento di soggetti terzi nella predisposizione delle pratiche di richiesta/gestione del finanziamento o nella successiva esecuzione di attività connesse con progetti/programmi finanziati, i contratti/lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- accettare e/o esibire consapevolmente documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- chiedere o indurre – anche a mezzo di intermediari - i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la Banca;
- utilizzare contributi, sovvenzioni, finanziamenti pubblici riconosciuti alla clientela per finalità diverse da quelle per le quali sono stati concessi al fine di procurare un vantaggio alla Banca, anche mediante compensazioni di crediti o mancato riconoscimento degli stessi;
- promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a soggetti della Pubblica Amministrazione con la finalità

di promuovere o favorire interessi della Banca. A titolo meramente esemplificativo e non esaustivo, tra i vantaggi che potrebbero essere accordati, si citano la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati l'erogazione di credito a condizioni non conformi ai principi di sana e prudente gestione previsti dalla normativa aziendale e, più in generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per i soggetti predetti.

- accettare omaggi, vantaggi di qualsiasi natura o somme di denaro da imprese, ovvero cedere a raccomandazioni e pressioni da parte delle stesse, al fine di facilitare l'espletamento della pratica e/o garantire il buon esito dell'intervento agevolato richiesto;
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza.

  In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dalla Policy Anticorruzione; ciò al fine di prevenire il rischio di commissione di reati di corruzione nelle loro varie tipologie, di "*induzione indebita a dare o promettere utilità*" e di "*traffico di influenze illecite*" che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare il rapporto con la Banca.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.2.4 Gestione delle attività inerenti la richiesta di concessioni, autorizzazioni, licenze o l'esecuzione di adempimenti verso la Pubblica Amministrazione

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, nella gestione delle attività inerenti alla richiesta di concessioni, autorizzazioni, licenze o l'esecuzione di adempimenti verso la Pubblica Amministrazione quali, a titolo esemplificativo e non esaustivo:

- gestione dei rapporti con Enti pubblici per la richiesta e l'ottenimento di concessioni o autorizzazioni edilizie;
- gestione dei rapporti con gli Enti assistenziali e previdenziali e realizzazione, nei tempi e nei modi previsti, degli adempimenti di legge in materia di lavoro e previdenza (INPS, INAIL, INPDAP, Direzione Provinciale del Lavoro, Medicina del Lavoro, Agenzia delle Entrate, Enti pubblici locali, ecc.);
- gestione dei rapporti con le Camere di Commercio per l'esecuzione delle attività inerenti al registro delle imprese;
- gestione dei rapporti con gli Enti Locali territorialmente competenti in materia di smaltimento rifiuti;
- gestione dei rapporti con Amministrazioni Statali, Regionali, Comunali o Enti locali (A.S.L., Vigili del Fuoco, Arpa, ecc.) per l'esecuzione di adempimenti in materia di igiene e sicurezza e/o di autorizzazioni, permessi, concessioni;

- gestione dei rapporti con il Ministero dell'Economia e delle Finanze, con le Agenzie Fiscali e con gli Enti pubblici locali per l'esecuzione di adempimenti in materia di imposte;
- gestione dei rapporti con Banca d'Italia per l'esecuzione degli adempimenti in materia di mantenimento della riserva obbligatoria;
- gestione dei rapporti con la Prefettura, la Procura della Repubblica e le Camere di Commercio competenti per la richiesta di certificati e autorizzazioni;
- gestione degli accertamenti bancari.

Ai sensi del D. Lgs. n. 231/2001, le predette attività potrebbero presentare ad esempio occasioni per la commissione dei reati di "corruzione", nelle loro varie tipologie, di "*Induzione indebita a dare o promettere utilità", di "Traffico di influenze illecite*" e di "*Truffa ai danni dello Stato o di altro Ente pubblico*".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa, in particolare:
  - tutti i soggetti che esercitano poteri autorizzativi e/o negoziali nella gestione delle attività inerenti alla richiesta di autorizzazioni alla Pubblica Amministrazione sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale, dal sistema di deleghe e poteri ovvero dal Responsabile di riferimento tramite delega interna, da conservare a cura della Banca e operano esclusivamente nell'ambito del perimetro/portafoglio di clientela loro assegnato dal Responsabile di riferimento;
  - nel caso in cui i rapporti con gli Enti pubblici vengano intrattenuti da soggetti terzi, questi ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali;
  - la gestione dei rapporti con i Funzionari pubblici in caso di accertamenti/sopralluoghi, effettuati anche allo scopo di verificare l'ottemperanza alle disposizioni di legge che regolamentano l'operatività dell'area di propria competenza, è attribuita al Responsabile della struttura/funzione e/o ai soggetti da quest'ultimo appositamente individuati.
- Segregazione dei compiti tra i soggetti coinvolti nel processo di gestione delle attività inerenti alla richiesta di concessioni, autorizzazioni, licenze o all'esecuzione di adempimenti verso la Pubblica Amministrazione;
  - agli incontri formali o informali con enti della Pubblica Amministrazione ovvero con rappresentanti/esponenti degli stessi, ove possibile, presenziano almeno due soggetti.
- Attività di controllo:
  - le attività per la predisposizione dei dati e delle informazioni a supporto dell'istanza di autorizzazione o forniti in esecuzione degli adempimenti previsti ai sensi di legge devono essere svolte in modo tale da garantire la veridicità, la completezza, la

congruità e la tempestività nella predisposizione, prevedendo, ove opportuno, specifici controlli in contraddittorio.

- laddove l'autorizzazione/adempimento preveda l'elaborazione di dati ai fini della predisposizione dei documenti richiesti dall'Ente pubblico, è effettuato un controllo sulla correttezza delle elaborazioni da parte di soggetti diversi da quelli deputati alla esecuzione delle attività per la richiesta di autorizzazioni e/o permessi, ovvero in merito all'esecuzione di adempimenti previsti rispetto alle disposizioni normative vigenti.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - copia della documentazione consegnata all'Ente pubblico per la richiesta di autorizzazione o per l'esecuzione di adempimenti è conservata e archiviata a cura delle strutture/funzioni competenti della Banca;
  - in occasione di contatti con pubblici funzionari connessi a fasi rilevanti dell'attività, è prevista la comunicazione formale al Responsabile di riferimento dell'avvenuto contatto (ad esempio, a mezzo email), in cui emergano con chiarezza l'oggetto del contatto e le informazioni ivi scambiate; tali comunicazioni sono conservate a cura del soggetto interessato, insieme a eventuale relativa documentazione;
  - il Responsabile della struttura/funzione, ovvero il soggetto aziendale all'uopo incaricato ha l'obbligo di firmare per accettazione il verbale redatto dai Funzionari pubblici in occasione degli accertamenti/sopralluoghi condotti presso la Banca e di mantenerne copia nei propri uffici, unitamente ai relativi allegati;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività relative alla richiesta di autorizzazioni alla Pubblica Amministrazione.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione dei rapporti con la Pubblica Amministrazione in occasione di richiesta di concessioni, autorizzazioni, licenze o esecuzione di adempimenti, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione.

In particolare:

- i soggetti coinvolti nel processo che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Banca devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla alla funzione di Internal Audit ed al per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;

- qualora sia previsto il coinvolgimento di soggetti terzi (professionisti, ditte, ecc.) nell'espletamento delle attività inerenti alla richiesta di autorizzazioni ovvero nell'esecuzione di adempimenti verso la Pubblica Amministrazione, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore;
- chiedere o indurre – anche a mezzo di intermediari - i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente il riscontro da parte della Pubblica Amministrazione;
- promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - a soggetti della Pubblica Amministrazione con la finalità di promuovere o favorire interessi della Banca. A titolo meramente esemplificativo e non esaustivo, tra i vantaggi che potrebbero essere accordati, si citano la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, l'erogazione di credito a condizioni non conformi ai principi di sana e prudente gestione previsti dalla normativa aziendale e, più in generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per i soggetti predetti.
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dalla Policy Anticorruzione; ciò al fine di prevenire il rischio di commissione ad esempio di reati di corruzione, nelle loro varie tipologie, di "*Induzione indebita a dare o promettere utilità*" e di "*Traffico di influenze illecite*" che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare la gestione del rapporto con la Banca.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

7.2.5 Gestione dei contenziosi (in via stragiudiziale e in via giudiziale) e degli accordi transattivi

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, nella gestione delle attività inerenti i contenziosi giudiziali e stragiudiziali (amministrativo, civile, penale, fiscale, giuslavoristico e previdenziale) e degli accordi transattivi con enti pubblici o con soggetti privati.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare ad esempio occasioni per la commissione dei reati di "*Corruzione*", nelle loro varie tipologie (ivi compresa la "corruzione in atti giudiziari"), di "*Induzione indebita a dare o promettere utilità*", di "*Traffico di influenze illecite"*, e di "*Truffa ai danni dello Stato o di altro Ente pubblico*" nonché del reato di "*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*". Potrebbe sussistere altresì il rischio della commissione dei reati di "*Corruzione tra privati*" e di "*Istigazione alla corruzione tra privati*".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa:
    - la gestione dei contenziosi, stragiudiziali e giudiziali, e degli accordi transattivi, inclusi quelli con gli Enti appartenenti alla Pubblica Amministrazione prevede l'accentramento delle responsabilità di indirizzo, gestione e monitoraggio delle singole fasi del processo in capo a diverse strutture/funzioni della Banca, a seconda che si tratti di profili giuridici di natura amministrativa, civile, penale, fiscale, giuslavoristica e previdenziale.
    - il funzionigramma ovvero il sistema dei poteri e delle deleghe stabilisce la chiara attribuzione dei poteri relativi alla definizione delle transazioni, nonché le facoltà di autonomia per la gestione del contenzioso ivi incluso quello nei confronti della Pubblica Amministrazione; la normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
    - il conferimento degli incarichi a legali esterni diversi da quelli individuati nell'ambito dell'albo predisposto e approvato dalla struttura/funzione competente è autorizzato dal Responsabile di funzione competente.
- Segregazione dei compiti:
    - attraverso il chiaro e formalizzato conferimento di compiti e responsabilità nell'esercizio delle facoltà assegnate nello svolgimento delle attività di cui alla gestione dei contenziosi e degli accordi transattivi, ivi inclusi quelli con la Pubblica Amministrazione. In particolare, le procedure aziendali prevedono adeguati livelli quantitativi oltre ai quali le singole transazioni devono essere autorizzate da funzioni diverse da quelle di business che hanno gestito la relazione.

- Attività di controllo:
    - rilevazione e monitoraggio periodico delle vertenze pendenti;
    - verifica periodica della regolarità, della completezza e correttezza di tutti gli adempimenti connessi a vertenze / transazioni che devono essere supportati da meccanismi di maker e checker.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
    - ciascuna fase rilevante del processo deve risultare da apposita documentazione scritta (verbalizzazione degli incontri intercorsi con l'Autorità giudicante e con la controparte per la definizione degli accordi transattivi);
    - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la struttura/funzione di volta in volta interessata è altresì responsabile dell'archiviazione e della conservazione della documentazione di competenza anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo di gestione dei contenziosi (in via stragiudiziale e giudiziale) e degli accordi transattivi ivi inclusi quelli con la Pubblica Amministrazione (archiviazione documento di chiusura delle trattive).

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione dei contenziosi (in via stragiudiziale e in via giudiziale) e degli accordi transattivi ivi inclusi quelli con la Pubblica Amministrazione sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione.

Si richiama anche la "Politica per la gestione dei reclami" che definisce le modalità di gestione dei reclami pervenuti dalla clientela e dei procedimenti presso gli organismi di risoluzione alternativa delle controversie.

In particolare:

- i soggetti coinvolti nel processo e che hanno la responsabilità di firmare atti o documenti con rilevanza esterna alla Banca devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione/induzione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla alla funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del contenzioso e degli accordi transattivi, i contratti / lettere di incarico con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- non è consentito riconoscere compensi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere e/o nel valore della controversia rapportato alle tariffe professionali applicabili;

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo è vietato, al fine di favorire indebitamente interessi della Banca, ed anche a mezzo di professionisti esterni o soggetti terzi:

- in sede di contatti formali od informali, o nel corso di tutte le fasi del procedimento, adottare comportamenti non conformi alle prescrizioni della presente Parte Speciale e al Codice Etico, per:
  - avanzare indebite richieste o esercitare pressioni su Giudici o Membri di Collegi Arbitrali (compresi gli ausiliari e i periti d'ufficio);
  - indurre chiunque al superamento di vincoli o criticità ai fini della tutela degli interessi della Banca;
  - indurre - con violenza o minaccia o, alternativamente, con offerta o promessa di denaro o di altra utilità - a tacere o a mentire la persona chiamata a rendere davanti all'Autorità Giudiziaria dichiarazioni utilizzabili in un procedimento penale;
  - influenzare indebitamente le decisioni dell'Organo giudicante o le posizioni della Pubblica Amministrazione, quando questa sia controparte del contenzioso/arbitrato;
- in occasione di ispezioni/controlli/verifiche influenzare il giudizio, il parere, il rapporto o il referto degli Organismi pubblici o nominati dall'Organo giudicante o della Polizia giudiziaria;
- chiedere o indurre – anche a mezzo di intermediari - i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la gestione del rapporto con la Banca;
- promettere versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore), o accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di soggetti della Pubblica Amministrazione, di esponenti apicali o persone a loro subordinate appartenenti a società controparti o in relazione con la Banca, al fine di favorire indebitamente gli interessi della Banca, oppure minacciarli di un danno ingiusto per le medesime motivazioni. A titolo meramente esemplificativo e non esaustivo, tra i vantaggi che potrebbero essere accordati si citano la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, l'erogazione di credito a condizioni non conformi ai principi di sana e prudente gestione previsti dalla normativa aziendale e, più in generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per i soggetti predetti;
- affidare incarichi a professionisti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del professionista devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dalla Policy Anticorruzione; ciò al fine di prevenire il rischio di commissione ad esempio del reato di corruzione nelle loro varie tipologie, di "*induzione indebita a dare o promettere utilità*" e

di "*Traffico di influenze illecite*" che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare il rapporto con la Banca.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.6 Gestione del processo di selezione, assunzione, amministrazione del personale

Il presente protocollo si applica a i Destinatari del Modello coinvolti, a qualsiasi titolo, nell'attività inerente la gestione del processo di selezione, assunzione e amministrazione del personale.

Ai sensi del D.Lgs.231/2001, le attività in oggetto potrebbero costituire una delle modalità strumentali attraverso cui commettere ad esempio i reati di "*Corruzione"*, nelle loro varie tipologie, di "*Induzione indebita a dare o promettere utilità*", di "*Traffico di influenze illecite*", nonché dei reati di "*Corruzione tra privati*" e di "*Istigazione alla corruzione tra privati*".

Una gestione non trasparente del processo di selezione, assunzione e amministrazione del personale, potrebbe, infatti, consentire la commissione di tali reati attraverso la promessa di assunzione verso rappresentanti della Pubblica Amministrazione, e/o esponenti apicali, e/o persone loro subordinate di società o enti controparti o in relazione con la Banca, o soggetti da questi indicati, concessa al fine di influenzarne l'indipendenza di giudizio o di assicurare un qualsivoglia vantaggio per la Banca. Potrebbe sussistere altresì il rischio della commissione del reato di "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Carifermo si è dotata di una policy che regolamenta l'attività medesima "Gestione del Personale" e "Politica del personale" - Allegato. Tali documenti si pongono a presidio dei reati della presente Parte Speciale.

Principi generali di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa:
    - la selezione avviene mediante specifici colloqui valutativi a cura di un Responsabile apicale selezionato dal Direttore Generale e da un membro del Comitato Esecutivo, che esprimono un proprio giudizio consultivo al Direttore Generale, che esprimerà il giudizio finale;
    - l'assunzione dei candidati individuati come idonei e per i quali è stata fornita autorizzazione all'inserimento viene effettuata dagli Organi Sociali competenti.
- Segregazione dei compiti tra i diversi soggetti coinvolti nel processo.
    - presenza di una segregazione dei compiti tra i diversi soggetti coinvolti nel processo in oggetto, in particolare tra la struttura/funzione responsabile della selezione e la struttura/funzione a cui è demandata l'approvazione finale dell'assunzione.

- l'approvazione finale dell'assunzione è demandata all'OFG per i rapporti a tempo determinato e all'Organo con Funzione di Supervisione Strategica in tutti gli altri casi.

- Attività di controllo:
  - compilazione da parte del candidato, al momento dello svolgimento della selezione, di un'apposita modulistica (compresa un'autocertificazione) per garantire la raccolta omogenea delle informazioni sui candidati;
  - previsione di attività di controllo da parte della competente struttura/funzione volte a riscontrare la presenza di tutte le informazioni necessarie e di tutti i documenti necessari all'instaurazione del rapporto di lavoro.
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - ogni esigenza di assunzione nasce da necessità legate a dinamiche organici (es. sostituzioni per assenze di lunga durata, cessazione del rapporto di lavoro, job rotation orizzontali o verticali) e deve essere formalizzata al fine di procedere allo svolgimento delle attività propedeutiche alla selezione dei candidati;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, l'Ufficio Risorse Umane è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo di selezione e assunzione del personale.

Principi di comportamento

Le Funzioni della Banca, a qualsiasi titolo coinvolte nella gestione del processo di selezione e assunzione del personale, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna (Policy "Gestione del Personale") nonché eventualmente le eventuali previsioni del Codice Etico e della Policy Anticorruzione.

In particolare:

- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente a conoscenza e deve immediatamente segnalarla alla Funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- la selezione deve essere effettuata tra una rosa di candidati, salvo il caso di personale specialistico qualificato, di categorie protette ovvero di figure destinate a posizioni manageriali;
- la valutazione comparativa dei candidati deve essere effettuata sulla base di criteri di competenza, professionalità ed esperienza in relazione al ruolo per il quale avviene l'assunzione;
- qualora il processo di assunzione riguardi:
  - personale diversamente abile, il reclutamento dei candidati avverrà nell'ambito delle liste di soggetti appartenenti alle categorie protette, da richiedere al competente Ufficio del Lavoro;
  - lavoratori stranieri, il processo dovrà garantire il rispetto delle leggi sull'immigrazione del Paese ove è sita l'unità organizzativa di destinazione e la verifica del possesso, per tutta la durata del rapporto di lavoro, dei permessi di soggiorno, ove prescritti;

- ex dipendenti pubblici, il processo dovrà garantire il rispetto dei divieti di legge.

- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo di selezione e assunzione del personale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- promettere o dare seguito – anche a mezzo di intermediari - a richieste di assunzione in favore di rappresentanti/esponenti della Pubblica Amministrazione ovvero di soggetti da questi indicati, al fine di influenzare l'indipendenza di giudizio o indurre ad assicurare qualsiasi vantaggio alla Banca;
- promettere o dare seguito a richieste di assunzioni di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la Banca ovvero di soggetti da questi indicati, al fine di favorire indebitamente il perseguimento di interessi della Banca.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.7 Gestione della formazione finanziata

Il presente protocollo si applica a tutti i Destinatari della Banca coinvolti, a qualsiasi titolo, nell'attività inerente la gestione della formazione finanziata.

Attraverso la gestione della formazione finanziata la Banca, laddove sussistano i presupposti, ricorre ai finanziamenti, sovvenzioni e contributi per la formazione concessi da soggetti pubblici nazionali ed esteri.

Ai sensi del D. Lgs. n. 231/2001, le attività in oggetto potrebbero presentare ad esempio occasioni per la commissione dei reati di "*Corruzione*" nelle loro varie tipologie, di "*Induzione indebita a dare o promettere utilità*", di "*Traffico di influenze illecite*", di "*Truffa aggravata per il conseguimento di erogazioni pubbliche*", di "*Malversazione*" e di "*Indebita percezione di erogazioni a danno dello Stato*".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa, in particolare:
  - tutti i soggetti che, nell'ambito della "gestione della formazione finanziata", esercitano poteri autorizzativi e/o negoziali nei rapporti con gli Enti finanziatori sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale,

dal sistema di deleghe e poteri o dal Responsabile di riferimento tramite delega interna, da conservare a cura della Banca e operano esclusivamente nell'ambito del perimetro loro assegnato dal Responsabile di riferimento;

- le richieste di finanziamento/contributo per l'erogazione di formazione al Personale della Banca sono sottoscritte dal Responsabile della struttura/funzione competente specificamente e formalmente facoltizzato in virtù del vigente sistema dei poteri e delle deleghe; la normativa interna illustra tali meccanismi autorizzativi, fornendo le indicazioni dei soggetti aziendali cui sono attribuiti i necessari poteri.
- in caso di eventuale ricorso a consulenti esterni, il processo di attribuzione dell'incarico avviene uniformemente a quanto previsto dalle disposizioni contenute nella specifica sezione dedicata nel presente Modello (protocollo per "la gestione degli acquisti di beni e servizi, degli incarichi professionali e dei consulenti"). La selezione di tali consulenti avviene in ogni caso prevedendo l'acquisizione di una pluralità di offerte e la scelta mediante criteri oggettivi e codificati.

- Segregazione dei compiti tra i soggetti coinvolti, volta a garantire, per tutte le fasi del processo, un meccanismo di maker e checker, in particolare:
  - la struttura/funzione competente attribuisce a ciascun ufficio organizzativamente dipendente, in funzione dei ruoli ricoperti da ciascun addetto, le attività operative e le attività di controllo da effettuare al fine di garantire la contrapposizione di ruoli tra i soggetti che gestiscono le fasi istruttorie del processo della formazione finanziata ed i soggetti deputati alle attività di verifica.
- Attività di controllo da parte di ciascuna Funzione competente connesse alla predisposizione della richiesta e all'ottenimento dell'erogazione di contributi e/o finanziamenti pubblici per la formazione, in particolare:
  - verifica della coerenza dei contenuti del progetto di formazione rispetto a quanto disposto dalle direttive del bando di finanziamento;
  - verifica della regolarità formale della documentazione da consegnare all'Ente per l'accesso al bando di finanziamento;
  - tenuta del registro presenze durante l'erogazione dei progetti formativi e utilizzo di sistemi informatici di supporto per la gestione del personale, in cui sono registrate tutte le informazioni relative alle presenze ed alle attività svolte;
  - puntuale attività di controllo sul processo di rendicontazione delle spese, attraverso:
    - raccolta e verifica dei registri di presenza compilati in ogni loro parte dai partecipanti agli interventi formativi;
    - raccolta della documentazione degli oneri aziendali dei dipendenti partecipanti / docenti, sulla base del corrispettivo orario calcolato a cura dell'ufficio competente in considerazione delle matricole che hanno partecipato all'iniziativa;
    - raccolta e verifica delle parcelle/fatture relative ai costi sostenuti per l'iniziativa;
    - verifica sulla puntuale e corretta contabilizzazione degli introiti.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - tutte le fasi di processo sono documentate, a livello di sistema informativo e/o in termini documentali, così come previsto dagli stessi bandi per l'ottenimento dei finanziamenti. In particolare, ciascuna Funzione coinvolta nell'ambito del processo della formazione finanziata, è responsabile dell'archiviazione e della conservazione della documentazione di propria competenza, ivi inclusa quella trasmessa all'Ente finanziatore pubblico anche in via telematica o elettronica.

Principi di comportamento

Le Funzione della Banca, a qualsiasi titolo coinvolte nella attività di gestione della formazione finanziata, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione.

In particolare:

- tutti i soggetti che, in fase di richiesta e gestione dei finanziamenti agevolati o contributi, intrattengono rapporti con la Pubblica Amministrazione per conto della Banca devono essere espressamente autorizzati;
- i soggetti coinvolti nel processo e che hanno la responsabilità di firmare atti o documenti con rilevanza all'esterno della Banca (es.: pratiche di richiesta, studi di fattibilità, piani di progetto, ecc.) devono essere appositamente incaricati;
- il personale non può dare seguito a qualunque richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla alla funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- qualora sia previsto il coinvolgimento di soggetti terzi nella predisposizione delle pratiche di richiesta / gestione del finanziamento o nella successiva esecuzione di attività connesse con i programmi finanziati, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi e alterati;
- tenere una condotta ingannevole che possa indurre gli Enti finanziatori/erogatori in errore di valutazione tecnico-economica della documentazione presentata;
- chiedere o indurre – anche a mezzo di intermediari - i soggetti della Pubblica Amministrazione a trattamenti di favore ovvero omettere informazioni dovute al fine di influenzare impropriamente la decisione di accoglimento delle domande di ammissione al contributo;

- destinare contributi, sovvenzioni, finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti;
- promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - a soggetti della Pubblica Amministrazione con la finalità di promuovere o favorire interessi della Banca nell'ottenimento di contributi. A titolo meramente esemplificativo e non esaustivo, tra i vantaggi che potrebbero essere accordati, si citano la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, l'erogazione di credito a condizioni non conformi ai principi di sana e prudente gestione previsti dalla normativa aziendale e tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per i soggetti predetti;
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità, e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dalla Policy Anticorruzione; ciò al fine di prevenire ad esempio il rischio di commissione di reati di corruzione nelle loro varie tipologie, di "induzione indebita a dare o promettere utilità" e di "*Traffico di influenze illecite*" che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone legate alla Pubblica Amministrazione e dalla conseguente possibilità di facilitare/velocizzare l'iter istruttorio delle pratiche.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

I principi di comportamento illustrati nel presente protocollo devono intendersi altresì estesi, per quanto compatibili, ad ogni eventuale ulteriore processo aziendale concernente la richiesta e la gestione di contributi/incentivi pubblici a favore della Banca concessi a qualsiasi altro titolo.

7.2.8 Gestione degli acquisti di beni e dei servizi, degli incarichi professionali e delle consulenze

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, nell'attività inerente la gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze.

Tra i beni vanno considerate anche le opere dell'ingegno di carattere creativo, mentre tra le prestazioni vanno ricomprese anche quelle a contenuto intellettuale di qualsiasi natura (es. legale, fiscale, tecnica, giuslavoristica, amministrativa, organizzativa, incarichi di mediazione, d'agenzia o di intermediazioni varie, ecc.), ivi incluso il conferimento di incarichi professionali ovvero di consulenze.

Ai sensi del D. Lgs. n. 231/2001, le attività in oggetto potrebbero costituire ad esempio una delle modalità strumentali attraverso cui commettere i reati di "*Corruzione*" nelle loro varie tipologie, e di "*Induzione indebita a dare o promettere utilità*", di "*Traffico di influenze illecite"*. Potrebbe sussistere altresì il rischio della commissione dei reati di "corruzione tra privati" e di "istigazione alla corruzione tra privati".

Si intende inoltre prevenire il rischio di acquisire beni o servizi di provenienza illecita, ed in particolare il coinvolgimento in altri reati al cui rischio potrebbe essere esposta l'attività della controparte.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Carifermo si è dotata di una policy che regolamenta l'attività medesima "Policy Fornitori".

Principi generali di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

Livelli autorizzativi definiti:

- i poteri di spesa relativi alla stipula di contratti di acquisto di beni e servizi, incarichi professionali e consulenze, sono attribuiti in funzione della natura della spesa e dei limiti di importo definiti nell'ambito del budget assegnato;
- l'approvazione della richiesta di acquisto, l'emissione dell'ordine, il conferimento di incarico e il perfezionamento del contratto spettano esclusivamente a soggetti muniti di idonei poteri in base al sistema di poteri, deleghe e procure in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno.
- la selezione dei fornitori di beni e servizi, dei professionisti e dei consulenti avviene sulla base di criteri e parametri definiti dalla Banca individuati nell'ambito della normativa interna ("Policy Fornitori"), fatte salve esigenze/forniture occasionali; in particolare è condizione di ammissione all'elenco dei fornitori che questi siano muniti di un Codice Etico e che si impegnino a rispettare le prescrizioni previste dal Codice Etico della Banca e del presente Modello. Tali soggetti devono garantire e su richiesta poter documentare, anche con riferimento ai subappaltatori da loro incaricati:
  - in relazione all'utilizzo di marchi o segni distintivi e alla commercializzazione di beni o servizi - il rispetto della disciplina in tema di protezione dei titoli di proprietà industriale e del diritto d'autore e, comunque, la legittima provenienza dei beni forniti;
  - in relazione ai lavoratori impiegati, il rispetto della disciplina in tema di immigrazione e la regolarità retributiva, contributiva, previdenziale, assicurativa e fiscale;
- la scelta dei fornitori di beni e servizi e/o professionisti, consulenti non presenti nelle liste di fornitori di beni e servizi e/o professionisti e consulenti accreditati è effettuata sulla base di un iter approvativo da parte delle competenti strutture/funzioni aziendali ed effettuata secondo criteri basati su parametri oggettivi e trasparenti;
  - l'eventuale affidamento a terzi - da parte dei fornitori della Banca - di attività in sub-appalto, è contrattualmente subordinato ad un preventivo assenso da parte della struttura della Banca che ha stipulato il contratto;
  - l'autorizzazione al pagamento della fattura spetta alla struttura/funzione competente per la quale è prevista l'assegnazione di un budget e delle relative facoltà di spesa o ai soggetti all'uopo incaricati a seguito del controllo di congruenza della prestazione/fornitura;
  - il pagamento delle fatture è effettuato da una specifica struttura/funzione aziendale dedicata.

- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo di gestione delle procedure acquisitive, in particolare:
  - le attività di cui alle diverse fasi del processo devono essere svolte da soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.
- Attività di controllo:

la normativa interna di riferimento identifica i controlli che devono essere svolti a cura di ciascuna Funzione interessata in ogni singola fase del processo:

- verifica dei limiti di spesa e della pertinenza della stessa;
- verifica della regolarità, completezza, correttezza e tempestività delle scritture contabili;
- verifica del rispetto dei criteri individuati dalla normativa aziendale per la scelta dei fornitori e dei professionisti/consulenti;
- verifica delle clausole contrattuali contenute nei nuovi contratti stipulati per l'acquisto di beni/servizi da parte della struttura/funzione competente, laddove diversi dagli standard definiti;
- verifiche periodiche in merito alla qualità dell'operato degli outsourcer e controllo sui costi derivati dall'attività svolta;
- valutazione propedeutiche all'accreditamento di fornitori di beni e servizi e dei professionisti terzi da parte delle strutture/funzioni competenti;
- l'inserimento o la modifica a sistema dell'anagrafica dei fornitori deve essere supportato da apposita documentazione giustificativa;
- verifica periodica da parte delle competenti strutture/funzioni sulla gestione dei contratti con i fornitori e sulla corretta esecuzione dei processi di acquisto in modo da testarne e verificarne l'effettività, l'applicabilità e l'utilizzo corrente;
- verifica del rispetto delle norme di legge che vietano o subordinano a determinate condizioni il conferimento di incarichi di qualunque tipologia a dipendenti pubblici o ex dipendenti pubblici.

Per quanto concerne infine il conferimento di incarichi professionali e consulenze il cui svolgimento comporta un rapporto diretto con la Pubblica Amministrazione (quali ad esempio spese legali per contenzioso, onorari a professionisti per pratiche edilizie, spese per consulenze propedeutiche all'acquisizione di contributi pubblici, ecc.) i Responsabili delle Funzioni devono disporre che venga regolarmente tenuto in evidenza l'elenco dei professionisti/consulenti, l'oggetto dell'incarico ed il relativo corrispettivo;

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;
  - documentabilità di ogni attività del processo con particolare riferimento alla fase di individuazione del fornitore di beni e/o servizi, o professionista/consulente, anche attraverso gare, in termini di motivazione della scelta nonché pertinenza e congruità della spesa. La normativa interna individua in quali casi l'individuazione del fornitore di beni

e/o servizi o professionista deve avvenire attraverso una gara o comunque tramite l'acquisizione di più offerte;

- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione delle procedure acquisitive di beni e servizi.

Principi di comportamento

Le Funzioni della Banca, a qualsiasi titolo coinvolte nel processo di gestione degli acquisti di beni e servizi e degli incarichi professionali, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione.

In particolare:

- la documentazione contrattuale che regola il conferimento di incarichi di fornitura/incarichi professionali deve contenere un'apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto;
- i pagamenti devono essere effettuati esclusivamente su un conto corrente intestato al fornitore/ consulente titolare della relazione;
- non è consentito effettuare pagamenti in contanti, né pagamenti in un Paese diverso da quello in cui è insediata la controparte o a un soggetto diverso dalla stessa.

In ogni caso è fatto divieto di porre in essere, collaborare, dare causa alla realizzazione di comportamenti che possano risultare strumentali alla commissione di fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- assegnare incarichi di fornitura ed incarichi professionali in assenza di autorizzazioni alla spesa e dei necessari requisiti di professionalità, qualità e convenienza del bene o servizio fornito;
- procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto;
- procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali;
- procedere all'autorizzazione del pagamento di parcelle in assenza di un'attenta valutazione del corrispettivo in relazione alla qualità del servizio ricevuto;
- effettuare pagamenti in favore di fornitori della Banca che non trovino adeguata giustificazione nel contesto del rapporto contrattuale in essere con gli stessi;
- minacciare i fornitori di ritorsioni qualora effettuino prestazioni a favore o utilizzino i servizi di concorrenti della Banca.

- promettere versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi dei regali di cortesia di modico valore), e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparti o in relazione con la Banca, al fine di favorire indebitamente gli interessi della Banca, oppure minacciarli di un danno ingiusto per le medesime motivazioni. A titolo meramente esemplificativo e non esaustivo, tra i vantaggi che potrebbero essere accordati si citano la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, l'erogazione del credito a condizioni non conformi ai principi di sana e prudente gestione previsti dalla normativa aziendale e, più in generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per i soggetti predetti.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi generali di controllo e comportamento descritti nel presente protocollo.

7.2.9 Gestione di omaggi, liberalità, spese di rappresentanza, beneficenze e sponsorizzazioni

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, nell'attività inerente la gestione di omaggi, liberalità, spese di rappresentanza, beneficenze e sponsorizzazioni.

Si precisa che, ai fini del presente protocollo, valgono le seguenti definizioni:

- per omaggi/liberalità si intendono le elargizioni di beni di modico valore offerte, nell'ambito delle ordinarie relazioni di affari, al fine di promuovere l'immagine della Banca;
- per spese di rappresentanza si intendono le spese sostenute dalla Banca nell'espletamento delle relazioni commerciali, destinate a promuovere e migliorare l'immagine della Banca (ad es.: spese per colazioni e rinfreschi, spese per forme di accoglienza ed ospitalità, ecc.);
- per iniziative di beneficenza si intendono le elargizioni in denaro che la Banca destina esclusivamente ad Enti senza fini di lucro;
- per sponsorizzazioni si intendono la promozione, la valorizzazione ed il potenziamento dell'immagine della Banca attraverso la stipula di contratti atipici (in forma libera, di natura patrimoniale, a prestazioni corrispettive) con Enti esterni (ad es.: società o gruppi sportivi che svolgono attività anche dilettantistica, Enti senza fini di lucro, Enti territoriali ed organismi locali, ecc.).

Ai sensi del D. Lgs. n. 231/2001, i relativi processi potrebbero costituire una delle modalità strumentali attraverso cui commettere ad esempio i reati di "*Corruzione*", nelle loro varie tipologie, e di "*Induzione indebita a dare o promettere utilità*", e di "*Traffico di influenze illecite*". Potrebbe sussistere altresì il rischio della commissione dei reati di "*Corruzione tra privati*" e di "*Istigazione alla corruzione tra privati*".

Una gestione non trasparente dei processi relativi a omaggi, liberalità, spese di rappresentanza, beneficenze e sponsorizzazioni potrebbe, infatti, consentire la commissione di tali reati, ad esempio attraverso il riconoscimento/concessione di vantaggi ad esponenti della Pubblica Amministrazione e/o ad esponenti apicali, e/o a persone loro subordinate, di società o enti controparti o in relazione

con la Banca, al fine di favorire interessi della Banca ovvero la creazione di disponibilità utilizzabili per la realizzazione dei reati in questione.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

La Banca ha definito una "Policy Anticorruzione" che definisce obblighi e controlli atti a prevenire i reati della specie.

Principi generali di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti:
    - per quanto attiene ai beni destinati ad omaggi, liberalità e alle spese di rappresentanza, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere che stabilisce le facoltà di autonomia gestionale per natura di spesa e impegno. La normativa interna illustra i predetti meccanismi autorizzativi, fornendo l'indicazione dei soggetti aziendali cui sono attribuiti i necessari poteri;
    - tutte le erogazioni di fondi devono essere approvate dai soggetti facoltizzati in base al vigente sistema dei poteri e delle deleghe;
    - gli omaggi o le altre utilità di valore superiore al limite previsto dalla Policy Anticorruzione possono essere ammissibili in via eccezionale, in considerazione del profilo del donante o del beneficiario, e comunque nei limiti della ragionevolezza, previa autorizzazione del Responsabile competente. I limiti di importo previsti, su base annua per gli omaggi e altre utilità, non si applicano alle spese di rappresentanza relative a colazioni, rinfreschi, eventi e forme di accoglienza e ospitalità che vedano la partecipazione di esponenti aziendali e personale della Banca, purché strettamente inerenti al rapporto di affari e ragionevoli rispetto alle prassi di cortesia commerciale e/o istituzionale comunemente accettate;
    - sono definiti diversi profili di utenza per l'accesso a procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite.
- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi, in particolare:
    - le attività di cui alle diverse fasi dei processi devono essere svolte da attori/soggetti differenti (tra chi propone il contratto/progetto, chi ne verifica gli aspetti normativi, etici e fiscali, chi lo sottoscrive e chi controlla l'effettività della prestazione) chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.
- Attività di controllo:
    - Per beneficienze e sponsorizzazioni: La normativa interna definisce le modalità con le quali le erogazioni relative a beneficenze e sponsorizzazioni devono essere precedute da un'attività di verifica da parte delle competenti strutture/funzioni al fine di riscontrare i requisiti alla base dell'erogazione (affinché vi sia una regolarità formale e sostanziale dell'erogazione), con particolare riguardo a quanto stabilito dalla Policy Anticorruzione, in particolare è prevista:

- l'analisi e la verifica del tipo di organizzazione e della finalità per la quale è costituita;
- la verifica ed approvazione di tutte le erogazioni da parte del Responsabile della Funzione interessata;
- la verifica che le erogazioni complessive siano stabilite annualmente e trovino capienza in apposito budget deliberato dagli Organi competenti;
- per le sponsorizzazioni: verifica del corretto adempimento della controprestazione (qualora prevista) a fronte della sponsorizzazione erogata, attraverso l'acquisizione di documentazione comprovante l'avvenuta esecuzione della stessa.

- Per omaggi, liberalità e spese di rappresentanza:
  - controlli volti ad accertare il rispetto dei limiti di budget;
  - tutte le fasi operative devono essere dotate della massima evidenza documentale;
  - è prevista un'apposita evidenza qualora la liberalità venga effettuata a favore di un soggetto/ente pubblico o comunque fornito di rilievo pubblicistico;
  - sono individuati limiti quantitativi, rapportati al loro valore, agli omaggi e alle spese di rappresentanza destinati ad esponenti della clientela (pubblica e privata).

Inoltre i Responsabili delle Funzioni interessate dovranno:

- disporre che venga regolarmente tenuto in evidenza l'elenco dei beneficiari, l'importo delle erogazioni ovvero gli omaggi/liberalità distribuiti nonché le relative date/occasioni di elargizioni. Tale obbligo non si applica per gli omaggi cosiddetti "marchiati", riportanti cioè il logotipo della Banca (quali biro, oggetti per scrivania, ecc.), nonché l'omaggistica standard predisposta dalle Banca (ad esempio, in occasione di fine anno);
- verificare periodicamente il succitato elenco al fine di individuare eventuali situazioni anomale.

- <u>Tracciabilità del processo</u> sia a livello di sistema informativo sia in termini documentali:
  - completa tracciabilità a livello documentale e di sistema dei processi di gestione degli omaggi, liberalità, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni anche attraverso la redazione, da parte di tutte le strutture/funzioni interessate, di una reportistica sulle erogazioni effettuate/contratti stipulati;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la struttur/funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito della gestione degli omaggi, delle liberalità, delle spese di rappresentanza, delle beneficenze e sponsorizzazioni.

Principi di comportamento

Premesso che le spese per omaggi/liberalità sono consentite purché di modico valore e, comunque, tali da non compromettere l'integrità e la reputazione di una delle parti e da non influenzare l'autonomia di giudizio del beneficiario, le strutture della Banca, a qualsiasi titolo coinvolte nella gestione di omaggi/liberalità, delle spese di rappresentanza, delle beneficenze e delle sponsorizzazioni sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione. In particolare:

- la Banca può effettuare erogazioni sotto forma di beneficenze o sponsorizzazioni per sostenere iniziative di Enti regolarmente costituiti ai sensi di legge e che non contrastino con i principi etici della Banca e nel caso di beneficenze, tali enti non devono avere finalità di lucro;
- eventuali iniziative la cui classificazione rientri nei casi previsti per le "sponsorizzazioni" non possono essere oggetto contemporaneo di erogazione per beneficenza fatta salva l'autorizzazione dell'organo di gestione;
- le erogazioni devono essere riconosciute esclusivamente su un conto corrente intestato all'ente beneficiario; non è consentito effettuare pagamenti in contanti, in un Paese diverso da quello dell'ente beneficiario o a un soggetto diverso dallo stesso.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- effettuare erogazioni, per iniziative di beneficenza o di sponsorizzazione, a favore di Enti coinvolti in note vicende giudiziarie, pratiche non rispettose dei diritti umani, o contrarie alle norme in tema di vivisezione e di tutela dell'ambiente. Non possono inoltre essere oggetto di erogazioni partiti e movimenti politici e le loro articolazioni organizzative, organizzazioni sindacali e di patronato, salvo specifiche iniziative connotate da particolare rilievo sociale, culturale o scientifico che devono essere approvate dal OFSS (Organo con Funzioni di Supervisione Strategica);
- effettuare elargizioni/omaggi a favore di Enti/esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero ad altre organizzazioni/persone ad essa collegate contravvenendo a quanto previsto nel presente protocollo e nella Policy Anticorruzione;
- promettere o versare/offrire – anche a mezzo di intermediari - somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri – a esponenti/rappresentanti della Pubblica Amministrazione, Autorità di Vigilanza o altre istituzioni pubbliche ovvero altre organizzazioni con la finalità di promuovere o favorire interessi della Banca, anche a seguito di illecite pressioni. Il personale non può dare seguito ad alcuna richiesta di indebiti vantaggi o tentativi di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente venire a conoscenza e deve immediatamente segnalarla alla Funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;

- promettere o versare/offrire somme di denaro non dovute, doni, gratuite prestazioni (al di fuori dalle prassi di regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura - direttamente o indirettamente, per sé o per altri - a favore di esponenti apicali o di persone a loro subordinate appartenenti a società controparte o in relazione con la Banca, al fine di favorire indebitamente gli interessi della Banca;
- dare in omaggio beni per i quali non sia stata accertata la legittima provenienza ed il rispetto delle disposizioni che tutelano le opere dell'ingegno, i marchi e i diritti di proprietà industriale in genere nonché le indicazioni geografiche e le denominazioni di origine protette.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

7.2.10 Gestione delle valutazioni immobiliari

La gestione delle valutazioni immobiliari riguarda qualunque tipologia di attività svolta dalla Banca finalizzata alle valutazioni immobiliari effettuate, direttamente o indirettamente, per conto e nell'interesse della Cassa di Risparmio di Fermo S.p.a.-

Ai sensi del D.Lgs. n. 231/2001, il processo in oggetto potrebbe costituire ad esempio una delle modalità strumentali attraverso cui commettere i reati di "*Corruzione*", nelle loro varie tipologie, e di "*Induzione indebita a dare o promettere utilità, di "Traffico di influenze illecite*". Potrebbe sussistere altresì il rischio della commissione dei reati di "*Corruzione tra privati*" e di "*Istigazione alla corruzione tra privati*".

Quanto definito dal presente protocollo è volto a garantire il rispetto da parte della Banca della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti. In particolare:
  - i soggetti che esercitano poteri autorizzativi e/o negoziali nella gestione dei rapporti inerenti il protocollo in oggetto sono individuati e autorizzati in base allo specifico ruolo loro attribuito dal funzionigramma aziendale ovvero dal Responsabile di riferimento tramite delega interna, da conservare a cura della Banca e operano esclusivamente nell'ambito del perimetro/portafoglio di clientela loro assegnato dal Responsabile di riferimento.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo. In particolare:
  - le attività di cui alle diverse fasi del processo devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di maker e checker.
- Attività di controllo
- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo di gestione delle valutazioni immobiliari.

Principi di comportamento

Le Funzioni a qualsiasi titolo coinvolte nella gestione delle valutazioni immobiliari, sono tenute ad osservare le modalità esposte nel presente documento, le previsioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione.

Carifermo si è inoltre dotata di un "Regolamento delle valutazioni immobiliari" che regolamenta l'attività in discorso e si pone a presidio dei reati ad essa connessi.

In particolare:

- il personale non può dare seguito ad alcuna richiesta di indebiti vantaggi o tentativo di concussione da parte di un funzionario della Pubblica Amministrazione di cui dovesse essere destinatario o semplicemente a conoscenza e deve immediatamente segnalarla al proprio responsabile, il quale a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla funzione di Internal Audit ed al per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- qualora sia previsto il coinvolgimento di soggetti terzi nel processo di gestione del patrimonio immobiliare, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto;
- non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano risultare strumentali alla commissione di fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- promettere o concedere beni immobili– anche a mezzo di intermediari - a Enti della Pubblica Amministrazione, istituzioni pubbliche o a soggetti da questi ultimi indicati a condizioni diverse da quelle di mercato;
- promettere o concedere beni immobili a esponenti apicali, e/o persone a loro subordinate, di società controparti o in relazione con la Banca ovvero a soggetti da questi indicati, al fine di favorire indebitamente il perseguimento di interessi della Banca;
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dalla Policy Anticorruzione; ciò al fine di prevenire il rischio di commissione di reati di corruzione nelle loro varie tipologie, di "induzione indebita a dare o promettere utilità", e di "*Traffico di influenze illecite*" che potrebbe derivare dall'eventuale scelta di soggetti "vicini" a persone

legate alla Pubblica Amministrazione e dalla conseguente possibilità di agevolare/condizionare la gestione del rapporto negoziale con la Banca.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

8 REATI DI FALSITA' IN MONETE, IN CARTE DI PUBBLICO CREDITO E IN VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO (ART.25-BIS D.LGS.231/2001)

8.1 Fattispecie di reato

Premessa

L'art. 25-*bis* del Decreto contempla una serie di reati previsti dal codice penale a tutela della fede pubblica, ossia dell'affidamento sociale nella genuinità ed integrità di alcuni specifici simboli, essenziale ai fini di un rapido e certo svolgimento del traffico economico. Le condotte punite hanno ad oggetto monete – a cui sono equiparate le carte di pubblico credito, vale a dire le banconote e le carte e cedole al portatore emesse da Governi o da Istituti a ciò autorizzati – valori di bollo, carte filigranate e strumenti od oggetti destinati al falso nummario.

I reati di cui all'art.25-bis sono legati al rischio di commissione di reati di spendita di monete falsificate in buona fede.

In particolare, si elencano di seguito le fattispecie di reato identificate quali rilevanti, in relazione all'operatività della Banca, nell'ambito della presente Parte Speciale:

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- Alterazione di monete (art. 454 c.p.);
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.).
- Contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali (art. 473 c.p.);
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

Circa il dettaglio delle fattispecie delittuose previste dall'art. 25-bis del Decreto si rimanda all'allegato "Elenco Reati".

8.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i reati di falsità in monete sono la:

- Gestione valori (banconote, monete e valori in genere);

- Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione;
- Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze.

In riferimento alle attività “Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione” e “Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze” si rimanda alle stesse attività a rischio-reato già oggetto di trattazione della Parte Speciale “Reati contro la Pubblica Amministrazione”, ove sono definiti i principi generali di controllo e i principi di comportamento a presidio anche dei reati della presente Parte Speciale.

Con riferimento alla “Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione” il rischio di commissione reati oggetto della presente Parte Speciale riguarda principalmente le attività di “sportello” e, in particolare, il processo di erogazione del credito. Il rischio in cui potrebbe incorrere la Banca consiste infatti nella possibilità di favorire, in maniera consapevole o inconsapevole, dovuta ad una inadeguata attività di verifica/istruttoria, clienti coinvolti in condotte riconducibili alle fattispecie di reato oggetto di trattazione nella presente parte speciale. Inoltre, è opportuno sottolineare che la conoscenza della clientela, componente rilevante al fine di presidiare i rischi-reato in esame, rappresenta uno dei principali adempimenti in materia di lotta al riciclaggio e al finanziamento del terrorismo (D.Lgs.231/2007 e s.m.i.); pertanto, una parte significativa dei presidi organizzativi aziendali è costituita, pur con le dovute specificità richieste dal Decreto, dalle iniziative organizzative e procedurali attuate dalla Banca in conformità alle disposizioni normative richiamate.

Si rimanda, per l’esposizione di tali presidi organizzativi, all’attività a rischio-reato “Gestione degli adempimenti in materia di contrasto al riciclaggio e al finanziamento al terrorismo” oggetto di trattazione della Parte Speciale “Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio”.

Di seguito viene descritto il protocollo che detta i principi generali di controllo e i principi di comportamento applicabili alle attività sensibili sopra individuate e che si aggiungono alle policy e ai regolamenti della Banca già in essere a cui l’operatività aziendale deve uniformarsi e che regolamenta l’attività medesima, in particolare il “Regolamento Gestione del Contante”.

Il protocollo è infatti posto a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, da outsourcer esterni (a titolo esemplificativo, l’attività di prelievo, trasporto, contazione e custodia sono esternalizzate presso società specializzate, in grado di assicurare il rispetto della normativa in materia di gestione del contante), da consulenti esterni e/o da fornitori di qualsiasi genere che abbiano rapporti con la Banca.

I principi generali di controllo e i principi di comportamento sono, pertanto, destinati a tutti gli operatori che a vario titolo entrano nel ciclo di gestione del contante: operatori di sportello, addetti alle apparecchiature di contazione/verifica del contante ad uso interno, addetti al carico/scarico del contante delle apparecchiature automatiche a disposizione della clientela, responsabili delle segnalazioni obbligatorie , referenti delle attività di contazione/trasporto valori esternalizzate.

8.2.1 Gestione valori (banconote, monete e valori in genere)

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, nell'attività inerente la trattazione di valori di qualsiasi natura con particolare riferimento a banconote, monete, valori di bollo aventi corso legale nello Stato e all'estero.

Ai sensi del D. Lgs. n. 231/2001, il relativo processo potrebbe presentare occasioni per la commissione dei reati di "*Falsificazione di monete, spendita e introduzione nello Stato, previo concerto di monete falsificate*" (art. 453 c.p.), "*Alterazione di monete*" (art. 454 c.p.), "*Spendita e introduzione nello Stato, senza concerto, di monete falsificate*" (art. 455 c.p.), "*Spendita di monete falsificate ricevute in buona fede*" (art. 457 c.p.).

Ancorché l'attività tradizionale della Banca sia propriamente incentrata sulla gestione dei valori appare remota la possibilità che operatori interni della Banca pongano in essere, autonomamente ovvero in concorso con terzi, nell'interesse della stessa, fatti di alterazione o contraffazione di valori.

Maggiori rischi si possono, invece, rinvenire in relazione alla messa in circolazione di valori falsificati e/o contraffatti posto che potrebbe sussistere la responsabilità amministrativa della Banca nel caso in cui, anche in assenza di concerto con gli autori della falsificazione, un operatore bancario, dubitando della autenticità di taluni valori al momento della ricezione, pur senza avere conoscenza certa della loro falsità, li mettesse in circolazione nell'intento di evitare alla Banca pregiudizi od anche solo gli inconvenienti derivanti dalla rilevazione e dalla denunzia della falsità dei valori alle Autorità competenti.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa, in particolare:
  - i soggetti che esercitano poteri autorizzativi e/o negoziali nell'ambito dell'attività a rischio-reato sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale, dal Regolamento vigente e dal vigente sistema di poteri e deleghe della Banca;
  - i soggetti che intervengono nel processo di movimentazione di valori (prelievo, trasporto, contazione e custodia) devono essere individuati e autorizzati dal Responsabile di riferimento della Banca, nel rispetto della normativa interna;
  - la stipula di rapporti contrattuali con intermediari addetti alla lavorazione dei valori deve essere autorizzata da soggetti a ciò facoltizzati in base al funzionigramma aziendale e al vigente sistema dei poteri e delle deleghe.
- Segregazione dei compiti tra i differenti soggetti coinvolti nel processo.
- Attività di controllo: la normativa interna di riferimento identifica i controlli di linea che devono essere svolti a cura di ciascuna struttura/punto operativo interessata nello svolgimento delle attività di trattazione dei valori (banconote/monete in euro o estere) inerenti all'esecuzione del processo oggetto del presente protocollo. In particolare:

- sotto la responsabilità del Responsabile della struttura/funzione aziendale del punto operativo, si riscontrano con periodicità i valori in carico a tutti gli operatori;
- con riferimento alla cassa continua/raccolta valori tramite intermediari, l'apertura del mezzo corazzato, il riscontro dei contenitori e dei valori deve avvenire con il concorso di due addetti senza soluzione di continuità;
- con riferimento alle attività di gestione delle apparecchiature ATM, l'apertura del mezzo corazzato, il riscontro dei contenitori e dei valori e la quadratura devono avvenire, ove possibile, con il concorso di due addetti senza soluzione di continuità.
- il Responsabile della struttura/funzione aziendale del punto operativo, o addetto designato, procede almeno una volta ogni trimestre alla verifica a campione del contenuto quali/quantitativo delle mazzette oggetto di rimessa, annotando i controlli effettuati e le relative risultanze.

Qualora sia previsto il coinvolgimento di soggetti terzi (a titolo esemplificativo, fornitori, consulenti e professionisti) nell'attività a rischio-reato di cui alla presente Parte Speciale:

- i principi generali di controllo e i principi di comportamento ivi contenuti si applicano anche a presidio delle attività poste in essere dagli stessi;
- i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e al Codice Etico e di impegno al loro rispetto;
- le strutture/funzioni aziendali che gestiscono la relazione con tali soggetti sono incaricate del monitoraggio circa il rispetto dei livelli di servizio definiti nell'ambito dei contratti stipulati con gli stessi dalla Banca;
- la selezione di tali soggetti avviene conformemente alla normativa interna di riferimento, nonché ai principi generali di controllo e ai principi di comportamento qualificati nell'ambito dell'attività a rischio-reato "Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze";
- le strutture/funzioni aziendali coinvolte nella gestione dei rapporti con tali soggetti si attengono alle prescrizioni di cui alla Policy anticorruzione e alla Policy fornitori.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - la realizzazione delle operazioni nella esecuzione degli adempimenti di cui alla messa in circolazione di valori prevede l'utilizzo di sistemi informatici di supporto che garantiscono la tracciabilità delle operazioni effettuate;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la struttura/funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo di gestione dei valori, inclusa quella rimessa alla Banca d'Italia con riferimento alla trasmissione di banconote sospette di falsità.

Principi di comportamento

Tutti i soggetti operanti in nome e per conto della Banca, a qualsiasi titolo coinvolti nella gestione dei valori, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

In particolare tutti i soggetti che, nell'espletamento delle attività di propria competenza, a qualunque titolo si trovino a dover trattare valori:

- sono tenuti ad operare con onestà, integrità, correttezza e buona fede;
- devono essere appositamente incaricati come sopra indicato;
- sono tenuti a prestare particolare attenzione in relazione alle negoziazioni con clientela non sufficientemente conosciuta ovvero avente ad oggetto importi di rilevante entità;
- sono tenuti ad effettuare uno scrupoloso controllo sui valori ricevuti, al fine di individuare, ove presente, quelli sospetti di falsità. L'attività di identificazione può avvenire anche attraverso l'utilizzo di apparecchiature di selezione e accettazione delle banconote, atte a verificare sia l'autenticità sia l'idoneità alla circolazione delle banconote oppure a verificarne esclusivamente l'autenticità, oppure mediante controlli di autenticità da parte di personale addestrato, attraverso accertamenti manuali e senza l'ausilio di dispositivi di selezione e accettazione;
- sono tenuti, in presenza di banconote sospette di falsità, a:
    - predisporre tempestivamente un verbale di ritiro delle banconote sospette di falsità ed a farne segnalazione alle competenti Autorità (Ufficio Centrale Antifrode dei Mezzi di Pagamento - UCAMP, Banca d'Italia), come previsto dalla normativa vigente e con le modalità ed entro i termini prescritti dalla normativa interna;
    - custodire le banconote sospette di falsità per le quali è stato redatto il verbale in idonei mezzi forti nel periodo intercorrente tra la data di accertamento/ritiro del valore a quella di inoltro alla Banca d'Italia;
    - segnalare immediatamente al proprio Responsabile qualunque tentativo di messa in circolazione di banconote o valori sospetti di falsità da parte della clientela o di terzi del quale il personale risulti destinatario o semplicemente a conoscenza. Il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla Funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza.

Inoltre:

- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione dei valori, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- non è consentito riconoscere compensi in favore di fornitori di servizi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- mettere in circolazione, in concorso o meno con terzi, valori falsi; l'addetto che riceva in buona fede una banconota ed abbia, successivamente, dei dubbi sulla sua legittimità non deve tentare a sua volta di metterla nuovamente in circolazione ovvero restituire la banconota sospetta di falsità all'esibitore, tagliarla a metà o distruggerla;
- contravvenire a quanto previsto dalla normativa vigente in materia di ritiro dalla circolazione e trasmissione alla Banca d'Italia delle banconote denominate in euro sospette di falsità.

I Destinatari della presente Parte Speciale sono tenuti ad osservare le previsioni legislative esistenti e i principi del Codice Etico e ad eseguire i controlli formalizzativi nella normativa interna rilevante. I soggetti a qualsiasi titolo coinvolti nelle attività a rischio-reato identificate, sono inoltre tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi generali di controllo e dei principi comportamento descritti nel presente protocollo.

9 REATI SOCIETARI (ART.25-TER D.LGS.231/2001)

9.1 Fattispecie di reato

Premessa

La presente Parte Speciale è volta a presidiare il rischio di commissione dei reati societari di cui all'art.25-ter del D.Lgs.231/2001.

In particolare, si elencano di seguito le fattispecie di reato identificate quali rilevanti, in relazione all'operatività della Banca, nell'ambito della presente Parte Speciale:

- False comunicazioni sociali (art. 2621 – 2621-bis c.c.);
- False comunicazioni sociali in danno della società, dei soci o dei creditori (art. 2622 c.c.);
- Impedito controllo (art. 2625 c.c.);
- Indebita restituzione di conferimenti (art. 2626 c.c.);
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.);
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
- Omessa comunicazione del conflitto d'interessi (art. 2629-bis c.c.);
- Formazione fittizia del capitale (art. 2632 c.c.);
- Corruzione tra privati (art. 2635 c.c.);
- Istigazione alla corruzione tra privati (art. 2635-bis c.c.);
- Illecita influenza sull'assemblea (art. 2636 c.c.);
- Aggiotaggio (art. 2637 c.c.);
- Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.);
- False o omesse dichiarazioni per il rilascio del certificato preliminare (art.54 D.Lgs.19/2023).

Con specifico riferimento ai reati di "Corruzione tra privati" e "Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza" si rimanda alla Parte Speciale "Reati contro la Pubblica Amministrazione", ove sono individuate le attività a rischio di commissione dei reati in oggetto e qualificati principi generali di controllo e principi di comportamento aventi efficacia anche a presidio dei medesimi.

Inoltre, in riferimento al reato di *Aggiotaggio*, si rimanda alla Parte Speciale "Reati di abuso di informazioni privilegiate e di manipolazione del mercato", in cui sono definiti principi generali di controllo e principi di comportamento aventi efficacia anche a presidio dei medesimi.

Circa il dettaglio delle fattispecie delittuose previste dall'articolo 25-ter del Decreto si rimanda all'allegato "Elenco Reati".

L'art. 25-*ter* del Decreto contempla quasi tutti i reati societari previsti dal Titolo XI del codice civile, che sono qualificabili come reati generali, in quanto non specificamente riferibili all'esercizio dell'attività bancaria.

I reati societari considerati hanno ad oggetto differenti ambiti, tra i quali assumono particolare rilevanza la formazione del bilancio, le comunicazioni esterne, talune operazioni sul capitale, l'impedito controllo e l'ostacolo all'esercizio delle funzioni di vigilanza, fattispecie accomunate dalla finalità di tutelare la trasparenza dei documenti contabili e della gestione societaria e la corretta informazione ai soci, ai terzi ed al mercato in generale.

Per quanto concerne le fattispecie criminose che si riferiscono ai documenti contabili ed ai controlli delle Autorità di Vigilanza, si rileva che la Banca si pone in una posizione privilegiata dal punto di vista della prevenzione e della corretta attuazione dei precetti normativi, in quanto risulta destinataria di una disciplina speciale che impone la procedimentalizzazione dell'intera fase di elaborazione di detta documentazione nonché una serie di obblighi ed adempimenti in relazione ai rapporti con le Autorità, con la conseguenza che le modalità di gestione del rischio dei reati qui considerati risultano replicare comportamenti già consolidati nella prassi bancaria o, comunque, derivanti dall'applicazione delle norme primarie e regolamentari vigenti.

9.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i reati societari sono indicate di seguito.

<u>Adempimenti amministrativi e societari:</u>

- Operazioni di rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nell'informativa periodica, nei bilanci, nelle relazioni sulla gestione e in altri documenti di impresa;
- Gestione dei rapporti con il Collegio Sindacale e la Società di Revisione;
- Attività della Banca nell'ambito di operazioni infragruppo, straordinarie o che incidono sul capitale sociale (acquisto, gestione e cessione di partecipazioni e di altri asset);
- Gestione dei rapporti con le Autorità di Vigilanza.

Nei successivi paragrafi si riportano i protocolli che dettano i principi generali di controllo e di comportamento applicabili a dette attività che si completano con la normativa aziendale di dettaglio che regolamenta le attività medesime, precisando che, con particolare riferimento al reato di corruzione tra privati, trattandosi di fattispecie a potenziale impatto trasversale su tutte le attività della Banca, si rimanda altresì alle attività sensibili già oggetto di trattazione nella Parte Speciale inerente i "Reati contro la Pubblica Amministrazione" in quanto contenenti principi che esplicano la loro efficacia preventiva anche in relazione ai reati di cui alla presente Parte Speciale, in particolare "Gestione dei contenziosi (in via stragiudiziale e in via giudiziale) e degli accordi transattivi", "Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze", "Gestione di omaggi, liberalità, spese di rappresentanza, beneficenze e sponsorizzazioni", "Gestione del processo di selezione, assunzione e amministrazione del personale".

Relativamente alla "Gestione dei rapporti con le Autorità di Vigilanza" si rimanda al protocollo di cui alla Parte Speciale "Reati contro la Pubblica Amministrazione", avente la specifica finalità di prevenire, oltre al reato di corruzione, anche il reato societario di cui all'art. 2638 c.c.

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, da outsourcer esterni.

L'Area Amministrazione, Controllo e Finanza si è dotata di una "Manuale di controllo dei conti di contabilità generale" e predispone di disposizioni relative agli "Adempimenti contabili e amministrativi di fine anno". È inoltre stata adottata una "Policy in materia di partecipazioni detenibili".

9.2.1 Operazioni di rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nell'informativa periodica, nei bilanci, nelle relazioni sulla gestione e in altri documenti di impresa

Il presente protocollo si applica a tutte le funzioni della Banca coinvolte nelle operazioni di rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nell'informativa periodica, nei bilanci, nelle relazioni sulla gestione e in altri documenti di impresa e in generale nella predisposizione dei documenti che contengono comunicazioni ai soci relative alla situazione economica, patrimoniale e finanziaria della Banca.

Ai sensi del D. Lgs. n. 231/2001, il processo di predisposizione dei documenti in oggetto potrebbe presentare occasioni per la commissione del reato di "false comunicazioni sociali", così come disciplinato agli artt. 2621 e 2622 del Codice Civile nonché i reati tributari, definiti nel paragrafo 17 (Area sensibile concernente i reati tributari). Inoltre, le regole aziendali e i controlli di completezza e di veridicità previsti nel presente protocollo sono predisposti anche al fine di una più ampia azione preventiva dei reati che potrebbero conseguire a una scorretta gestione delle risorse finanziarie, quali i reati di "Corruzione", nelle loro varie tipologie, di "Induzione indebita", di "Corruzione tra privati" e di "Istigazione alla corruzione tra privati", nonché i reati di "Riciclaggio", di "Autoriciclaggio".

Il processo di predisposizione dei documenti in oggetto è governato secondo il funzionigramma dal "Responsabile Area Amministrazione Controllo e Finanza".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi generali di controllo

I documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Banca devono essere redatti in base alle specifiche procedure, prassi e logiche aziendali in essere che:

- identificano con chiarezza e completezza le funzioni interessate nonché i dati e le notizie che le stesse devono fornire;
- identificano i criteri per le rilevazioni contabili dei fatti aziendali, inclusa la valutazione delle singole poste;
- determinano le scadenze, gli argomenti oggetto di comunicazione e informativa, l'organizzazione dei relativi flussi e l'eventuale richiesta di rilascio di apposite attestazioni;
- prevedono la trasmissione di dati ed informazioni alla Struttura responsabile della raccolta attraverso un sistema che consente la tracciabilità delle singole operazioni e l'identificazione dei soggetti che inseriscono i dati nel sistema.

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Ruoli e responsabilità definiti:
  - ogni singola Struttura è responsabile dei processi che contribuiscono alla produzione delle voci contabili e/o delle attività valutative ad essa demandate e degli eventuali commenti in bilancio di propria competenza;
  - il sistema dei poteri e delle deleghe stabilisce le facoltà di autonomia gestionale in relazione alle attività in oggetto, in particolare per quanto riguarda il passaggio a perdite;
  - sono definiti diversi profili di utenza per l'accesso alle procedure informatiche ai quali corrispondono specifiche abilitazioni in ragione delle funzioni attribuite;
- Segregazione delle funzioni
  - Il processo di predisposizione dei documenti che contengono comunicazioni ai soci e/o ai terzi relative alla situazione economica, patrimoniale e finanziaria della Banca prevede il coinvolgimento di distinte Strutture, operanti nelle diverse fasi del processo in base a quanto riportato nei documenti "Manuale di controllo dei conti di contabilità generale" e nelle Disposizioni relative agli "Adempimenti contabili e amministrativi di fine anno".
- Attività di controllo
  - Le attività di predisposizione dei documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Banca sono soggette a puntuali controlli di completezza e veridicità sia di sistema sia manuali. Si riportano nel seguito i principali controlli svolti dalle singole Strutture:
    - verifiche, con cadenza periodica, dei saldi dei conti di contabilità generale, al fine di garantirne la quadratura con i rispettivi partitari;
    - verifica, con periodicità prestabilita, di tutti i saldi dei conti lavorazione, transitori e similari, per assicurare che le Unità interessate che hanno alimentato la contabilità eseguano le necessarie scritture nei conti appropriati;
    - esistenza di controlli maker e checker attraverso i quali la persona che esegue l'operazione è differente da quella che la autorizza, previo controllo di adeguatezza;
    - produzione, per tutte le operazioni registrate in contabilità, di prima nota contabile, debitamente validata, e della relativa documentazione giustificativa;
    - analisi degli scostamenti, attraverso il confronto tra i dati contabili esposti nel periodo corrente e quelli relativi a periodi precedenti;
    - controllo di merito in sede di accensione di nuovi conti ed aggiornamento del piano dei conti;
    - quadratura della versione definitiva del bilancio con i dati contabili.
  - La verifica dell'adeguatezza dei processi sensibili ai fini dell'informativa contabile e finanziaria e dell'effettiva applicazione dei relativi controlli è articolata nelle seguenti fasi:
    - verifica del disegno dei controlli;

- test dell'effettiva applicazione dei controlli;
- identificazione delle criticità e dei piani di azione correttivi;
- monitoraggio sull'avanzamento e sull'efficacia delle azioni correttive intraprese.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - il processo decisionale, con riferimento alle attività di predisposizione dei documenti che contengono comunicazioni ai soci e/o al mercato relative alla situazione economica, patrimoniale e finanziaria della Banca è garantito dalla completa tracciabilità di ogni operazione contabile sia tramite sistema informatico sia tramite supporto cartaceo;
  - tutte le scritture di rettifica effettuate dalle singole Strutture responsabili dei conti di propria competenza o dalla Struttura deputata alla gestione del Bilancio, sono supportate da adeguata documentazione dalla quale sia possibile desumere i criteri adottati ed, analiticamente, lo sviluppo dei relativi calcoli;
  - tutta la documentazione relativa ai controlli periodici effettuati viene archiviata presso ciascuna Struttura coinvolta per le voci contabili di propria competenza.

9.2.2 Gestione dei rapporti con il Collegio Sindacale e con la Società di Revisione

Il presente protocollo si applica ai membri del Consiglio di Amministrazione e a tutti gli Organi e le Funzioni della Banca coinvolti nella gestione dei rapporti con il Collegio Sindacale, nell'ambito delle attività di controllo attribuite agli stessi, e con la Società di Revisione, nell'ambito delle proprie attività di revisione e certificazione del bilancio.

Ai sensi del D. Lgs. n. 231/2001, il processo in oggetto potrebbe presentare occasioni per la commissione del reato di "impedito controllo", ai sensi dell'art. 2625 del codice civile, del reato di "corruzione tra privati" ed "istigazione alla corruzione tra privati".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nella gestione dei rapporti in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio del processo si deve basare sui seguenti fattori:

- Livelli autorizzativi nell'ambito di ciascuna fase operativa. In particolare, i rapporti con il Collegio Sindacale e la Società di revisione sono intrattenuti dal Responsabile della struttura/funzione di riferimento o dai soggetti dal medesimo appositamente incaricati.
- Segregazione dei compiti tra i differenti soggetti coinvolti nell'attività a rischio reato. In particolare, per ciascuna struttura/funzione, è individuato un responsabile della raccolta e dell'elaborazione delle informazioni richieste e trasmesse al Collegio sindacale e alla Società di revisione.
- Attività di controllo: il soggetto individuato nell'ambito di ciascuna struttura/funzione quale responsabile della raccolta e dell'elaborazione delle informazioni richieste e trasmesse al Collegio Sindacale e alla Società di revisione, verifica preliminarmente la completezza, inerenza e correttezza della documentazione trasmessa.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:
  - è prevista la formalizzazione e verbalizzazione delle attività di verifica e controllo poste in essere dal Collegio Sindacale e/o dalla Società di Revisione;
  - le richieste e le trasmissioni di dati e informazioni, nonché ogni rilievo, comunicazione o valutazione espressa dal Collegio Sindacale o dalla Società di revisione, sono documentate e conservate a cura del responsabile di struttura/funzione, o da un soggetto da lui delegato.

Principi di comportamento

Le Strutture e gli Organi della Banca, a qualsiasi titolo coinvolti nella gestione dei rapporti con il Collegio Sindacale e la Società di Revisione, sono tenute alla massima diligenza, professionalità, trasparenza, collaborazione, disponibilità e al pieno rispetto del ruolo istituzionale degli stessi, dando puntuale e sollecita esecuzione alle prescrizioni ed agli eventuali adempimenti richiesti nel presente protocollo, in conformità alle disposizioni di legge esistenti in materia nonché alle eventuali previsioni del Codice Etico.

In particolare:

- deve essere sempre assicurato il regolare funzionamento della Banca e degli Organi Sociali, agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge;
- i dati ed i documenti devono essere resi disponibili in modo puntuale ed in un linguaggio chiaro, oggettivo ed esaustivo in modo da fornire informazioni accurate, complete, fedeli e veritiere;
- ciascuna Funzione aziendale è responsabile dell'archiviazione e della conservazione di tutta la documentazione formalmente prodotta e/o consegnata al Collegio Sindacale e/o ai Revisori, nell'ambito della propria attività, ivi inclusa quella trasmessa in via elettronica.
- Deve essere garantito alla Società di revisione il libero accesso alla contabilità aziendale per un corretto svolgimento dell'incarico

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre il Collegio Sindacale, altri Organi societari e la Società di Revisione in errore di valutazione tecnico-economica della documentazione presentata;
- promettere o dare somme di denaro o altre utilità a membri del Collegio Sindacale e/o della Società di Revisione, con la finalità di promuovere o favorire interessi della Banca.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

9.2.3 Attività della Banca nell'ambito di operazioni infragruppo, straordinarie o che incidono sul capitale sociale (acquisto, gestione e cessione di partecipazioni e di altri asset)

Il presente protocollo si applica a tutte le Funzioni aziendali coinvolte, a qualsiasi titolo, in attività della Banca nell'ambito di operazioni infragruppo, straordinarie o che incidono sul capitale sociale quali, a titolo esemplificativo e non esaustivo, fusioni, scissioni, costruzioni societarie, operazioni sul capitale sociale e sulle partecipazioni infragruppo, finanziamenti e prestazione di garanzie infragruppo, contratti di finanziamento o di consolidamento fiscale infragruppo, ecc.

Ai sensi del D.Lgs. n. 231/2001, le attività in oggetto potrebbero presentare potenzialmente occasioni per la commissione dei reati di Omessa comunicazione del conflitto d'interessi, Corruzione tra privati, Formazione fittizia del capitale, Illecita influenza sull'assemblea, Indebita restituzione dei conferimenti, Illegale ripartizione di utili e riserve, Illecite operazioni sulle azioni o quote sociali o della società controllata, Operazioni in pregiudizio ai creditori e Autoriciclaggio. Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Carifermo si è dotata di una "Policy in materia di partecipazioni detenibili" e di una "Policy Operazioni di Maggior Rilievo" che regolamentano alcuni aspetti dell'attività in discorso e si pongono a presidio dei reati connessi.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

- Livelli autorizzativi definiti. In particolare:
  - i soggetti che esercitano poteri autorizzativi e/o negoziali in ogni fase del processo sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile di riferimento tramite delega interna, da conservare a cura della Banca;
  - gli atti e documenti che impegnano la Banca devono essere sottoscritti da soggetti muniti dei necessari poteri.
- Segregazione dei compiti tra i soggetti coinvolti nel processo al fine di garantire tra le fasi del processo un meccanismo di maker e checker.
- Attività di controllo:
  - verifica dell'istruttoria effettuata secondo quanto previsto dalla normativa interna mediante l'eventuale esecuzione di specifiche attività di verifica (ad es. economico/finanziaria, contabile, legale, fiscale, ecc) sull'impresa oggetto d'investimento (cd. "impresa target") e sulla controparte con particolare riguardo a quanto stabilito dalla Policy Anticorruzione;
  - verifica che la delibera contenga i criteri di valutazione del prezzo dell'operazione secondo le prassi di mercato;
  - verifica del rispetto degli adempimenti legislativi e regolamentari (ad es. in tema di antiriciclaggio);
  - verifica della tenuta ed aggiornamento dell'anagrafe delle partecipazioni in essere;

- verifica del processo di valutazione periodica delle partecipazioni in essere nell'ambito della predisposizione del Bilancio d'impresa;
- ove richiesto o opportuno, la Società di revisione e il Collegio Sindacale esprimono un motivato parere sull'operazione.

- Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali, in particolare:
  - le strutture/funzioni proponenti l'operazione, in coordinamento con eventuali altre strutture/funzioni competenti, predispongono idonea documentazione a supporto dell'operazione proposta, nonché una relazione informativa preliminare che illustra i contenuti, l'interesse sottostante, le finalità strategiche dell'operazione e la compatibilità con le norme del Codice Etico e del Modello;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni sottostanti all'istruttoria svolta per l'assunzione della partecipazione e alle scelte effettuate nell'attività di gestione e cessione di partecipazioni ed altri asset, ciascuna struttura/funzione è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica oggetto del presente protocollo.

Principi di comportamento

Le Funzioni della Banca, a qualsiasi titolo coinvolte nel processo di acquisto, gestione e cessione di partecipazioni e altri asset sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della Policy Anticorruzione. In particolare:

- i soggetti che esercitano poteri autorizzativi e/o negoziali in sede pre-contrattuale, contrattuale e di gestione di rapporti partecipativi devono essere individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile di riferimento tramite delega interna, da conservare a cura degli stessi;
- la documentazione relativa ai contratti funzionali all'acquisto, gestione e cessione di partecipazioni ed altri asset deve essere conforme alla normativa generale e speciale vigente per il settore di riferimento, anche mediante il ricorso al contributo consulenziale delle competenti funzioni aziendali e/o di professionisti esterni;
- devono essere rispettate le disposizioni di legge in materia di operazioni con soggetti collegati, con specifico riferimento agli obblighi e ai divieti volti a prevenire conflitti di interesse, al processo deliberativo e ai flussi informativi verso gli organi aziendali;
- il personale non può dare seguito a qualunque richiesta di denaro o altra utilità di cui dovesse essere destinatario o venire a conoscenza formulata da esponenti apicali, o da persone loro subordinate, appartenenti a società controparti o in relazione con la Banca, finalizzata al compimento o all'omissione da parte di questi di un atto contrario agli obblighi inerenti al proprio ufficio o agli obblighi di fedeltà e deve immediatamente segnalarla alla funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza;
- qualora sia previsto il coinvolgimento di soggetti terzi nella stipula e/o nella gestione dei contratti funzionali all'acquisto, gestione e cessione di partecipazioni ed altri asset, i

contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001, delle disposizioni di legge contro la corruzione e di impegno al loro rispetto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- comunicare dati falsi o alterati;
- promettere o versare/offrire somme di denaro non dovute, doni o gratuite prestazioni (al di fuori delle prassi dei regali di cortesia di modico valore) e accordare vantaggi o altre utilità di qualsiasi natura – direttamente o indirettamente, per sé o per altri - ad amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori di società, o a soggetti sottoposti alla direzione o vigilanza dei medesimi al fine di ottenere da parte di questi il compimento o l'omissione di un atto contrario agli obblighi inerenti il loro ufficio o agli obblighi di fedeltà con la finalità di promuovere o favorire interessi della Banca. Tra i vantaggi che potrebbero essere accordati si citano, a titolo esemplificativo, la promessa di assunzione per parenti ed affini, la sponsorizzazione o la beneficenza a favore di soggetti collegati, l'erogazione di credito a condizioni non conformi ai principi di sana e prudente gestione previsti dalla normativa aziendale e, più in generale, tutte le operazioni bancarie o finanziarie che comportino la generazione di una perdita per la Banca e la creazione di un utile per i soggetti predetti (es. stralcio ingiustificato di posizione debitoria e/o applicazioni di sconti o condizioni non in linea con i parametri di mercato);
- affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta del consulente devono ispirarsi ai criteri di chiarezza e documentabilità dettati dal Codice Etico e dalla Policy Anticorruzione.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

10 REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA, NONCHÉ DI AUTORICICLAGGIO (ART.25-OCTIES D.L.GS.231/2001)

10.1 Fattispecie di reato

Premessa

La presente Parte Speciale è volta a presidiare il rischio di commissione dei "Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio", di cui all'art.25-octies del D.Lgs.231/2001.

In particolare, si elencano di seguito le fattispecie di reato identificate quali rilevanti, in relazione all'operatività della Banca, nell'ambito della presente Parte Speciale:

- Ricettazione (art. 648 c.p.);
- Riciclaggio (art. 648-bis c.p.);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.);
- Autoriciclaggio (art. 648-ter 1 c.p.).

Circa il dettaglio delle fattispecie delittuose previste dall'articolo 25-octies del Decreto si rimanda all'allegato "Elenco Reati".

Il D.Lgs. 21 novembre 2007, n. 231 (di seguito "Decreto antiriciclaggio"), in attuazione di disposizioni comunitarie, ha rafforzato la normativa in tema di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di contrasto al finanziamento del terrorismo.

L'art. 25-*octies* del D.Lgs. n. 231/01 ha esteso la responsabilità dell'ente ai reati di ricettazione, riciclaggio e impiego illecito e successivamente al reato di autoriciclaggio.

Il rafforzamento della disciplina della responsabilità amministrativa degli Enti intende prevenire e reprimere più efficacemente il fenomeno dell'immissione nel circuito economico lecito di denaro, beni od utilità provenienti dalla commissione di delitti, in quanto di ostacolo all'amministrazione della giustizia nelle attività di accertamento dei reati e di persecuzione dei colpevoli, oltre che, più in generale, lesiva dell'ordine economico, dell'integrità dei mercati e della libera concorrenza, in ragione degli indebiti vantaggi competitivi di cui godono gli operatori che dispongono di capitali di origine illecita.

Su un piano diverso, ma pur sempre finalizzate al contrasto del riciclaggio e del finanziamento del terrorismo, si collocano le previsioni contenute nel Decreto antiriciclaggio di specifici adempimenti posti a carico delle banche, degli intermediari finanziari e di altri determinati soggetti obbligati (adeguata verifica della clientela; registrazione e conservazione della documentazione delle operazioni; segnalazione di operazioni sospette; comunicazioni delle violazioni dei divieti in tema di denaro contante e dei titoli al portatore; comunicazione da parte degli Organi di controllo dell'Ente delle infrazioni riscontrate). La violazione di detti obblighi di per sé non comporta la responsabilità amministrativa dell'Ente ai sensi del D. Lgs. n. 231/2001, non essendo detti illeciti ricompresi nell'elencazione dei cosiddetti reati presupposto, ma è sanzionata ai sensi del Decreto antiriciclaggio.

È importante sottolineare che qualora l'operatore bancario contravvenisse a detti adempimenti nella consapevolezza della provenienza illecita dei beni oggetto delle operazioni, potrebbe essere chiamato a rispondere per i predetti reati, e potrebbe quindi conseguirne anche la responsabilità amministrativa della Banca ai sensi del D. Lgs. n. 231/2001.

Lo scopo della presente parte speciale è di definire canoni comportamentali volti a disciplinare aspetti propri della gestione caratteristica della Banca per i quali, tramite attività di risk assessment, sono stati rilevati potenziali profili di rischiosità in relazione al dettato del D.Lgs. n. 231/2001.

10.2 Attività aziendali sensibili

Il rischio che si verifichino nel contesto bancario i reati di riciclaggio, intesi in senso lato (ivi compreso, quindi, l'autoriciclaggio), appare invero, più marcato, quale rischio tipico del circuito bancario e finanziario, essenzialmente con riferimento ai rapporti con la clientela, e ad ipotesi di coinvolgimento/concorso in attività criminose della stessa, in particolare concerne:

- Gestione degli adempimenti in materia di contrasto al riciclaggio e al finanziamento al terrorismo;
- Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promoter finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione;
- Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze;
- Gestione di omaggi, liberalità, spese di rappresentanza, beneficienze e sponsorizzazioni;
- Gestione dei contenziosi (in via stragiudiziale e in via giudiziale) e degli accordi transattivi;
- Gestione dei valori;
- Gestione del credito su pegno.

In riferimento alle attività "Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promoter finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione", "Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze", "Gestione di omaggi, liberalità, spese di rappresentanza, beneficienze e sponsorizzazioni", "Gestione dei contenziosi (in via stragiudiziale e in via giudiziale) e degli accordi transattivi" si rimanda alle medesime attività a rischio reato già oggetto di trattazione nella Parte Speciale "Reati contro la Pubblica Amministrazione", in riferimento alla "Gestione dei valori", si rimanda alle medesime attività a rischio reato già oggetto di trattazione nella Parte Speciale "Reati di falsità in monete".

Più in generale, tutti i protocolli del presente Modello, laddove tesi a prevenire la commissione di reati che possono generare proventi illeciti, si devono intendere predisposti anche al fine della prevenzione dei reati di riciclaggio in senso lato.

In riferimento alle attività "Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promoter finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione" il rischio di commissione dei reati oggetto della presente Parte Speciale riguarda principalmente il processo di erogazione del credito, nonché l'eventuale prestazione di servizi volti a supportare la clientela nell'ambito di operazioni societarie straordinarie e/o particolarmente complesse. Il rischio in cui potrebbe incorrere la Banca infatti consiste nella possibilità di favorire clienti coinvolti in condotte riconducibili alle fattispecie di reato in esame (a titolo meramente esemplificativo, la Banca potrebbe finanziare e/o supportare in altro modo – consapevolmente ovvero a seguito di un'inadeguata attività

di istruttoria – società coinvolte in organizzazioni terroristiche e/o impegnate in attività di ricettazione/riciclaggio/impiego di denaro, beni o utilità di provenienza illecita/autoriciclaggio).

In riferimento alla "Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze" e "Gestione di omaggi, liberalità, spese di rappresentanza, beneficienze e sponsorizzazioni", la potenziale commissione dei reati da parte della Banca potrebbe configurarsi in concorso con soggetti eventualmente coinvolti nelle attività delittuose contemplate nelle fattispecie in oggetto, laddove la Banca medesima – nel proprio interesse o vantaggio – supporti a vario titolo tali soggetti (a titolo esemplificativo, attraverso la selezione di fornitori di beni servizi o l'instaurazione di partnership commerciali con enti/soggetti implicati in tali attività, tramite l'erogazione di omaggi o beneficenze a favore degli stessi, ecc.).

Con specifico riferimento all'attività "Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), inclusi gli Enti Pubblica Amministrazione", inoltre, in considerazione del fatto che la conoscenza della clientela – componente rilevante ai fini del presidio dei rischi-reato nell'ambito dell'attività a rischio-reato in esame – rappresenta uno dei principali adempimenti disposti dalla normativa in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (D.Lgs. 231/2007 e s.m.i.), una parte significativa dei presidi organizzativi aziendali è costituita, pur con le dovute specificità richieste dal Decreto, dalle iniziative organizzative e procedurali attuate dalla Banca in conformità alle disposizioni normative richiamate. Si rimanda, per l'esposizione di tali presidi organizzativi, all'attività a rischio-reato oggetto di trattazione nel seguito della presente Parte Speciale.

L'attività di prevenzione si basa sull'approfondita conoscenza della clientela e delle controparti e sull'osservanza degli adempimenti previsti dalla normativa in tema di contrasto al riciclaggio dei proventi di attività criminose ed al finanziamento del terrorismo.

La centralità del rispetto rigoroso delle disposizioni dettate dal Decreto antiriciclaggio ai fini della prevenzione dei reati presupposto in questione discende anche dalle considerazioni che seguono. Va innanzitutto ricordato che il Decreto - ai fini dell'individuazione della tipologia delle condotte con le quali può concretarsi il riciclaggio, sottoposte all'obbligo di segnalazione delle operazioni sospette – all'art. 1 definisce "operazione" la trasmissione o la movimentazione di mezzi di pagamento" e all'art. 2 contiene un'elencazione di condotte, qualificate come di riciclaggio, di amplissima estensione, tale da comprendere comportamenti che, ai fini penali, potrebbero integrare la commissione del reato di autoriciclaggio, oppure la commissione degli altri reati presupposto in esame e che, se posti in essere da dipendenti o da soggetti apicali, potrebbero far sorgere la responsabilità amministrativa dell'ente stesso.

Il rischio assume connotati diversi e appare meno rilevante laddove si abbia riguardo all'impresa bancaria come "società", con riferimento a quelle aree in cui la banca, anche a prescindere dallo svolgimento delle attività tipiche, compie operazioni strumentali, acquista partecipazioni o movimenta il proprio patrimonio, assolve gli adempimenti contabili e fiscali. In tali ambiti difatti, sussiste una sviluppata articolazione dei presidi di controllo e delle procedure al fine di assicurare il rispetto di principi di trasparenza, correttezza, oggettività e tracciabilità della gestione.

Si riporta qui di seguito il protocollo che detta i principi generali di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose.

Carifermo è particolarmente attenta alla Responsabilità Sociale d'Impresa e si impegna in una gestione proattiva dei rischi di riciclaggio e di finanziamento del terrorismo, promuovendo politiche e azioni volte al rispetto della normativa vigente e all'efficace assolvimento degli obblighi di collaborazione attiva e passiva. Essa adotta misure di prevenzione e di contrasto secondo un approccio basato sul rischio e considera le attività di conoscenza della clientela come punto fondamentale ed imprescindibile per la gestione dei rischi a cui è esposta.

A tal fine la Banca ha adottato la "Politica della Cassa di Risparmio di Fermo S.p.a. per il contrasto del riciclaggio e del finanziamento al terrorismo" (anche "Policy Antiriciclaggio") e il "Manuale Antiriciclaggio".

La Policy Antiriciclaggio si inserisce nel più ampio sistema di controlli interni della Banca volti a garantire il rispetto della normativa vigente, costituendo in tal modo il documento base dell'intero sistema dei presidi antiriciclaggio e antiterrorismo della Banca, definito dal Consiglio di Amministrazione in collaborazione con la Funzione Antiriciclaggio. Il Manuale Antiriciclaggio costituisce il documento, costantemente aggiornato, che definisce responsabilità, compiti e modalità operative nella gestione del rischio in discorso.

La normativa aziendale di dettaglio che regolamenta le attività medesime si applica anche a presidio delle attività eventualmente svolte da soggetti esterni (rete distributiva indiretta) sulla base di appositi contratti di servizio (vincoli contrattuali).

10.2.1 Gestione degli adempimenti in materia di contrasto al riciclaggio e al finanziamento al terrorismo

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, nella gestione degli adempimenti in materia di contrasto al riciclaggio e al finanziamento al terrorismo.

La presente Parte Speciale ha l'obiettivo di definire i ruoli, le responsabilità operative, i principi generali di controllo e di comportamento per il contrasto finanziario al terrorismo e al riciclaggio dei proventi di attività criminose. Un efficace assetto organizzativo antiriciclaggio, infatti, si basa su un ampio coinvolgimento degli Organi aziendali, delle strutture operative, delle Funzioni aziendali e sulla chiara definizione dei compiti e delle responsabilità delle stesse.

Si intendono qui richiamate le vigenti disposizioni aziendali, e in particolare la "Policy Antiriciclaggio" e il "Manuale Antiriciclaggio".

Il presente protocollo si applica a tutte le strutture della Banca coinvolte nelle attività sensibili sopra individuate nonché nelle attività di presidio dei rischi connessi alla normativa antiriciclaggio.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività, tracciabilità e riservatezza nell'esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio dei processi sopra descritti si basa sui seguenti fattori:

- Responsabilità definite:
    - la normativa interna individua i soggetti e le Funzioni responsabili dell'attivazione/gestione/controllo dei processi sopra descritti;
    - Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa:

- i soggetti che esercitano poteri autorizzativi e/o negoziali sono individuati e autorizzati in base allo specifico ruolo attribuito loro dalla Policy e dal Manuale Antiriciclaggio e dal vigente sistema dei poteri e delle deleghe della Banca;

- individuazione dei soggetti e delle strutture/funzioni responsabili dell'attivazione/gestione dell'iter di segnalazione delle operazioni sospette;

- nomina del Responsabile Antiriciclaggio, quale Responsabile della Funzione Antiriciclaggio collocato in posizione gerarchico-funzionale adeguata senza responsabilità dirette di aree operative né gerarchicamente dipendente da soggetti responsabili di queste aree;

- nomina del Responsabile delle segnalazioni di operazioni sospette (anche "Responsabile SOS"), ai sensi dell'art.36 del D.Lgs 231/2007 collocato in posizione gerarchico-funzionale adeguata senza responsabilità dirette di aree operative né gerarchicamente dipendente da soggetti responsabili di queste aree;

- Segregazione dei compiti tra i differenti soggetti coinvolti nell'attività a rischio reato, in particolare in relazione all'attività di monitoraggio dell'operatività volta ad individuare operazioni potenzialmente sospette, in base alla quale:

o gli operatori di Filiale o di altre strutture operative/funzioni aziendali investite da analoghe responsabilità monitorano le operazioni relative alla loro area di competenza, segnalando i movimenti sospetti al Responsabile della Dipendenza/ Responsabile di funzione o ufficio per l'approfondimento e l'eventuale segnalazione;

o il Responsabile della Dipendenza/ il Responsabile di funzione o ufficio, sulla scorta delle informazioni in proprio possesso ovvero di segnalazioni e/o richieste pervenute dagli operatori, dalle Funzioni di controllo o da altre Unità Operative o da alerts prodotti dagli applicativi di supporto, analizza l'operatività e se risulta sospetta, provvede alla segnalazione della stessa al Responsabile SOS;

o il Delegato SOS effettua l'analisi della segnalazione e svolge autonomamente le necessarie indagini sull'operazione sospetta, disponendo l'inoltro o meno delle segnalazioni alla competente Autorità.

- Attività di controllo: il sistema di controllo a presidio dei processi descritti si basa sui seguenti fattori:
  - nell'ambito di una puntuale profilatura della clientela, verifica secondo un approccio risk based, all'atto dell'accensione del rapporto, da parte del Responsabile della Dipendenza, della correttezza e completezza dei dati censiti in anagrafe, nonché in merito alle informazioni acquisite in relazione alla attività economica svolta; tali informazioni devono essere aggiornate, di volta in volta, in relazione alle motivazioni economiche sottostanti alle operazioni richieste o eseguite;
  - verifica, in occasione del censimento del cliente e periodicamente, dell'eventuale presenza del nominativo nelle versioni aggiornate delle specifiche liste antiterrorismo;
  - verifica, nell'ambito della concessione e gestione delle linee di credito alla clientela, della coerenza tra il finanziamento richiesto ed il profilo economico-finanziario del cliente, per una valutazione circa la (potenziale) esposizione a fenomeni di riciclaggio o di finanziamento del terrorismo;

- software diagnostici deputati alla valutazione della qualità dei dati conservati nell'Archivio Unico Informatico;
- monitoraggio costante da parte delle Strutture operative preposte che garantisca un controllo incrociato tra il profilo soggettivo del cliente, la tipologia di operazione, la frequenza e le modalità di esecuzione, l'area geografica di riferimento (con particolare riguardo all'operatività da/verso Paesi a rischio) e ancora il grado di rischio attribuito al prodotto oggetto dell'operazione, i fondi impiegati, , il comportamento tenuto dal cliente al momento dell'esecuzione dell'operazione (qualora venga eseguita in presenza del cliente);
- monitoraggio e presidio da parte delle strutture/funzioni preposte al controllo interno della puntuale esecuzione delle attività delle strutture/funzioni operative in merito alla:
  - acquisizione delle informazioni per l'identificazione e la profilatura della clientela;
  - valutazione delle operazioni rilevate dalla procedura Gianos (o da altre procedure informatiche in uso);
  - rilevazione e valutazione degli altri indici di anomalia eventualmente presenti nella concreta operatività;
  - rilevazione delle infrazioni delle disposizioni in tema di limitazioni nell'utilizzo del contante e dei titoli al portatore;
  - registrazione dei rapporti e delle operazioni in AUI ("Archivio unico informatico") e conservazione dei documenti e delle informazioni;
    - tutti i rapporti continuativi e le operazioni che comportano la trasmissione di mezzi di pagamento devono essere processati con modalità che consentano la registrazione procedurale nell'Archivio Unico Informatico con dati corretti e completi, anche avvalendosi di controlli automatici sulla qualità dei dati. A tale fine è indispensabile procedere alle attività di "integrazione" e "sistemazione" delle operazioni o dei rapporti in stato di "sospeso" entro i termini consentiti dalle procedure e comunque nei termini previsti dalla norma;
- presidio sulla corretta esecuzione degli adempimenti prescritti in materia di contrasto finanziario al terrorismo;
- adozione di sistemi di controllo informatici atti ad impedire l'operatività riguardanti soggetti/Paesi/ oggetto di restrizioni di natura finanziaria

- <u>Tracciabilità del processo</u> sia a livello di sistema informativo sia in termini documentali:
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo descritto;
  - archiviazione sistematica di tutta la documentazione relativa all'operatività e ai controlli periodici effettuati sulle posizioni relative ai clienti, presso le strutture operative di competenza.

- Riservatezza delle informazioni, con particolare riguardo a quelle relative alle segnalazioni delle operazioni sospette, mediante l'adozione di idonee misure informatiche e fisiche.
- Formazione: è prevista la sistematica erogazione di attività specificamente dedicate alla formazione e addestramento continuo dei dipendenti e dei collaboratori sugli obblighi previsti dalla normativa antiriciclaggio. L'addestramento e la formazione assicurano una specifica preparazione del personale a più diretto contatto con la clientela e di quello addetto alla funzione antiriciclaggio.

Principi di comportamento

Le Funzioni della Banca, a qualsiasi titolo coinvolte nelle attività di contrasto del riciclaggio e del finanziamento del terrorismo, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

In particolare, le Funzioni competenti sono tenute a:

- assicurare lo sviluppo e la gestione operativa delle applicazioni utilizzate nelle attività di contrasto finanziario al terrorismo/antiriciclaggio e comunque in tutte le attività che si basano sulla "adeguata conoscenza della clientela";
- verificare e garantire il rispetto all'interno delle strutture della Banca, dei provvedimenti restrittivi in materia di antiterrorismo emanati dalle competenti autorità nazionali ed internazionali, nonché l'adozione di procedure automatiche di rilevazione;
- dettagliare nell'ambito di regolamenti/norme operative interne le regole comportamentali ad integrazione e maggiore specificazione della normativa esterna e dei principi sanciti dal presente protocollo;
- nel caso di valutazione di clientela ovvero di operazioni che interessino più strutture operative, collaborare tra loro e, ove consentito dalla normativa vigente, scambiare le informazioni finalizzate alla completa ed adeguata conoscenza del cliente e delle sue abitudini operative;
- assicurare con continuità e sistematicità la formazione e l'addestramento del personale sulla normativa antiriciclaggio e sulle finalità dalla stessa perseguite;
- diffondere a tutti i collaboratori, indipendentemente dalle mansioni in concreto svolte, la normativa di riferimento ed i relativi aggiornamenti.

Inoltre, tutti i dipendenti e collaboratori, attenendosi a quanto prescritto nelle procedure aziendali, devono:

- all'atto dell'accensione di rapporti continuativi o del compimento di operazioni oltre la soglia di legge, anche se frazionate:
    - procedere all'identificazione della clientela e verificare l'eventuale presenza del nominativo nelle versioni aggiornate delle "Black List";
    - verificare la sussistenza di eventuali titolari effettivi, acquisire informazioni sullo scopo e sulla natura del rapporto o dell'operazione e, qualora il cliente sia una società o un Ente, verificare la sussistenza dei poteri di rappresentanza e la struttura di proprietà e di controllo del cliente;

- mantenere aggiornati tutti i dati del Cliente al fine di consentire una costante valutazione del suo profilo economico e finanziario;
- effettuare l'adeguata verifica e la profilatura della clientela quando, indipendentemente da qualsiasi soglia di importo o di esenzione applicabile, vi sia il sospetto di riciclaggio, di finanziamento del terrorismo, o sorgano dubbi sulla veridicità o sull'adeguatezza dei dati identificativi già acquisiti;
- mantenere l'assoluto riserbo sulle informazioni relative alla fascia di rischio antiriciclaggio attribuita al cliente e al relativo punteggio calcolato dalla procedura, che in nessun caso devono essere comunicati alla clientela;
- collaborare attivamente ai processi per la rilevazione e la segnalazione delle operazioni sospette;
- valutare se dare avvio all'iter di segnalazione in presenza di indici di anomalia anche se non rilevati dalle procedure informatiche, o nei casi in cui risulti impossibile rispettare gli obblighi di adeguata verifica;
- verificare l'eventuale presenza dei clienti nelle versioni aggiornate delle Black List e bloccare o, comunque, non dare esecuzione ad operazioni che vedano coinvolti soggetti/Paesi/ oggetto di restrizioni di natura finanziaria;
- inoltrare le comunicazioni delle infrazioni delle disposizioni in tema di limitazioni all'uso del contante e dei titoli al portatore rilevabili nell'operatività della clientela;
- rispettare rigorosamente le procedure interne in tema di registrazione dei rapporti e delle operazioni in AUI e di conservazione della documentazione.

I dipendenti della Banca incaricati di attività valutative o autorizzative previste dai processi in materia di antiriciclaggio, devono esercitare la discrezionalità loro rimessa secondo criteri di professionalità e ragionevolezza. In caso di conflitti di interesse, anche potenziali, di ordine personale o aziendale devono:

- informare immediatamente il proprio superiore gerarchico della sussistenza del conflitto di interessi precisandone la natura, i termini, l'origine e la portata;
- astenersi dall'attività valutativa / autorizzativa, rimettendo la decisione al proprio superiore gerarchico o alla Struttura specificamente individuata nella normativa interna per l'evenienza;
- è inoltre fatto divieto comunicare, anche in modo involontario, a terzi (inclusi i soggetti con i quali sussistono rapporti di familiarità diretta o stretti legami propri o dei propri congiunti) per ragioni diverse da quelle di ufficio, il contenuto delle attività valutative / autorizzative al di fuori dei casi previsti dalla legge.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. 231/2001 e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- instaurare rapporti continuativi, o mantenere in essere quelli preesistenti, ed eseguire operazioni quando non è possibile attuare gli obblighi di adeguata verifica nei confronti del cliente, ad esempio per il rifiuto del cliente a fornire le informazioni richieste;
- ricevere od occultare denaro o cose provenienti da un qualsiasi delitto o compiere qualunque attività che ne agevoli l'acquisto, la ricezione o l'occultamento;

- sostituire o trasferire denaro, beni o altre utilità provenienti da illeciti, ovvero compiere in relazione ad essi altre operazioni che possano ostacolare l'identificazione della loro provenienza delittuosa;
- partecipare ad uno degli atti di cui ai punti precedenti, associarsi per commetterli, tentare di perpetrarli, aiutare, istigare o consigliare qualcuno a commetterli o agevolarne l'esecuzione;

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

11 DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI (ART.25-OCTIES.1 D.L.GS.231/2001)

11.1 Fattispecie di reato

Premessa

La presente Parte Speciale è volta a presidiare il rischio di commissione dei "Delitti in materia di strumenti di pagamento diversi dai contanti", di cui all'art.25-octies.1 del D.Lgs.231/2001.

In particolare, si elencano di seguito le fattispecie di reato identificate quali rilevanti, in relazione all'operatività della Banca, nell'ambito della presente Parte Speciale:

- Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.);
- Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.);
- Frode informatica aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.);
- Trasferimento fraudolento di valori (art. 512-bis c.p.).

Circa il dettaglio delle fattispecie delittuose previste dall'articolo 25-octies.1 del Decreto si rimanda all'allegato "Elenco Reati".

L'articolo 25 octies.1 - inserito recentemente nel D.Lgs 231/2001 con il D.Lgs 8 novembre 2021, n. 184 che, a sua volta dava attuazione, nell'ordinamento interno, alla direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti - introduce la responsabilità amministrativa delle persone giuridiche in relazione alla commissione di "delitti in materia di strumenti di pagamento diversi dai contanti".

La definizione di strumenti di pagamento diversi dal contante è rinvenibile nell'art. 1 del d.lgs. 184/2021, il quale definisce come tale «un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali», chiarendo ulteriormente che per «dispositivo, oggetto o record protetto» si intende un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta (per esempio mediante disegno, codice o firma); con la locuzione «mezzo di scambio digitale» si intende invece «qualsiasi moneta elettronica definita all'art. 1, comma 2, lett. h ter), d.lgs. 385/1993, e la valuta virtuale», intendendosi quest'ultima come una «rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente».

Il legislatore ha voluto rivolgersi a quelle aree organizzative dell'ente che si occupano di gestire, controllare e monitorare i flussi patrimoniali e finanziari, in quanto la gestione illecita - diretta o

indiretta - degli strumenti di pagamento (in entrata o in uscita) e dei movimenti monetari, potrebbe rappresentare fonti di entrate per la criminalità organizzata.

Caratteristiche e contesto di detti reati fanno sì che gli stessi possano essere ricondotti nell'area sensibile dei reati informatici di cui all'art.24-bis; inoltre le attività sensibili previste in quest'area, ricomprendenti reati che possono generare proventi illeciti, si devono intendere predisposte anche al fine della prevenzione dei reati di riciclaggio di cui all'art.25-octies.

Lo scopo della presente parte speciale è di definire canoni comportamentali volti a disciplinare aspetti propri della gestione caratteristica della Banca per i quali, tramite attività di risk assessment, sono stati rilevati potenziali profili di rischiosità in relazione al dettato del D.Lgs. n. 231/2001.

11.2 Attività aziendali sensibili

Il rischio che si verifichino nel contesto bancario i delitti in materia di strumenti di pagamento diversi dai contanti, appare potenziale nel circuito bancario e finanziario, in particolare per quanto riguarda la commissione del reato di "Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti" e ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal Codice penale, a condizione che ne siano oggetto materiale gli strumenti di pagamento diversi dai contanti; in particolare il processo di gestione e utilizzo degli strumenti di pagamento diversi dai contanti si articola nei seguenti processi:

- Gestione dell'assegnazione e dell'utilizzo di carte di debito/credito aziendali;
- Gestione degli strumenti di pagamento diversi dai contanti (carte di debito, carte di credito, carte prepagate etc.);
- Gestione di incassi e pagamenti;
- Gestione dei servizi di accesso ai canali digitali.

In relazione all'art.493-ter c.p., la condotta presa in considerazione è quella dell'utilizzo, da parte di chi non è titolare, di strumenti di pagamento diversi dal contante; il rischio attiene alla gestione di carte di credito/debito aziendali, smart card o di altri strumenti e all'utilizzo dei medesimi da parte di soggetti non abilitati. La giurisprudenza inoltre ritiene integrato il reato anche in caso di uso dello strumento di pagamento da parte di un terzo delegato per operazioni differenti da quelle espressamente autorizzate dal titolare. Al fine di ridurre il predetto rischio, si rende necessario procedere a una chiara identificazione dei soggetti intestatari degli strumenti di pagamento aziendali diversi dal contante, delle modalità di autorizzazione dei pagamenti e, in caso di utilizzazione di tali strumenti da parte di soggetti non intestatari, prevedere il conferimento di una delega con istruzioni chiare e ambito di operatività preciso per gli utilizzatori.

Con riferimento alla condotta di falsificazione o alterazione degli strumenti o dei documenti diversi dal contante (ivi compresi gli strumenti immateriali, quali denaro elettronico, valuta virtuale e pagamenti realizzati attraverso telefoni cellulari) ovvero il possesso, la cessione o l'acquisto di strumenti di pagamento diversi dal contante di provenienza illecita, si rileva che, ai fini della responsabilità dell'ente, appare rischiosa non solo l'azione intenzionale di falsificazione, ma anche, ad esempio, la "colposa" detenzione o cessione, attuata cioè senza operare, nel dubbio sull'autenticità o sulla provenienza degli strumenti di pagamento, le opportune verifiche. In tale ultimo caso, benché la fattispecie di reato punisca soltanto la condotta sorretta dal dolo, il rischio deriva dalla possibilità per l'ente di essere coinvolto nella fattispecie criminosa commessa da soggetti terzi,

qualora venga in possesso, anche se non dolosamente, di strumenti di pagamento diversi dal contante di provenienza illecita.

Al fine di ridurre tale rischio, si rende necessario prevedere presidi sul controllo dell'autenticità e della provenienza degli strumenti di pagamento trattati (con riferimento a tale ultimo aspetto, i presìdi da adottare saranno equivalenti a quelli previsti dalla normativa antiriciclaggio), con riferimento, soprattutto, a clientela occasionale e/o ad operazioni di rilevanti entità.

Il presente reato potrebbe configurarsi anche in caso di rilascio ai clienti di strumenti di pagamento diversi dal contante falsificati o alterati oppure in caso di indebito utilizzo di tali strumenti da parte dei dipendenti della banca. Un presidio utile per ridurre il rischio di commissione di tali condotte è rappresentato dal costante monitoraggio e dalla tracciabilità degli strumenti di pagamento diversi dal contante gestiti dalla banca.

Il reato di frode informatica (art. 640-ter c.p.) potrebbe invece configurarsi quando un dipendente, alterando in qualsiasi modo il funzionamento del sistema informatico o telematico, o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi, procura un ingiusto profitto alla Banca a danno di un ente pubblico o a rilevanza pubblica, quali ad es. l'Agenzia delle Entrate o la Banca d'Italia.

In via esemplificativa: accedere abusivamente al proprio sistema informatico al fine di alterare e/o cancellare dati e informazioni. Detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico, al fine di acquisire informazioni riservate.

Inoltre, stante l'uso sempre più diffuso della tecnologia informatica, in particolare per l'attività tipica degli scambi sui mercati finanziari che avviene attraverso sistemi totalmente telematici, si potrebbe verificare il rischio di commissione di tale reato. Una probabilità di rischio in tal senso si individua, in particolare, con riferimento allo svolgimento dei servizi di investimento che comportino la custodia e l'amministrazione dei beni della clientela; particolare attenzione va prestata alle attività di negoziazione che vengono svolte tramite interconnessioni telematiche.

Le procedure per attuare un'efficace prevenzione del rischio sopra evidenziato sono essenzialmente di natura tecnologica. Si ritiene che tali procedure possano essere predisposte alla luce delle misure attuate per la protezione dei dati aziendali e personali (e.g. diversi livelli di accesso a tali dati) o di quelle previste per i reati presupposto di cui all'articolo 24-bis.

Carifermo si è dotata di una "Policy di sicurezza dei servizi di pagamento", di una "Policy Sicurezza delle informazioni" e di un "Regolamento sicurezza delle informazioni", di una "Policy di sicurezza per i servizi di pagamento via internet", di una "Policy dei controlli di sicurezza swift", di un "Regolamento per la gestione del sito internet" e di un "Regolamento della Funzione Rischi ICT e Sicurezza", oltre alla procedure previste in materia di antiriciclaggio.

Le modalità operative per la gestione dei processi descritti sono disciplinate nell'ambito della normativa interna, sviluppata ed aggiornata a cura delle Strutture competenti, che costituisce parte integrante e sostanziale del presente protocollo.

Principi generali di controllo

Il sistema di controllo a presidio dei processi sopra descritti si basa sui seguenti fattori:

- <u>Responsabilità definite</u>:
    - la normativa interna individua i soggetti e le Funzioni responsabili dell'attivazione/gestione/controllo dei processi sopra descritti;

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa:
  - i soggetti che esercitano poteri autorizzativi e/o negoziali sono individuati e autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale, dalla "Policy di gestione dei rischi operativi e di sicurezza sui servizi di pagamento" e dal vigente sistema dei poteri e delle deleghe della Banca;
  - sono identificati meccanismi di autenticazione basati sul rischio delle operazioni relativi a strumenti di pagamento diverso dai contanti.
- Segregazione dei compiti tra i differenti soggetti coinvolti nell'attività a rischio reato, in particolare sono attribuite precise responsabilità nel processo di gestione:
  - delle carte di pagamento – comprese le carte di credito aziendali – attraverso la definizione di compiti e controlli specifici in merito alle attività di emissione, consegna, sostituzione, rinnovo, attivazione, revoca, rinuncia o recesso del cliente o del dipendente;
  - degli assegni (rilascio o emissione, gestione dei blocchi procedurali e/o limitazioni al rilascio degli assegni, gestione delle segnalazioni alla Centrale Allarme Interbancaria, gestione degli adempimenti in caso di smarrimento, sottrazione e distruzione degli stessi);
  - dei canali digitali (attivazione del servizio, gestione delle credenziali ivi compresi dei blocchi);
  - delle frodi (monitoraggio dell'operatività anomala o sospetta, blocco precauzionale o definitivo degli strumenti di pagamento, ecc.);
  - dei disconoscimenti dei pagamenti che sono svolte da strutture differenti da quelle incaricate dello sviluppo commerciale dei prodotti / servizi.

- Attività di controllo: il sistema di controllo a presidio dei processi descritti si basa sulla verifica delle disposizioni normative in fase di progettazione di nuovi prodotti e/o servizi collegati a strumenti di pagamento diverso dai contanti e sull'adozione di misure organizzative e tecnologiche:
  - per l'analisi degli eventi intercorsi e delle minacce per la comprensione dei rischi e delle tipologie di frode al fine di incrementare la capacità di rilevazione e prevenzione di fenomeni criminosi;
  - per la gestione della richiesta da parte della clientela di recupero dei meccanismi di autenticazione relativi a strumenti di pagamento diversi dai contanti;
  - per la gestione del magazzino delle carte prepagate, di debito e di servizio e, in particolare, per l'attività periodica di quadratura delle carte e degli eventuali PIN cartacei;
  - per il pagamento degli assegni tratti sulla Banca (identificazione del presentatore, regolarità del titolo e delle firme, esistenza di eventuali blocchi operativi);

Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali:

- al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la Funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito del processo descritto;

- utilizzo di sistemi e strumenti informatici a supporto dell'operatività che garantiscano la registrazione e l'archiviazione dei dati e delle informazioni acquisite nell'ambito del processo descritto.

Principi di comportamento

Le Funzioni della Banca, a qualsiasi titolo coinvolte nelle attività di gestione e di utilizzo degli strumenti di pagamento diversi dai contanti sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

In particolare:

- i soggetti che esercitano poteri autorizzativi (ivi compresi la gestione delle operazioni non autorizzate, delle frodi e dei disconoscimenti) e/o negoziali nella gestione dei rapporti contrattuali devono essere appositamente incaricati;
- qualora sia previsto il coinvolgimento di soggetti terzi/outsourcer nella gestione dei sistemi di pagamento deversi dai contanti, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. 231/2001 e di impegno al suo rispetto;
- tutti i dipendenti devono segnalare immediatamente al proprio Responsabile qualunque tentativo di falsificazione ed indebito utilizzo di strumenti finanziari diversi dai contanti da parte della clientela o di terzi del quale il personale venga a conoscenza. Il Responsabile a sua volta ha l'obbligo di trasmettere la segnalazione ricevuta alla struttura avente funzione di Internal Audit per le valutazioni del caso e gli eventuali adempimenti nei confronti dell'Organismo di Vigilanza.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D.Lgs. 231/2001 e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- utilizzare indebitamente e/o favorire l'utilizzo indebito da parte di terzi che non ne sono titolari di carte di pagamento, ovvero di qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, o comunque di ogni altro strumento di pagamento diverso dai contanti;
- falsificare o alterare gli strumenti di pagamento diversi dai contanti, possedere, cedere o acquisire strumenti di pagamento diversi dai contanti o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi;
- introdursi abusivamente, direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di utilizzare indebitamente, falsificare o alterare strumenti di pagamento diversi dai contanti.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

12 REATI E ILLECITI AMMINISTRATIVI RICONDUCIBILI ALL'ABUSO DI MERCATO (ART.25-SEXIES D.LGS.231/2001)

12.1 Fattispecie di reato

Premessa

Il T.U.F. prevede i reati di "*Abuso di informazioni privilegiate*" e di "*Manipolazione di mercato*", disciplinati rispettivamente agli articoli 184 e 185.

L'art. 187-quinquies del T.U.F. medesimo prevede gli illeciti amministrativi di "Divieto di abuso *di informazioni privilegiate e comunicazione illecita di informazioni privilegiate*" e di "Divieto di *manipolazione del mercato*" le cui condotte sono sostanzialmente identiche a quelle già penalmente punite dai due reati predetti.

La responsabilità dell'Ente nell'interesse del quale siano commesse le due condotte penalmente rilevanti è sancita dal D. Lgs. n. 231/2001 (art. 25-*sexies*) mentre per le due fattispecie di illeciti amministrativi la responsabilità dell'Ente discende dal T.U.F. stesso (art. 187-*quinquies*) che rimanda ai medesimi principi, condizioni ed esenzioni del D. Lgs. n. 231/2001, salvo stabilire che per questi illeciti amministrativi la responsabilità dell'Ente sussiste in ogni caso in cui lo stesso non riesca a fornire la prova che l'autore dell'illecito ha agito esclusivamente nell'interesse proprio o di un terzo.

Le predette norme mirano a garantire l'integrità, la trasparenza, la correttezza e l'efficienza dei mercati finanziari in ottemperanza al principio per cui tutti gli investitori debbono operare in condizioni di uguaglianza sotto il profilo dell'accesso all'informazione, della conoscenza del meccanismo di fissazione del prezzo e della conoscenza delle origini delle informazioni pubbliche.

Circa il dettaglio delle fattispecie delittuose previste dall'articolo 25-sexies del Decreto si rimanda all'allegato "Elenco Reati".

In considerazione degli obblighi posti in capo alla Banca, Carifermo ha adottato il "Regolamento per la prevenzione e la gestione degli abusi di mercato" quale codice di comportamento operante all'interno dell'azienda, il quale si pone a presidio dei rischi reato oggetto della presente Parte Speciale. Al predetto Regolamento, si affiancano il Codice Etico, la "Policy per la gestione delle operazioni personali dei soggetti rilevanti" e le "Politiche per la gestione dei rischi finanziari".

A tal fine si precisa che, per:

- abuso di mercato: si devono intendere le condotte illecite nei mercati finanziari, con ciò intendendo abuso di informazioni privilegiate, comunicazione illecita di informazioni privilegiate e manipolazione del mercato;

- informazioni rilevanti: si devono intendere quei tipi di informazione che l'emittente ritiene rilevanti, in quanto relativi a dati, eventi, progetti o circostanze che, in modo continuativo, ripetitivo, periodico, oppure saltuario, occasionale o imprevisto, riguardano direttamente l'emittente stesso e che possono assumere natura privilegiata;

- specifiche informazioni rilevanti: si devono intendere le singole informazioni che rientrano nei tipi di informazioni rilevanti e che, a giudizio dell'emittente, risultano effettivamente rilevanti in quanto possono assumere natura privilegiata;

- informazione privilegiata: si deve intendere un'informazione avente carattere preciso che non è stata resa pubblica, concernente direttamente o indirettamente uno o più emittenti o uno o più

strumenti finanziari e che, se resa pubblica, potrebbe avere un effetto significativo sui prezzi di tali strumenti o sui prezzi di strumenti finanziari collegati;

- raccomandazioni di investimento: si intendono le informazioni destinate al pubblico o ai canali di distribuzione, volti implicitamente o esplicitamente a raccomandare o a consigliare una strategia di investimento in relazione ad uno o più strumenti finanziari o emittenti, ivi compresi pareri sul valore o sul prezzo presenti o futuri di tali strumenti;

- segnalazioni di ordini o operazioni sospette: si intendono segnalazioni degli ordini o operazioni sospette che potrebbero costituire abuso di informazioni privilegiate, manipolazione di mercato, compresa qualsiasi cancellazione o modifica degli stessi;

- sistema multilaterale di negoziazione: si intende un sistema multilaterale gestito da un'impresa di investimento o da un gestore del mercato che consente l'incontro, al suo interno e in base a regole non discrezionali, di interessi multipli di acquisto e di vendita di terzi relativi a strumenti finanziari, in modo da dare luogo a contratti conformemente al titolo II della direttiva UE 65/2014 MiFID II.

12.2 Attività aziendali sensibili

Le attività sensibili identificate dal Modello nelle quali è maggiore il rischio che siano posti in essere i reati ed illeciti amministrativi riconducibili ad abusi di mercato sono le seguenti:

- Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato;
- Gestione degli ordini e delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato.

Le operazioni sottoposte alla disciplina degli abusi di mercato sono quelle, effettuate dalla Banca nell'ambito della prestazione di un servizio di investimento e dell'operatività del portafoglio di proprietà, che hanno per oggetto strumenti finanziari "quotati" o "quotandi" su un mercato regolamentato, un MTF (sistema multilaterale di negoziazione) ovvero OTF (sistema organizzato di negoziazione) di un Paese UE, nonché agli strumenti il cui prezzo dipende o ha un effetto sui prezzi di uno dei citati strumenti.

Si riportano di seguito, per ognuna delle sopraelencate attività sensibili, i protocolli che dettano i principi generali di controllo ed i principi di comportamento applicabili a dette attività e che si completano con la normativa aziendale di dettaglio che regolamenta le attività medesime ("Regolamento per la prevenzione e la gestione degli abusi di mercato").

La disciplina di cui alle presenti disposizioni interne si applica a qualsiasi operazione, ordine di compravendita o condotta relativi agli strumenti finanziari come sopra identificati, indipendentemente dal fatto che tale operazione, ordine di compravendita o condotta avvenga in una sede di negoziazione.

Le disposizioni relative alla manipolazione del mercato si applicano anche ai contratti a pronti su merci (e ai derivati che hanno un effetto sul prezzo di questi) e alle condotte in relazione agli indici di riferimento (benchmark).

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio da outsourcer esterni.

Sono escluse dall'ambito di applicazione della disciplina le operazioni aventi per oggetto le obbligazioni, non quotate ovvero non ammesse su alcun MTF, emesse dalla Banca.

12.2.1 Gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato

Premessa

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, in attività connesse alla gestione e divulgazione delle informazioni e delle comunicazioni esterne ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato, come anche meglio descritto nel "Regolamento per la prevenzione e la gestione degli abusi di mercato".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio dei processi descritti si basa sui seguenti fattori:

Livelli autorizzativi definiti nell'ambito di ciascuna fase operative:

- Istituzione di un registro delle persone che hanno accesso, nell'ambito della propria attività lavorativa, a informazioni privilegiate che riguardano emittenti quotati ed eventualmente soggetti che controllano gli stessi;
- individuazione di soggetti/strutture/funzioni responsabili della gestione del predetto registro;
- nell'ambito della normativa interna sono definite le responsabilità relative alla gestione degli obblighi in materia di market abuse;
- la normativa interna individua la struttura responsabile del presidio della comunicazione istituzionale, interna ed esterna, e del coordinamento di tutte le strutture/funzioni coinvolte in tale attività.

Segregazione dei compiti tra i differenti soggetti coinvolti nell'attività a rischio reato, in particolare:

- adozione di separazione funzionale e logistica tra le strutture/funzioni organizzative che possono avere accesso a informazioni privilegiate nell'ambito delle proprie attività lavorative e quelle che prestano servizi e attività di investimento;
- i soggetti che eseguono attività nell'ambito della gestione degli obblighi in materia di market abuse sono differenti rispetto ai soggetti che le autorizzano.

Attività di controllo:

- implementazione di sistemi di sicurezza logica e fisica a garanzia della corretta gestione delle informazioni;
- implementazione di un'applicazione informatica per l'identificazione di operazione che possano configurare abuso di informazioni privilegiate. Eventuali operazioni evidenziate da tali dati diagnostici sono analizzate dalle strutture competenti, individuate nella Direzione Amministrazione e, ove necessario con il supporto della Funzione Compliance e/o di altre strutture/funzioni;

Tracciabilità delle attività sia a livello di sistema informatico sia in termini documentali, in particolare sono previste modalità di trasmissione, conservazione e archiviazione della documentazione contenente informazioni confidenziali o privilegiate volte a garantirne la riservatezza.

Regolamentazione: è formalizzata specifica regolamentazione che descrive le soluzioni e le metodologie adottate dalla Banca per individuare e segnalare eventuali operazioni sospette di abuso di informazioni privilegiate o di manipolazione del mercato.

Principi di comportamento

Le Strutture della Banca, come pure i singoli dipendenti e collaboratori, a qualsiasi titolo coinvolti nelle attività di gestione e divulgazione delle informazioni privilegiate, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

In particolare è vietato:

- è vietato compiere operazioni su strumenti finanziari della Banca e di Società terze in rapporto d'affari con la Banca stessa, in relazione alle quali si posseggano informazioni privilegiate circa l'emittente o il titolo stesso conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse; tale divieto si applica a qualsiasi tipo di operazione in strumenti finanziari (ad esempio: azioni, obbligazioni, warrant, covered warrant, opzioni, futures);
- è vietato comunicare le medesime informazioni a terzi per ragioni diverse da quelle di ufficio (a titolo esemplificativo e non esaustivo: clienti, emittenti di titoli pubblicamente contrattati, ecc.) ovvero raccomandare o indurre terzi a compiere operazioni connesse alle informazioni privilegiate; qualora dette informazioni debbano essere comunicate a terzi per ragioni d'ufficio, è fatto obbligo di accertare che costoro siano soggetti ad un obbligo di riservatezza legale, regolamentare, statutario o contrattuale; in difetto è necessario formalizzare mediante sottoscrizione di specifici accordi di confidenzialità, il reciproco dovere di riservatezza circa le informazioni scambiate.
- è vietato discutere informazioni privilegiate in luoghi pubblici o in locali in cui siano presenti estranei o comunque soggetti che non hanno necessità di conoscere tali informazioni; si deve porre particolare attenzione nell'uso di telefoni cellulari e di telefoni "viva voce";
- è vietato comunicare al mercato o ai media informazioni privilegiate relative alle società clienti della Banca. Qualora fosse richiesto un commento su specifiche operazioni relative a tali emittenti, ci si dovrà limitare a commentare i fatti già resi pubblici dall'emittente in base all'art. 114 del T.U.F.; in ogni caso sono previsti obblighi di consultazione con le strutture/funzioni aziendali che sono legittimamente in possesso delle informazioni privilegiate.
- è vietato diffondere sia ad altro personale sia all'esterno della Banca, attraverso qualsiasi canale informativo, compreso internet, informazioni, voci o notizie non corrispondenti alla realtà, ovvero informazioni di cui non sia certa la veridicità, capaci, o anche solo potenzialmente suscettibili, di fornire indicazioni false o fuorvianti in relazione alla Banca e/o ai relativi strumenti finanziari nonché in relazione a Società terze in rapporto d'affari con la Banca e ai relativi strumenti finanziari;
- è vietato produrre e diffondere studi e ricerche o altre comunicazioni di marketing in violazione delle norme, interne ed esterne, specificamente dettate per tale attività e, in particolare, senza comunicare nei modi richiesti dalla normativa gli interessi rilevanti e/o i conflitti eventualmente sussistenti;

E' fatto obbligo:

- è fatto obbligo di mantenere riservate tutte le informazioni e i documenti acquisiti nello svolgimento delle proprie funzioni, sia aventi ad oggetto la Banca e gli strumenti finanziari della stessa, sia riguardanti Società terze in rapporto d'affari con la Banca e gli strumenti finanziari di queste ultime nonché di utilizzare le informazioni o i documenti stessi esclusivamente per l'espletamento dei propri compiti lavorativi;
- è fatto obbligo, secondo quanto stabilito dalle norme interne in tema di sicurezza fisica e logica di custodire accuratamente documenti contenenti informazioni confidenziali e riservate, di assicurarsi che le proprie password rimangano segrete e che il proprio computer sia adeguatamente protetto attraverso il blocco temporaneo dello stesso nei momenti in cui ci si allontana dalla propria postazione. Si evidenzia inoltre che:
    - l'attività di produzione dei documenti (quali, ad esempio, stampa e fotocopiatura di documenti) contenenti informazioni privilegiate deve essere presidiata da personale a ciò abilitato;
    - i documenti in oggetto devono essere classificati come "confidenziali", "riservati" o, ove possibile, utilizzando nomi in codice per salvaguardare la natura dell'informazione in essi contenuta; l'accesso a informazioni confidenziali e riservate, quando elaborate/trattate/trasmesse/archiviate in formato elettronico, deve essere regolato tramite inserimento di password o, per le Strutture che ne siano fornite, mediante l'apposito applicativo di crittografia;
    - i supporti recanti informazioni confidenziali e riservate devono essere custoditi in locali ad accesso fisico controllato, ovvero riposti in archivi custoditi o protetti al termine del loro utilizzo e non devono mai essere lasciati incustoditi, particolarmente quando portati all'esterno delle sedi di lavoro;
    - la distruzione dei supporti recanti informazioni confidenziali e riservate deve avvenire a cura degli stessi soggetti che ne dispongono, con le modalità più idonee ad evitare ogni improprio recupero del contenuto informativo.

E' possibile diffondere le informazioni privilegiate nell'ambito delle strutture/funzioni della Banca solo nei riguardi di coloro che abbiano effettiva necessità di conoscerla per motivi attinenti al normale esercizio del lavoro, evidenziando la natura riservata delle informazioni.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

12.2.2 Gestione delle operazioni di mercato ai fini della prevenzione degli illeciti penali e amministrativi in tema di abusi di mercato

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, come anche meglio descritto nel "Regolamento per la prevenzione e la gestione degli abusi di mercato", nella gestione delle attività inerenti la gestione degli ordini e delle operazioni di mercato su strumenti finanziari.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi di controllo

Il sistema di controllo a presidio del processo descritto si basa sui seguenti fattori:

Livelli autorizzativi definiti e in particolare approvazione da parte degli Organi competenti in base al vigente sistema dei poteri e delle deleghe:

- delle linee guida per la gestione del portafoglio titoli immobilizzati e non immobilizzati della Banca;
- del perimetro operativo per l'effettuazione delle operazioni di negoziazione sui mercati in termini di compravendita titoli;
- delle delibere volte all'autorizzazione degli investimenti/disinvestimenti partecipativi;
- di limiti operativi in funzione dell'anzianità e del grado del personale interessato.

Separatezza organizzativa tra le strutture che hanno a disposizione delle informazioni privilegiate (con particolare riferimento a quelle che gestiscono la relazione commerciale con la clientela corporate, che svolgono attività di erogazione e gestione del credito e prestazione di servizi di finanza aziendale, che gestiscono le società partecipate) rispetto alle strutture che hanno rapporti diretti con il mercato.

Attività di controllo sulle operazioni di compravendita titoli eseguite attraverso un sistema di controlli differenziato che tenga conto delle diverse tipologie di strumenti finanziari trattati e della specificità del mercato di riferimento.

Tracciabilità del processo sia a livello di sistema informativo sia in termini documentali: in particolare, le operazioni di compravendita titoli sono gestite attraverso sistemi applicativi dedicati, nei quali sono mantenuti tutti i dettagli delle transazioni effettuate.

Regolamentazione: è formalizzata specifica regolamentazione che descrive le soluzioni e le metodologie adottate dalla Banca per individuare e segnalare eventuali operazioni sospette di abuso di informazioni privilegiate o di manipolazione del mercato.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione di patrimoni dei clienti ovvero in attività di trading, per conto proprio della Banca o di terzi, attraverso la negoziazione ed il regolamento di operazioni sui mercati, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna, con particolare riferimento alle "Politiche per la gestione dei rischi finanziari", al Regolamento Market Abuse, al Regolamento delle operazioni con soggetti collegati, che si intendono qui richiamati, nonché le eventuali previsioni del Codice Etico.

In particolare è fatto divieto di:

- porre in essere operazioni simulate o altri artifizi concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari;
- compiere operazioni o impartire ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
- compiere operazioni o ordini di compravendita che consentano, anche tramite l'azione di concerto di più persone, di fissare il prezzo di mercato di strumenti finanziari ad un livello anomalo o artificiale;

- compiere operazioni od ordini di compravendita che utilizzano artifizi od ogni altro tipo di inganno di espediente;
- utilizzare altri artifizi idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

Sono vietati i seguenti comportamenti, salvo nei casi e con le procedure previste dalla vigente normativa:

- eseguire operazioni o impartire ordini di compravendita che rappresentano una quota significativa del volume giornaliero degli scambi dello strumento finanziario pertinente nel mercato interessato, in particolare quando tali ordini o operazioni conducono ad una significativa variazione del prezzo dello strumento finanziario;
- eseguire operazioni o impartire ordini di compravendita avendo una significativa posizione in acquisto o in vendita su uno strumento finanziario che conducono a significative variazioni del prezzo dello strumento finanziario o dello strumento derivato collegato o dell'attività sottostante;
- eseguire operazioni che non determinano alcuna variazione nella proprietà ovvero non comportano alcun trasferimento effettivo della proprietà di uno strumento finanziario;
- eseguire operazioni o impartire ordini di compravendita che prevedono inversioni di posizione in acquisto o in vendita nel breve periodo e rappresentano una quota significativa del volume giornaliero di scambi dello strumento finanziario nel mercato interessato e possono associarsi a significative variazioni del prezzo di uno strumento finanziario;
- eseguire operazioni o impartire ordini di compravendita concentrati in un breve lasso di tempo nel corso della sessione di negoziazione che conducano a una variazione del prezzo che successivamente si inverte;
- impartire ordini di compravendita che modificano la rappresentazione dei migliori prezzi delle proposte di acquisto o di vendita di uno strumento finanziario o, più in generale, modificano la rappresentazione del book di negoziazione a disposizione dei partecipanti al mercato, e sono revocati prima della loro esecuzione;
- eseguire operazioni o impartire ordini nei momenti o intorno ai momenti utili per il calcolo dei prezzi delle aste di apertura o di chiusura, dei prezzi di controllo, dei prezzi di riferimento, dei prezzi di regolamento o di valutazione di strumenti finanziari, conducendo a variazioni di tali prezzi;
- eseguire operazioni o impartire ordini di compravendita facendo precedere o seguire dette operazioni dalla diffusione, anche per il tramite di persone collegate, di informazioni false o fuorvianti;
- eseguire operazioni o impartire ordini di compravendita prima o dopo avere elaborato o diffuso, anche per il tramite di persone collegate, ricerche o raccomandazioni di investimento errate o tendenziose o manifestamente influenzate da interessi rilevanti.

I Responsabili delle Strutture interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

13 REATI IN MATERIA DI SALUTE E SICUREZZA SUI LUOGHI DI LAVORO (Art.25-SEPTIES D.LGS.231/2001)

13.1 Fattispecie di reato

Premessa

La presente "Parte Speciale" è volta a presidiare il rischio di commissione dei reati di cui all'art. 25 septies del D.Lgs. n. 231/2001.

In particolare, si elencano di seguito le fattispecie di reato identificate quali rilevanti, in relazione all'operatività della Banca, nell'ambito della presente Parte Speciale:

- Omicidio colposo (Art. 589 c.p.);
- Lesioni personali colpose (Art. 590 co. 3 c.p.).

Circa il dettaglio delle fattispecie delittuose previste dall'articolo 25-septies del Decreto si rimanda all'allegato "Elenco Reati".

L'art. 25-*septies* del Decreto prevede tra gli illeciti presupposto della responsabilità degli Enti i delitti di omicidio colposo e di lesioni colpose gravi o gravissime, se commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

Il Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro, (D. Lgs. 9 aprile 2008 n. 81) ha profondamente riordinato le molteplici fonti normative previgenti in materia e all'art. 30 ha esplicitato le caratteristiche che deve presentare il Modello di organizzazione, gestione e controllo al fine della prevenzione dei reati in esame.

Finalità delle citate disposizioni è quella di fornire più efficaci mezzi di prevenzione e repressione in relazione al fenomeno degli incidenti sul lavoro ed alla esigenza di tutela dell'integrità psicofisica dei lavoratori e della sicurezza degli ambienti lavorativi.

13.2 Attività aziendali sensibili

La tutela della salute e della sicurezza sul lavoro è materia che pervade ogni ambito ed attività aziendale.

Costituiscono situazioni di particolare attenzione, in riferimento alle suddette fattispecie di reato, le attività connesse alla gestione degli adempimenti in materia di salute e sicurezza sul lavoro ("Testo Unico della Sicurezza"). A titolo esemplificativo e non esaustivo:

- identificazione dei rischi in materia di salute e sicurezza sul lavoro, loro classificazione e valutazione;
- individuazione e predisposizione delle misure di prevenzione e di protezione, definizione e successiva implementazione di un piano di intervento con l'identificazione delle strutture aziendali competenti all'attuazione di detti interventi;
- verifica sull'attuazione e controllo sull'efficacia delle misure adottate;
- adempimenti connessi alla gestione dei contratti di appalto, contratti d'opera, contratti di somministrazione (verifica dell'idoneità tecnico professionale delle imprese e dei lavoratori autonomi, informativa alla controparte circa i rischi specifici presenti nei luoghi in cui è chiamata ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla attività oggetto del contratto, predisposizione del Documento di Valutazione dei Rischi

Interferenziali (DUVRI), controllo sul rispetto degli adempimenti contrattuali nell'esecuzione delle attività, ecc.).

Si riporta qui di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia di salute e sicurezza sul lavoro. Tale protocollo si completa con la normativa aziendale di dettaglio vigente in argomento.

Detto protocollo si applica anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, da outsourcer esterni.

Gestione dei rischi in materia di salute e sicurezza sui luoghi di lavoro

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, nell'attività inerente la gestione dei rischi in materia di salute e sicurezza sui luoghi di lavoro.

La gestione dei rischi in materia di salute e sicurezza sul lavoro riguarda qualunque tipologia di attività finalizzata a sviluppare ed assicurare un sistema di prevenzione e protezione dei rischi esistenti sul luogo di lavoro, in ottemperanza a quanto previsto dal D.Lgs. n. 81/2008 (di seguito Testo Unico).

Si rammenta anzitutto che, ai sensi del Testo Unico compete al Datore di lavoro la responsabilità per la definizione della politica aziendale riguardante la salute e la sicurezza dei lavoratori sul luogo di lavoro e/o ai suoi delegati, per le materie delegabili.

In ottemperanza a quanto disposto dalla predetta normativa la Banca adotta e tiene aggiornato i "Documenti di Valutazione dei Rischi" (un DVR per ciascuna sede/Filiale), che contengono:

- la valutazione dei rischi per la sicurezza e la salute durante l'attività lavorativa;
- l'individuazione delle misure di prevenzione e protezione poste a tutela dei lavoratori ed il programma delle misure ritenute opportune per garantire il miglioramento nel tempo del livello di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
- l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, dei rappresentanti dei lavoratori per la sicurezza e dei medici competenti che hanno partecipato alla valutazione del rischio;
- l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

Tali Documenti sono redatti in conformità alla normativa vigente. A tal fine il Documento di Valutazione dei Rischi individua, all'interno dell'organizzazione aziendale, le responsabilità, le procedure, i processi e le risorse per la realizzazione della propria politica di prevenzione nel rispetto delle norme di salute e sicurezza vigenti. Nel medesimo Documento vengono descritte le modalità specifiche con le quali l'organizzazione risponde ai requisiti delle predette Linee Guida e sono esplicitati i processi operativi ed i documenti societari atti a garantire l'adempimento di quanto previsto dall'art. 30 – Modelli di organizzazione e di gestione – del D. Lgs. 81/2008.

Le Strutture aziendali incaricate della gestione della documentazione inerente la materia, quali autorizzazioni/certificazioni/nullaosta rilasciati dalla Pubblica Amministrazione, sono tenute al rispetto

dei principi di comportamento stabiliti e descritti nel protocollo “Gestione delle attività inerenti la richiesta di concessioni, autorizzazioni, licenze o l’esecuzione di adempimenti verso la Pubblica Amministrazione”.

. Le linee d’azione generali della Banca devono essere orientate verso un costante miglioramento della qualità della sicurezza e devono contribuire allo sviluppo effettivo di un “sistema di prevenzione e protezione”. Tutte le Strutture della Banca devono osservare le disposizioni in materia di salute, di sicurezza e di igiene del lavoro e tenerne conto in occasione di qualsivoglia modifica degli assetti esistenti, compresi ristrutturazioni/allestimenti di siti operativi.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio del processo descritto si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell’ambito del processo:
  - i soggetti che esercitano poteri autorizzativi e/o negoziali sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dalla normativa interna e dal vigente sistema dei poteri e delle deleghe della Banca;
  - adozione di una politica aziendale di salute e sicurezza quale valore aziendale che caratterizza la strategia di impresa da conseguire ed implementare, con l’ausilio di un sistema organizzativo che ne individui, in particolare, gli strumenti, le procedure e le responsabilità;
  - il sistema di gestione aziendale prevede la definizione di specifiche responsabilità e procedure al fine di consentire la piena attuazione della politica di salute e sicurezza sul lavoro con un approccio sistematico e pianificato. In particolare, è stata individuata la figura aziendale che riveste il ruolo di “Datore di Lavoro”. Tali figure possono impartire disposizioni in materia alle Strutture aziendali, godono della più ampia autonomia organizzativa e dispongono di adeguati e congrui poteri di spesa, anche con facoltà di delega e subdelega ai sensi dell’art. 16 comma 3 *bis* del Testo Unico;
  - è prevista un'articolazione di distinte funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
  - tutti i soggetti/figure aziendali che intervengono nelle fasi del processo sopra descritto devono essere individuati e autorizzati con espressa previsione della normativa interna o tramite delega, da conferirsi e conservarsi a cura del Datore di Lavoro, ovvero a cura dei soggetti facoltizzati.
- Segregazione dei compiti tra i differenti soggetti/figure aziendali coinvolte nel processo di gestione dei rischi in materia di salute e sicurezza sul lavoro. In particolare:
  - il Datore di Lavoro, in qualità di principale garante della sicurezza all’interno della Banca, è tenuto agli obblighi indicati nell’art. 18 del Testo Unico, avvalendosi anche dell’istituto della delega di funzioni ai sensi dell’art. dall’art. 16 del Testo Unico, fatta eccezione per l’attività indelegabili;

- il Responsabile del Servizio Prevenzione e Protezione coordina le strutture operative che hanno il compito di realizzare e gestire gli interventi (di natura immobiliare, di sicurezza fisica, ovvero attinenti a processi di lavoro e alla gestione del personale), che sono distinte e separate dalla struttura alla quale sono attribuiti compiti di consulenza in tema di valutazione dei rischi e di controllo sulle misure atte a prevenirli e a ridurli;
- le strutture operative che hanno il compito di realizzare e di gestire gli interventi sono distinte e separate dalla Struttura alla quale, per legge e/o normativa interna, sono attribuiti compiti di consulenza in tema di valutazione dei rischi e di controllo sulle misure atte a prevenirli e a ridurli;
- le strutture competenti designano i soggetti ai quali sono attribuite specifiche mansioni per la gestione/prevenzione dei rischi per la sicurezza e la salute sul lavoro;
- i Rappresentanti dei Lavoratori per la Sicurezza, laddove eletti, collaborano attivamente col Datore di Lavoro al fine di segnalare criticità ed individuare le conseguenti soluzioni.

- Attività di controllo:
  - previsione di idonee attività di gestione del rischio attraverso:
    - individuazione e determinazione delle misure di prevenzione e protezione e dei dispositivi di protezione individuale;
    - individuazione di procedure per l'attuazione delle misure e di figure aziendali coinvolte in questo processo;
    - programmazione delle misure più idonee a garantire il miglioramento nel tempo dei livelli di sicurezza;
    - individuazione ed organizzazione delle procedure di emergenza e di primo soccorso.
  - le strutture competenti devono attivare un piano aziendale di controllo sistematico al fine di verificare periodicamente la corretta applicazione/gestione nonché l'efficacia delle procedure adottate e delle misure messe in atto per valutare, in ottemperanza alle prescrizioni di legge, i luoghi di lavoro. Il piano, in particolare, deve contemplare:
    - aree e attività aziendali da verificare (tra le quali le attività di natura organizzativa, di sorveglianza sanitaria, di informazione e formazione dei lavoratori, di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori);
    - modalità di esecuzione delle verifiche, modalità di rendicontazione.

    Il piano aziendale deve altresì assicurare:
    - il rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
    - l'acquisizione di documentazioni e certificazioni obbligatorie di legge (relative ad edifici, impianti persone, società ecc.) da parte delle competenti strutture;
    - il rispetto del processo e degli adempimenti tecnici ed amministrativi previsti dalle normative interne e di legge;

- deve inoltre prevedere un idoneo sistema di controllo sulla sua efficace attuazione e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate.

- tutti gli ambienti di lavoro sono visitati e valutati da soggetti in possesso dei requisiti di legge e di adeguata formazione tecnica. Il Medico Competente ed il Responsabile del Servizio Prevenzione e Protezione visitano i luoghi di lavoro;
- pianificazione delle attività di informazione e di formazione previste dalla normativa vigente.

- Tracciabilità del processo sia a livello di sistema informativo, sia in termini documentali:
  - al fine di consentire la ricostruzione delle responsabilità, deve dotarsi di idonei sistemi di registrazione dell'avvenuta effettuazione delle attività, ed è responsabile dell'archiviazione e della conservazione dei contratti stipulati nonché di tutta la documentazione prodotta anche in via telematica o elettronica, inerente alla esecuzione degli adempimenti svolti nell'ambito delle attività proprie del processo della gestione dei rischi in materia di sicurezza e salute dei lavoratori nonché della relativa attività di controllo, ivi compresa l'acquisizione, la conservazione e l'archiviazione di documentazioni e certificazioni obbligatorie di legge.

Principi di comportamento

Le Funzioni della Banca e i dipendenti, a qualsiasi titolo coinvolte nella gestione dei rischi in materia di salute e sicurezza sul lavoro, sono tenuti ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

In particolare, tutte le Funzioni/figure sono tenute – nei rispettivi ambiti - a:

- assicurare, per quanto di competenza, gli adempimenti in materia di sicurezza e salute dei lavoratori sul luogo di lavoro osservando le misure generali di tutela;
- astenersi dall'affidare incarichi a consulenti esterni eludendo criteri documentabili ed obiettivi quali professionalità e competenza, competitività, prezzo, integrità e capacità di garantire un'efficace assistenza. In particolare, le regole per la scelta devono ispirarsi ai criteri di chiarezza e documentabilità;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es. Ispettorato del Lavoro, A.S.L., Vigili del Fuoco, ecc.) in occasione di accertamenti/procedimenti ispettivi;
- provvedere, nell'ambito dei contratti di appalto, d'opera o di fornitura, ad informare le controparti sui rischi specifici dell'ambiente in cui sono destinate ad operare e ad elaborare ed applicare le misure atte a governare in sicurezza le eventuali interferenze fra le imprese, compresi gli eventuali lavoratori autonomi, evidenziando nei contratti per i quali sia prescritto i costi per la sicurezza;
- favorire e promuovere l'informazione e formazione interna in tema di rischi connessi allo svolgimento delle attività, misure ed attività di prevenzione e protezione adottate, procedure di pronto soccorso, lotta antincendio ed evacuazione dei lavoratori;
- curare il rispetto delle normative in tema di salute e sicurezza nei confronti di tutto il personale;

- osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dalle Funzioni aziendali e dalle Autorità competenti;
- segnalare immediatamente al proprio responsabile e/o agli addetti alla gestione delle emergenze, ogni situazione di pericolo potenziale o reale, adoperandosi, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre tale situazione di pericolo;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia di salute e sicurezza sul lavoro, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

14 REATI INFORMATICI (Art.24-BIS D.LGS.231/2001)

14.1 Fattispecie di reato

Premessa

La presente “Parte Speciale” è volta a presidiare il rischio di commissione dei reati informatici e relativi al trattamento illecito di dati di cui all’art. 24 bis del D.Lgs. 231/2001.

In particolare, si elencano di seguito le fattispecie di reato identificate quali rilevanti, in relazione all’operatività della Banca, nell’ambito della presente Parte Speciale:

- falsità in documenti informatici (art. 491-bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all’accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);
- distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici (art. 635-bis c.p.);
- distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità (art. 635-ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art.640-quinquies c.p.);
- violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art.1 comma 11 D.L.105/2019).

Circa il dettaglio delle fattispecie delittuose previste dall’articolo 24-bis del Decreto si rimanda all’allegato “Elenco Reati”.

La legge 18.3.2008 n. 48, entrata in vigore il 5.4.2008, ha introdotto nell’ordinamento italiano una serie di nuove fattispecie di reato che possono essere commesse attraverso un illecito utilizzo di documenti informatici e/o di sistemi informatici. Tale legge ha altresì introdotto una nuova fattispecie di reato al D.Lgs.231/2001, l’articolo 24-bis che estende agli Enti la responsabilità amministrativa per i reati informatici.

La natura informatica che qualifica questi reati può riguardare le modalità di realizzazione della condotta, il suo oggetto materiale, il bene giuridico tutelato o la natura dei mezzi di prova.

Preliminarmente, al fine di agevolare la lettura delle norme contenute nell'allegato "Elenco dei reati presupposto", di seguito vengono fornite le definizioni di sistema informatico e di documento informatico:

- "sistema informatico": qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, eseguono l'elaborazione automatica dei dati;
- "dato informatico": qualunque rappresentazione di fatti, informazioni o concetti in forma idonea per l'elaborazione con un sistema informatico, incluso un programma in grado di consentire ad un sistema informatico di svolgere una funzione.

14.2 Attività aziendali sensibili

Le attività della Banca nelle quali possono essere commessi i reati informatici e trattati in modo illecito i dati aziendali informatici sono proprie di ogni ambito aziendale che utilizza le tecnologie dell'informazione.

La Banca ha predisposto appositi presidi organizzativi e si è dotata di adeguate soluzioni di sicurezza, in conformità alle disposizioni di Vigilanza ed alla normativa europea e nazionale in materia di protezione dei dati personali, per prevenire e controllare i rischi in tema di tecnologia dell'informazione (IT) e di Cybersecurity, a tutela del proprio patrimonio informativo, della clientela e dei terzi.

L'attività sensibile identificata dal Modello nella quale è maggiore il rischio che siano posti in essere i comportamenti illeciti come sopra descritti è la:

- Gestione e utilizzo dei sistemi informativi della Banca.

Si riporta di seguito il protocollo che detta i principi di controllo ed i principi di comportamento applicabili a detta attività e che si completa con la normativa aziendale di dettaglio che regolamenta l'attività medesima.

Carifermo si è dotata di una "Policy sulla sicurezza informatica", di una "Policy di sicurezza per i servizi di pagamento via internet", di una "Policy dei controlli di sicurezza swift", di un "Regolamento per la gestione e l'aggiornamento del sito web" e di un "Regolamento della Funzione Rischi ICT e Sicurezza". Specifiche disposizioni volte ad accrescere la sicurezza dei sistemi sono inoltre contenute nella "Data protection policy" e nel "Regolamento Privacy", che regolamenta, tra l'altro, l'attività degli amministratori di sistema e l'attribuzione dei privilegi di accesso ai dati nel rispetto della normativa in materia di protezione dei dati personali.

È stato definito inoltre il "Piano di continuità operativa (BCP) volto a garantire la disponibilità dei dati e sistemi in caso di crisi.

Il protocollo si applica anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, da outsourcer esterni.

14.2.1 Gestione e utilizzo dei sistemi informativi della Banca

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, nell'attività inerente alla Gestione e l'utilizzo dei sistemi informativi della Banca.

In particolare, si applica a:

- tutte le Funzioni della Banca coinvolte nella gestione e l'utilizzo dei sistemi informativi che si interconnettono/utilizzano software della Pubblica Amministrazione ovvero delle Autorità di Vigilanza;
- tutte le Funzioni deputate alla progettazione, alla realizzazione o gestione di strumenti informatici, tecnologici o di telecomunicazioni;
- tutte le Funzioni che hanno la responsabilità di realizzare interventi di tipo organizzativo, normativo e tecnologico per garantire la protezione del sistema informatico;
- tutte le figure professionali coinvolte nei processi aziendali e ivi operanti a qualsiasi titolo, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale, che utilizzano i sistemi informativi della Banca e trattano i dati della stessa.

Ai sensi del D.Lgs. n. 231/2001, i relativi processi potrebbero presentare occasioni per la commissione di uno dei delitti informatici contemplati dall'art. 24-*bis*; inoltre, mediante l'accesso alle reti informatiche potrebbero essere integrate le condotte illecite aventi ad oggetto le opere dell'ingegno protette.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi generali di controllo

Fatti salvi i requisiti di sicurezza propri del software della Pubblica Amministrazione o delle Autorità di Vigilanza utilizzato dalla Banca, il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito di ciascuna fase operativa caratteristica dei processi sopra descritti, in particolare:
  - la gestione delle abilitazioni avviene tramite la definizione di "profili di accesso" in ragione delle funzioni svolte all'interno della Banca;
  - le variazioni al contenuto dei profili sono eseguite da Amministratori di sistema nominati in conformità al Provvedimento del Garante Privacy come individuate nel Regolamento Privacy e nel Regolamento della funzione Rischi ICT e Sicurezza, su richiesta delle Funzioni interessate. La Funzione richiedente deve comunque garantire che le abilitazioni informatiche richieste corrispondano alle mansioni lavorative coperte;
  - ad ogni utente sono associati profili abilitativi in relazione al proprio ruolo aziendale nel rispetto del principio del minimo privilegio. In caso di trasferimento o di modifica dell'attività dell'utente, viene attribuito il profilo abilitativo corrispondente al nuovo ruolo assegnato;
- Segregazione dei compiti
  - sono assegnati distinti ruoli e responsabilità di gestione della sicurezza delle informazioni;

- le attività di implementazione e modifica dei software, gestione delle procedure informatiche, controllo degli accessi fisici, logici e della sicurezza del software sono organizzativamente demandate a strutture differenti rispetto agli utenti, a garanzia della corretta gestione e del presidio continuativo sul processo di gestione e utilizzo dei sistemi informativi;
- sono attribuite precise responsabilità per garantire che il processo di sviluppo, manutenzione e gestione delle applicazioni, effettuato internamente o presso terzi, sia gestito in modo controllato e verificabile attraverso un opportuno iter autorizzativo.

- Attività di controllo:
  - le attività di gestione ed utilizzo dei sistemi informativi della Banca sono soggette ad una costante attività di controllo che si esplica sia attraverso l'utilizzo di adeguate misure per la protezione delle informazioni, salvaguardandone la riservatezza, l'integrità e la disponibilità con particolare riferimento al trattamento dei dati personali, sia tramite l'adozione, per l'insieme dei processi aziendali, di specifiche soluzioni di continuità operativa di tipo tecnologico, organizzativo e infrastrutturale che assicurino la predetta continuità anche a fronte di situazioni di emergenza;
  - le attività di controllo costituiscono valido presidio anche a garanzia della tracciabilità delle modifiche apportate alle procedure informatiche, della rilevazione degli utenti che hanno effettuato tali modifiche e di coloro che hanno effettuato i controlli sulle modifiche apportate;
  - con riferimento alla sicurezza fisica: protezione e controllo delle aree fisiche (perimetri/zone riservate) in modo da scongiurare accessi non autorizzati, alterazione o sottrazione degli asset informativi;
  - con riferimento alla sicurezza logica: identificazione e autenticazione dei codici identificativi degli utenti; autorizzazione relativa agli accessi alle informazioni richiesti; previsione di tecniche crittografiche e di firma digitale per garantire la riservatezza, l'integrità e il non ripudio delle informazioni archiviate o trasmesse;
  - con riferimento all'esercizio ed alla gestione di applicazioni, sistemi e reti: previsione di una separazione degli ambienti (sviluppo, collaudo e produzione) nei quali i sistemi e le applicazioni sono installati, gestiti e manutenuti in modo tale da garantire nel tempo la loro integrità e disponibilità; predisposizione e protezione della documentazione di sistema relativa alle configurazioni, personalizzazioni e procedure operative, funzionale ad un corretto e sicuro svolgimento delle attività; previsione di misure per le applicazioni in produzione in termini di installazione, gestione dell'esercizio e delle emergenze, protezione del codice, che assicurino il mantenimento della riservatezza, dell'integrità e della disponibilità delle informazioni trattate; attuazione di interventi di rimozione di sistemi, applicazioni e reti individuati come obsoleti; pianificazione e gestione dei salvataggi di sistemi operativi, software, dati e delle configurazioni di sistema; gestione delle apparecchiature e dei supporti di memorizzazione per garantire nel tempo la loro integrità e disponibilità tramite la regolamentazione ed il controllo sull'utilizzo degli strumenti, delle apparecchiature e di ogni asset informativo in dotazione nonché mediante la definizione di modalità di custodia, riutilizzo, riproduzione, distruzione e trasporto fisico dei supporti rimuovibili di memorizzazione delle informazioni, al fine di proteggerli da danneggiamenti, furti o accessi non autorizzati;

- monitoraggio di applicazioni e sistemi, tramite la definizione di efficaci criteri di raccolta e di analisi dei dati relativi, al fine di consentire l'individuazione e la prevenzione di azioni non conformi;
- prevenzione da software dannoso tramite sia opportuni strumenti ed infrastrutture adeguate (tra cui i sistemi antivirus) sia l'individuazione di responsabilità e procedure per le fasi di installazione, verifica di nuovi rilasci, aggiornamenti e modalità di intervento nel caso si riscontrasse la presenza di software potenzialmente dannoso;
- formalizzazione di responsabilità, processi, strumenti e modalità per lo scambio delle informazioni tramite posta elettronica e siti web;
- adozione di opportune contromisure per rendere sicura la rete di telecomunicazione e gli apparati a supporto e garantire la corretta e sicura circolazione delle informazioni;
- previsione di specifiche procedure per le fasi di progettazione, sviluppo e cambiamento dei sistemi e delle reti, definendo i criteri di accettazione delle soluzioni;
- previsione di specifiche procedure per garantire che l'utilizzo di materiali eventualmente coperti da diritti di proprietà intellettuale sia conforme alle disposizioni di legge e contrattuali;
- con riferimento allo sviluppo ed alla manutenzione delle applicazioni: individuazione di opportune contromisure ed adeguati controlli per la protezione delle informazioni gestite dalle applicazioni, che soddisfino i requisiti di riservatezza, integrità e disponibilità delle informazioni trattate, in funzione degli ambiti e delle modalità di utilizzo, dell'integrazione con i sistemi esistenti e del rispetto delle disposizioni di Legge e della normativa interna; previsione di adeguati controlli di sicurezza nel processo di sviluppo delle applicazioni, al fine di garantirne il corretto funzionamento anche con riferimento agli accessi alle sole persone autorizzate, mediante strumenti, esterni all'applicazione, per l'identificazione, l'autenticazione e l'autorizzazione;
- con riferimento alla gestione degli incidenti di sicurezza: previsione di opportuni canali e modalità di comunicazione per la tempestiva segnalazione di incidenti e situazioni sospette al fine di minimizzare il danno generato, prevenire il ripetersi di comportamenti inadeguati e attivare l'eventuale escalation che può condurre anche all'apertura di uno stato di crisi;
- controlli sulla correttezza delle comunicazioni con particolare riguardo al rispetto dei termini previsti per l'invio delle informazioni, comunicazioni e segnalazioni di incidenti.

- <u>Tracciabilità del processo</u> sia a livello di sistema informativo sia in termini documentali:
  - in generale, al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la struttura/funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica;
  - il processo decisionale, con riferimento all'attività di gestione e utilizzo di sistemi informatici, è garantito dalla completa tracciabilità a sistema;
  - tutti gli eventi e le attività effettuate (tra le quali gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, ad esempio rettifiche contabili, variazioni dei profili

utente, ecc.), con particolare riguardo all'operato di utenze con privilegi speciali, risultano tracciate attraverso sistematica registrazione (sistema di log files);

- è prevista la tracciatura, ove tecnicamente possibile, delle attività effettuate sui dati, compatibili con le leggi vigenti al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate.

Principi di comportamento

Le Funzioni della Banca, a qualsiasi titolo coinvolte nelle attività di gestione e utilizzo di sistemi informatici e del Patrimonio Informativo sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

In particolare:

- i soggetti coinvolti nel processo devono essere appositamente incaricati;
- ogni dipendente/amministratore del sistema è tenuto alla segnalazione alla Funzione di Sicurezza Informatica aziendale e, nel caso risultino trattamenti illeciti o violazioni di dati personali, al Responsabile della Protezione Dati (DPO),di eventuali incidenti di sicurezza (anche concernenti attacchi al sistema informatico da parte di hacker esterni) mettendo a disposizione e archiviando tutta la documentazione relativa all'incidente;
- ogni dipendente è responsabile del corretto utilizzo delle risorse informatiche a lui assegnate (es. personal computer fissi o portatili), che devono essere utilizzate esclusivamente per l'espletamento della propria attività. Tali risorse devono essere conservate in modo appropriato e la Banca dovrà essere tempestivamente informata di eventuali furti o danneggiamenti;
- qualora sia previsto il coinvolgimento di soggetti terzi/outsourcer nella gestione e utilizzo dei sistemi informatici e nell'utilizzo dei software della Pubblica Amministrazione o delle Autorità di Vigilanza, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;
- non è consentito riconoscere compensi in favore di collaboratori o consulenti esterni che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere o svolto.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001 e, più in particolare, a titolo meramente esemplificativo e non esaustivo:

- introdursi abusivamente, direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Banca, o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;

- utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, worm, troian, spyware, dialer, keylogger, rootkit, ecc.) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;
- detenere, procurarsi, riprodurre o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;
- porre in essere mediante l'accesso alle reti informatiche condotte illecite costituenti violazioni di diritti sulle opere dell'ingegno protette;
- importare, promuovere, installare, porre in vendita, modificare o utilizzare, apparati di decodificazione di trasmissioni audiovisive ad accesso condizionato, anche se ricevibili gratuitamente.
- omettere di comunicare entro i termini prescritti dalla normativa vigente in materia di "sicurezza nazionale cibernetica" dati, informazioni o elementi di fatto rilevanti;
- esibire documenti e dati incompleti e/o comunicare dati falsi o alterati nell'ambito delle comunicazioni in materia di "sicurezza nazionale cibernetica".

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e di comportamento descritti nel presente protocollo.

15 REATI CONTRO L'INDUSTRIA E IL COMMERCIO (ART.25-BIS.1 D.LGS.231/2001)

15.1 Fattispecie di reato

Premessa

La presente "Parte Speciale" è volta a presidiare il rischio di commissione dei reati di cui all'art. 25 bis.1 del D.Lgs. 231/2001.

In particolare, si elencano di seguito le fattispecie di reato identificate quali rilevanti, in relazione all'operatività della Banca, la fattispecie di reato identificata come rilevante nell'ambito della presente Parte Speciale è l'"Illecita concorrenza con minaccia o violenza" (art. 513 bis c.p.);

Circa il dettaglio delle fattispecie delittuose previste dall'articolo 25-bis.1 del Decreto si rimanda all'allegato "Elenco Reati".

15.2 Attività aziendali sensibili

Con riferimento all'operatività bancaria, i rischi di commissione dei reati contro l'industria ed il commercio più verosimilmente possono presentarsi:

- "Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione;
- "Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose";
- "Gestione di omaggi, liberalità, spese di rappresentanza, beneficenze e sponsorizzazioni";
- "Gestione e utilizzo dei sistemi informativi della Banca";

In rifermento alla "Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), il rischio di commissione reati potrebbe riguardare con riferimento ai reati di "Illecita concorrenza con minaccia o violenza", ad esempio potenziali condotte suscettibili di condizionare il corretto svolgimento delle gare indette a finalità commerciali da clienti/potenziali clienti.

In riferimento alle predette attività, si rimanda alle attività a rischio-reato già oggetto di trattazione nella Parte Speciale "Reati contro la Pubblica Amministrazione" e alle attività a rischio oggetto di trattazione nella Parte Speciale "Reati informatici", ove sono qualificati principi generali di controllo e principi di comportamento aventi efficacia anche a presidio dei reati di cui alla presente Parte Speciale.

La conoscenza della clientela rappresenta una componente rilevante ai fini del presidio dei rischi reato in esame e rappresenta uno dei principali adempimenti disposti dalla normativa antiriciclaggio; a tal fine si rimanda, per l'esposizione di tali presidi organizzativi all'attività a rischio reato "Gestione degli adempimenti in materia di contrasto al riciclaggio e al finanziamento del terrorismo".

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio da outsourcer esterni.

16 REATI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ART. 25-NOVIES D.LGS.231/2001)

16.1 Fattispecie di reato

Premessa

La presente "Parte Speciale" è volta a presidiare il rischio di commissione dei reati di cui all'art. 25 novies del D.Lgs. 231/2001.

Circa il dettaglio delle fattispecie delittuose previste dall'articolo 25-novies del Decreto si rimanda all'allegato "Elenco Reati".

L'art. 25-*novies* - al fine di contrastare ancor più severamente la pirateria delle opere dell'ingegno e i gravi danni economici arrecati agli autori e all'industria connessa – rimanda a reati contemplati dalla legge sul diritto d'autore (L. n. 633/1941).

16.2 Attività aziendali sensibili

Costituiscono situazioni di particolare attenzione, in riferimento alle suddette fattispecie di reato, le seguenti attività:

- "Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione;
- "Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze;
- "Gestione e utilizzo dei sistemi informativi della Banca";
- "Gestione del sito internet e dei canali social della Banca";
- "Produzione materiale pubblicitario".

In rifermento alla "Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione il rischio di commissione dei reati in oggetto potrebbe riguardare ad esempio il processo di erogazione del credito, ove la Banca favorisse clienti coinvolti in condotte riconducibili alle fattispecie in oggetto.

In riferimento alla "Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze", il rischio di commissione dei reati in oggetto potrebbe configurarsi ad esempio in concorso con fornitori di beni/servizi eventualmente coinvolti nelle attività delittuose contemplate nelle fattispecie in oggetto (ad esempio laddove la Banca acquisti da tali fornitori beni che violano la disciplina in tema di protezione dei titoli di proprietà industriale e del diritto d'autore).

In riferimento alle predette attività, si rimanda alle attività a rischio-reato già oggetto di trattazione nella Parte Speciale "Reati contro la Pubblica Amministrazione" e alle attività a rischio oggetto di trattazione nella Parte Speciale "Reati informatici", ove sono qualificati principi generali di controllo e principi di comportamento aventi efficacia anche a presidio dei reati di cui alla presente Parte Speciale.

La conoscenza della clientela rappresenta una componente rilevante ai fini del presidio dei rischi reato in esame e rappresenta uno dei principali adempimenti disposti dalla normativa antiriciclaggio; a tal fine si rimanda, per l'esposizione di tali presidi organizzativi all'attività a rischio reato "Gestione degli adempimenti in materia di contrasto al riciclaggio e al finanziamento del terrorismo".

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio da outsourcer esterni.

17 REATI AMBIENTALI (ART. 25-UNDECIES D.LGS.231/2001)

17.1 Fattispecie di reato

Premessa

La presente "Parte Speciale" è volta a presidiare il rischio di commissione dei reati di cui all'art. 25 undecies D.Lgs. 231/2001.

In particolare, si elencano di seguito le fattispecie di reato identificate quali rilevanti, in relazione all'operatività della Banca, la fattispecie di reato identificata quale rilevante nell'ambito della presente Parte Speciale è la "Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari" (art. 258 D.Lgs.152/2006).

Circa il dettaglio delle fattispecie delittuose previste dall'articolo 25-undecies del Decreto si rimanda all'allegato "Elenco Reati".

L'art. 25-*undecies* del D.Lgs. n. 231/01 individua gli illeciti dai quali, nella materia della tutela penale dell'ambiente, fondata su disposizioni di matrice comunitaria, discende la responsabilità amministrativa degli enti.

Si tratta di reati descritti nel codice penale, nel D.Lgs. n. 152/06 (Codice dell'ambiente) e in varie leggi speciali, sia di natura delittuosa sia di tipo contravvenzionale.

17.2 Attività aziendali sensibili

Con riferimento all'operatività bancaria, i rischi di commissione dei reati ambientali possono presentarsi ad esempio più verosimilmente nei rapporti con la clientela, con riguardo alla concessione di finanziamenti o alla prestazione di servizi a favore di soggetti coinvolti nelle attività illecite in questione.

Si riporta qui di seguito il protocollo che detta i principi di controllo e i principi di comportamento applicabili alla gestione dei rischi in materia ambientale. Tale protocollo si completa con la normativa aziendale di dettaglio che regolamenta l'attività medesima, in particolare si fa riferimento alle seguenti attività:

- Gestione dei rischi in materia ambientale;
- Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (promotori finanziari e partner commerciali), inclusi gli Enti della Pubblica Amministrazione;
- Gestione delle attività inerenti la richiesta di concessioni, autorizzazioni, licenze o l'esecuzione di adempimenti verso la Pubblica Amministrazione;
- Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze;

In riferimento alla Stipula e gestione dei rapporti contrattuali con la clientela e le controparti, inclusi gli Enti della Pubblica Amministrazione, il rischio di commissione reati riguarda ad esempio il processo di erogazione del credito. Il rischio in cui potrebbe incorrere la Banca consiste nella possibilità di favorire clienti coinvolti in condotte riconducibili alle fattispecie di reato richiamate.

In riferimento alla Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze, la potenziale commissione dei reati da parte della Banca potrebbe configurarsi in concorso con soggetti eventualmente coinvolti nelle attività delittuose contemplate nelle fattispecie in oggetto, laddove la Banca, ad esempio, nel proprio interesse o vantaggio supporti a vario titolo

tali soggetti (a titolo esemplificativo, attraverso la selezione di fornitori di beni/servizi implicati in tali attività).

Per tutte le attività sopra individuate si rimanda alle attività a rischio reato già oggetto di trattazione nella Parte Speciale "Reati contro la Pubblica Amministrazione", che contengono principi di controllo e principi di comportamento diretti a prevenire anche la commissione dei reati di cui al presente paragrafo.

Con riferimento al rischio di commissione dei reati in oggetto in concorso con la clientela, si precisa che la conoscenza della clientela rappresenta uno dei principali adempimenti disposti dalla normativa in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose, si rimanda pertanto al protocollo "Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose".

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio, da outsourcer esterni.

Gestione dei rischi in materia ambientale

Premessa

Il presente protocollo si applica a tutti i Destinatari del Modello coinvolti, a qualsiasi titolo, nell'attività inerente la gestione dei rischi in materia ambientale.

Le Funzioni aziendali incaricate della gestione della documentazione inerente la materia ambientale, quali autorizzazioni e certificazioni rilasciate dalla Pubblica Amministrazione, sono tenute al rispetto dei principi di comportamento stabiliti e descritti nel protocollo "Gestione delle attività inerenti la richiesta di concessioni, autorizzazioni, licenze o l'esecuzione di adempimenti verso la Pubblica Amministrazione".

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell'esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell'ambito del processo:
    - i soggetti che esercitano poteri autorizzativi e/o negoziali nell'ambito delle attività a rischio-reato, sono individuati e autorizzati in base allo specifico ruolo attribuito loro dalla normativa interna e dal vigente sistema di poteri e deleghe della Banca;
    - per quanto attiene l'acquisto di beni e servizi, l'approvazione della richiesta di acquisto, il conferimento dell'incarico, il perfezionamento del contratto e l'emissione dell'ordine spettano esclusivamente a soggetti muniti di idonee facoltà in base al sistema di poteri e deleghe in essere;
    - sono individuati e formalmente incaricati i responsabili delle attività di gestione dei rifiuti con espressa assunzione in capo agli stessi delle relative responsabilità;
    - l'eventuale affidamento a terzi - da parte dei fornitori della Banca - di attività in sub-appalto, è contrattualmente subordinato a un preventivo assenso da parte della struttura

della Banca che ha stipulato il contratto ed al rispetto degli specifici obblighi sul rispetto della normativa ambientale.

- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi di gestione dei rischi in materia ambientale. In particolare:
    - le Strutture operative che hanno il compito di realizzare e di gestire gli interventi quali servizi alle persone, servizi all'edificio, manutenzioni edili, opere edilizie/impiantistiche ed altri servizi integrati (es.: fornitura toner, gestione infermerie, gestione delle apparecchiature di informatica distribuita, verifica/ricondizionamento/smaltimento dei materiali o prodotti informatici, ecc.) sono distinte e separate dalle Strutture alle quali sono attribuiti compiti di consulenza in tema di valutazione dei rischi ambientali e di controllo sulle misure atte a prevenirli e a ridurli;
- Attività di controllo:
    - attività di verifica periodica, nell'ambito della revisione dei contratti con fornitori terzi in scadenza, circa la validità delle certificazioni/autorizzazioni richieste ai fornitori incaricati per lo svolgimento delle attività di smaltimento dei rifiuti;
    - controllo sul corretto espletamento, da parte dei fornitori, dei servizi di manutenzione/pulizia (servizi all'edificio, servizi alle persone, ecc.) degli immobili, con particolare riguardo alla regolare tenuta dei libretti d'impianto per la climatizzazione
- Tracciabilità del processo sia a livello di sistema informativo, sia in termini documentali:
    - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la struttura/funzione di volta in volta interessata è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica;
    - utilizzo di sistemi informatici a supporto dell'operatività, che garantiscono la registrazione e l'archiviazione dei dati e delle informazioni inerenti al processo acquisitivo;
    - documentabilità di ogni attività inerente ai processi;
    - conservazione nei termini di legge (cinque anni dall'ultima registrazione) del formulario d'identificazione dei rifiuti speciali, ove presenti, e del registro di carico e scarico dei rifiuti pericolosi, ove presente.

Principi di comportamento

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione dei rischi in materia ambientale oggetto del protocollo come pure tutti i dipendenti, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico.

In particolare, tutte le Strutture sono tenute – nei rispettivi ambiti - a:

- vigilare, per quanto di competenza, sul rispetto degli adempimenti in materia ambientale;
- segnalare immediatamente al Responsabile e/o agli addetti alla gestione delle emergenze, qualsiasi situazione di emergenza ambientale;
- osservare le disposizioni di legge, la normativa interna e le istruzioni impartite dalle Strutture aziendali e dalle Autorità competenti;

- prevedere, nell'ambito dei contratti di appalto, d'opera e di fornitura di servizi alle persone, servizi all'edificio, manutenzioni edili, opere edilizie/impiantistiche ed altri servizi integrati (es.: fornitura toner, gestione infermerie, gestione delle apparecchiature di informatica distribuita, verifica/ricondizionamento/smaltimento dei materiali o prodotti informatici, ecc.) specifiche clausole sul rispetto della normativa ambientale;
- nell'ambito delle procedure acquisitive di prodotti, macchine e attrezzature a fini strumentali che a fine ciclo vita potrebbero essere classificati potenzialmente pericolosi per l'ambiente, le Strutture committenti e la funzione acquisti competente devono ottenere preventivamente dal potenziale fornitore la "scheda di sicurezza/pericolosità del prodotto" ed il codice CER e tutte le informazioni necessarie per il corretto smaltimento degli stessi;
- considerare come requisito rilevante per la valutazione del fornitore, ove la natura della fornitura lo renda possibile e opportuno, le certificazioni ambientali;
- adottare una condotta trasparente e collaborativa nei confronti degli Enti preposti al controllo (es, A.S.L., Vigili del Fuoco, ARPA, Comune, Provincia, ecc.) in occasione di accertamenti / procedimenti ispettivi;
- qualora sia previsto il coinvolgimento di soggetti terzi nella gestione/prevenzione dei rischi in materia ambientale, i contratti con tali soggetti devono contenere apposita dichiarazione di conoscenza della normativa di cui al D. Lgs. n. 231/2001 e di impegno al suo rispetto;

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre gli Enti pubblici in errore.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

18 REATI TRIBUTARI (ART.25-QUINQUIESDECIES D.LGS.231/2001)

18.1 Fattispecie di reato

Premessa

La Legge 19 dicembre 2019, n. 157 (pubblicata in G.U. il 24 dicembre 2019) ha convertito con emendamenti il D.L. 26 ottobre 2019, n.124 recante "Disposizioni urgenti in materia fiscale e per esigenze indifferibili" e ha introdotto nel D.L.gs 231/2001 l'art. 25-quinquiesdecies rubricato "Reati tributari" che espressamente prevede la responsabilità amministrativa dell'ente per i delitti in materia di dichiarazioni, nel dettaglio: dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs.74/2000), dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs.74/2000); e i delitti in materia di documenti e pagamento di imposte: emissione di fatture per operazioni inesistenti (art. 8 D.Lgs.74/2000), occultamento o distruzione di documenti contabili (art. 10 D.Lgs.74/2000) e sottrazione fraudolenta al pagamento delle imposte (art. 11 D.Lgs.74/2000).

La responsabilità degli enti è estesa ad alcuni dei reati in materia di imposte sui redditi e sul valore aggiunto previsti dal D. Lgs. n. 74/2000, che detta la disciplina di portata generale sui reati tributari, riformata per rafforzare la repressione del fenomeno dell'evasione fiscale.

Il Decreto Legislativo 14 luglio 2020, n.75 ha introdotto nuovi reati, in particolare: dichiarazione infedele (art.4 D.Lgs.74/2000), omessa dichiarazione (art.5 D.Lgs.74/2000) e indebita compensazione (art.10-quater D.Lgs.74/2000), limitando la punibilità degli enti per questi specifici reati, solo se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a 10 milioni di euro.

Le nuove fattispecie in materia tributaria sono state inserite nell'articolo 25-quinquiesdecies (reati tributari).

In particolare, si elencano di seguito le fattispecie di reato identificate quali rilevanti, in relazione all'operatività della Banca, nell'ambito della presente Parte Speciale:

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art.2 D.Lgs.74/2000);
- Dichiarazione fraudolenta mediante altri artifici (art.3 D.Lgs.74/2000);
- Emissione di fatture o altri documenti per operazioni inesistenti (art.8 D.Lgs.74/2000);
- Occultamento o distruzione di documenti contabili (art.10 D.Lgs.74/2000);
- Sottrazione fraudolenta al pagamento di imposte (art.11 D.Lgs.74/2000);
- Dichiarazione infedele (art.4 D.Lgs.74/2000);
- Omessa dichiarazione (art.5 D.Lgs.74/2000);
- Indebita compensazione (art.10-quater D.Lgs.74/2000).

Circa il dettaglio delle fattispecie delittuose previste dall'articolo 25-quinquiesdecies del Decreto si rimanda all'allegato "Elenco Reati".

18.2 Attività aziendali sensibili

Il rischio di commissione dei reati tributari può presentarsi in ogni attività aziendale. Esso è specificamente presidiato dal protocollo "Gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari".

Carifermo si è dotata di una “Manuale di controllo dei conti di contabilità generale”, di specifiche disposizioni relative agli “Adempimenti contabili e amministrativi di fine anno” e di una “Policy in materia di partecipazioni detenibili”

Per quanto riguarda la posizione di contribuente della Banca, tale rischio è inoltre presidiato dal protocollo “Operazioni di rilevazione, registrazione e rappresentazione dell’attività di impresa nelle scritture contabili, nell’informativa periodica, nei bilanci, nelle relazioni sulla gestione e in altri documenti di impresa”.

Per quanto riguarda i rapporti con i terzi, quali clienti, fornitori, partner e controparti in genere al fine di mitigare il rischio di essere coinvolta in illeciti fiscali dei medesimi, considerato anche che la legge, ai sensi dell’art. 13 bis del D. Lgs. n. 74/2000, punisce più severamente gli intermediari bancari e finanziari che concorrono nell’elaborazione o nella commercializzazione di modelli di evasione fiscale, la Banca ha altresì predisposto i protocolli che disciplinano le seguenti attività:

- Gestione degli acquisti di beni e servizi, degli incarichi professionali e delle consulenze;
- Gestione di omaggi, liberalità, spese di rappresentanza, beneficienze e sponsorizzazioni;
- Gestione degli adempimenti in materia di contrasto al riciclaggio e al finanziamento al terrorismo;

Tali protocolli contengono principi di controllo e di comportamento da rispettare anche ai fini della prevenzione dei reati fiscali.

Con riferimento alla gestione del rischio fiscale relativo a prodotti e servizi offerti alla clientela, che riguardano fattispecie in cui si potrebbe configurare un potenziale coinvolgimento della Banca in operazioni fiscalmente irregolari della clientela, vengono effettuate specifiche verifiche nel corso del processo di approvazione dei prodotti.

Detti protocolli si applicano anche a presidio delle attività eventualmente svolte, sulla base di appositi contratti di servizio da outsourcer esterni.

18.2.1 Gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari

Il presente protocollo si applica a tutte le strutture della Banca coinvolte nella gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari.

Ai sensi del D. Lgs. n. 231/2001, il processo potrebbe presentare occasioni per la commissione dei reati tributari elencati in precedenza.

Inoltre, le regole aziendali e i controlli di completezza e di veridicità previsti nel presente protocollo sono predisposti anche al fine di una più ampia azione preventiva dei reati che potrebbero conseguire a una scorretta gestione delle risorse finanziarie, quali i reati “*Riciclaggio*” e di “*Autoriciclaggio*”.

Quanto definito dal presente protocollo è volto a garantire il rispetto, da parte della Banca, della normativa vigente e dei principi di trasparenza, correttezza, oggettività e tracciabilità nell’esecuzione delle attività in oggetto.

Principi generali di controllo

Il sistema di controllo a presidio dei processi descritti si deve basare sui seguenti fattori:

- Livelli autorizzativi definiti nell’ambito del processo, in particolare:

- tutti i soggetti che intervengono nella gestione delle attività inerenti alla predisposizione delle dichiarazioni fiscali, e nelle prodromiche attività di emissione / contabilizzazione delle fatture sono individuati ed autorizzati in base allo specifico ruolo attribuito loro dal funzionigramma aziendale ovvero dal Responsabile della di riferimento tramite delega interna, da conservare a cura Banca;
- nel caso in cui intervengano consulenti esterni/fornitori, questi ultimi vengono individuati con lettera di incarico/nomina ovvero nelle clausole contrattuali; operano esclusivamente nell'ambito del perimetro di attività loro assegnato dal Responsabile di riferimento; ogni accordo/convenzione con l'Agenzia delle Entrate è formalizzato in un documento, debitamente firmato da soggetti muniti di idonei poteri in base al sistema dei poteri e delle deleghe in essere;

- Segregazione dei compiti tra i differenti soggetti coinvolti nei processi di gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari. In particolare le attività di cui alle diverse fasi del processo devono essere svolte da attori/soggetti differenti chiaramente identificabili e devono essere supportate da un meccanismo di *maker* e *checker;*
- Attività di controllo:
  - controlli di completezza, correttezza ed accuratezza delle informazioni trasmesse alle autorità fiscali da parte della Funzione interessata per le attività di competenza che devono essere supportate da meccanismi di *maker* e *checker*;
  - controlli di carattere giuridico sulla conformità alla normativa di riferimento della dichiarazione fiscale;
  - controlli continuativi automatici di sistema, con riferimento alle dichiarazioni periodiche;
  - controlli sulla corretta emissione, applicazione delle aliquote IVA e contabilizzazione delle fatture del ciclo attivo e sulla loro corrispondenza con i contratti e impegni posti in essere con i terzi;
  - controlli sull'effettività, sia dal punto di vista soggettivo che oggettivo, del rapporto sottostante alle fatture passive ricevute e sulla corretta registrazione e contabilizzazione.
- Tracciabilità del processo sia a livello di sistema informativo, sia in termini documentali:
  - ciascuna fase rilevante del processo di gestione del rischio e degli adempimenti ai fini della prevenzione dei reati tributari deve risultare da apposita documentazione scritta;
  - al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, ciascuna struttura è responsabile dell'archiviazione e della conservazione della documentazione di competenza prodotta anche in via telematica o elettronica.

Principi di comportamento

Le Funzioni della Banca, a qualsiasi titolo coinvolte nella gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari oggetto del protocollo come pure tutti i dipendenti, sono tenute ad osservare le modalità esposte nel presente protocollo, le disposizioni di legge esistenti in materia, la normativa interna nonché le eventuali previsioni del Codice Etico e della normativa interna adottata. In particolare, tutte le Strutture sono tenute – nei rispettivi ambiti - a:

- garantire la corretta e veritiera rappresentazione dei risultati economici, patrimoniali e finanziari della Banca nelle dichiarazioni fiscali;

- rispettare i principi di condotta in materia fiscale al fine di: (i) garantire nel tempo la conformità alle regole fiscali e tributarie e, (ii) l'integrità patrimoniale e la reputazione della Società;
- agire secondo i valori dell'onestà e dell'integrità nella gestione della variabile fiscale, nella consapevolezza che il gettito derivante dai tributi costituisce una delle principali fonti di contribuzione allo sviluppo economico e sociale;
- garantire la diffusione di una cultura aziendale improntata ai valori di onestà e integrità e al principio di legalità;
- mantenere un rapporto collaborativo e trasparente con l'Autorità Fiscale garantendo a quest'ultima, tra l'altro, la piena comprensione dei fatti sottesi all'applicazione delle norme fiscali;
- eseguire gli adempimenti fiscali nei tempi e nei modi definiti dalla normativa o dall'autorità fiscale;
- evitare forme di pianificazione fiscale che possano essere giudicate aggressive da parte delle autorità fiscali;
- interpretare le norme in modo conforme al loro spirito e al loro scopo;
- rappresentare gli atti, i fatti e i negozi intrapresi in modo da rendere applicabili forme di imposizione fiscale conformi alla reale sostanza economica delle operazioni;
- garantire trasparenza alla propria operatività e alla determinazione dei propri redditi e patrimoni evitando l'utilizzo di strutture, anche di natura societaria, che possano occultare l'effettivo beneficiario dei flussi reddituali o il detentore finale dei beni;
- rispettare le diposizioni atte a garantire idonei prezzi di trasferimento per le operazioni infragruppo con la finalità di allocare, in modo conforme alla legge, i redditi generati;
- collaborare con le autorità competenti per fornire in modo veritiero e completo le informazioni necessarie per l'adempimento e il controllo degli obblighi fiscali;
- stabilire rapporti di cooperazione con le amministrazioni fiscali, ispirati alla trasparenza e fiducia reciproca e volti a prevenire i conflitti, riducendo quindi la possibilità di controversie;
- proporre alla clientela prodotti e servizi che non consentano di conseguire indebiti vantaggi fiscali non altrimenti ottenibili, prevedendo inoltre idonee forme di presidio per evitare il coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela.

In ogni caso è fatto divieto di porre in essere/collaborare/dare causa alla realizzazione di comportamenti che possano rientrare nelle fattispecie di reato considerate ai fini del D. Lgs. n. 231/2001, e più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- esibire documenti incompleti e/o comunicare dati falsi o alterati;
- tenere una condotta ingannevole che possa indurre le Autorità Fiscali in errore;
- procedere con il pagamento di una fattura senza verificare preventivamente l'effettività, la qualità, la congruità e tempestività della prestazione ricevuta e l'adempimento di tutte le obbligazioni assunte dalla controparte;
- utilizzare strutture o società artificiose, non correlate all'attività imprenditoriale, al solo fine di eludere la normativa fiscale;
- emettere fatture o rilasciare altri documenti per operazioni inesistenti al fine di consentire a terzi di commettere un'evasione fiscale;

- indicare nelle dichiarazioni annuali relative alle imposte sui redditi e sul valore aggiunto: i) elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture, per operazioni inesistenti; ii) elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi (ad esempio costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento; iii) una base imponibile in misura inferiore a quella effettiva attraverso l'esposizione di elementi attivi per un ammontare inferiore a quello reale o di elementi passivi fittizi; iv) fare decorrere inutilmente i termini previsti dalla normativa applicabile per la presentazione delle medesime così come per il successivo versamento delle imposte da esse risultanti.

I Responsabili delle Funzioni interessate sono tenuti a porre in essere tutti gli adempimenti necessari a garantire l'efficacia e la concreta attuazione dei principi di controllo e comportamento descritti nel presente protocollo.

19 AREA SENSIBILE CONCERNENTE I REATI DI CRIMINALITÀ ORGANIZZATA, I REATI DI IMPIEGO DI CITTADINI TERZI IL CUI SOGGIORNO È IRREGOLARE E IL REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA

19.1 Fattispecie di reato

Premessa

Attraverso ripetuti interventi legislativi sono state introdotte nel sistema della responsabilità amministrativa degli Enti varie categorie di illeciti, con la comune finalità di contrastare fenomeni di criminalità che destano particolare allarme a livello internazionale, specie in relazione a reati di matrice politico-terroristica, oppure commessi nei settori e con le forme tipiche della delinquenza organizzata, anche transnazionale, o particolarmente lesivi di fondamentali diritti umani.

Il settore bancario - e con esso la politica della Banca - ha da sempre dedicato particolare attenzione ed impegno nella collaborazione alla prevenzione di fenomeni criminali nel mercato finanziario ed al contrasto al terrorismo, impegno questo che la Banca assume anche ai fini della tutela della sana e prudente gestione, della trasparenza e correttezza dei comportamenti e del buon funzionamento del sistema nel suo complesso. Inoltre, nell'esercizio dell'attività bancaria e finanziaria è di particolare evidenza il rischio di mettere a disposizione di clientela appartenente o comunque contigua alla malavita organizzata servizi, risorse finanziarie o disponibilità economiche che risultino strumentali al perseguimento di attività illecite.

Si fornisce qui di seguito una sintetica esposizione delle categorie di fattispecie in questione.

* * *

Sezione I - Delitti di criminalità organizzata (art.24-ter del D.Lgs.231/2001)

L'art. 24-*ter* del Decreto, inserito dalla L. n. 94/2009, prevede innanzitutto un gruppo di reati inerenti alle varie forme di associazioni criminose, e cioè:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso, anche straniera e scambio elettorale politico-mafioso (artt. 416-*bis* e 416-ter);

Il rischio che siano posti in essere i reati di criminalità organizzata, riguarda principalmente, nell'ambito dell'attività bancaria, le attività di instaurazione dei rapporti con la clientela, di trasferimento di fondi, l'operatività di "sportello" ed, in particolare, il processo di erogazione del credito, attività che, ai fini della prevenzione dei reati in questione, si devono basare sul fondamentale principio dell'adeguata conoscenza della clientela.

In tale ambito più alto è il rischio che si verifichino anche reati di riciclaggio. Pertanto, ai fini della prevenzione dei reati sopra illustrati, sono ritenuti idonei i principi di controllo e di comportamento individuati nel protocollo inerente al contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose.

* * *

Sezione II - Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art.25-duodecies del D.Lgs.231/2001)

L'art.25-duodecies del Decreto punisce, all'art. 22, comma 12-bis, del D. Lgs. n. 286/1998 - Testo Unico sull'immigrazione, i datori di lavoro che assumano o si avvalgano di dipendenti extracomunitari privi di permesso di soggiorno, ovvero scaduto senza che sia richiesto il rinnovo, revocato, o annullato. La responsabilità dell'ente per tale reato, attiguo al reato di sfruttamento di lavoratori clandestini è prevista solo al ricorrere di determinate circostanze aggravanti.

Il rischio di responsabilità per i delitti in questione si può ritenere maggiormente rilevante con riferimento alla selezione e all'assunzione di personale, ovvero all'ipotesi in cui un esponente o un dipendente della Banca agiscano in concorso con l'autore materiale del reato. La forma di concorso che presenta maggiori profili di rischio è quella connessa al finanziamento da parte della Banca in favore di organizzazioni o di soggetti che pongano in essere reati dei tipi sopra menzionati.

Sezione III – Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art.25-decies del D.Lgs.231/2001)

L'art.25-decies del Decreto punisce la fattispecie richiamata nel presente paragrafo. Il delitto è caratterizzato dall'induzione di terzi (chiamati a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, ed aventi la facoltà di non rispondere) a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria attraverso l'offerta o la promessa di denaro o di altra utilità, ovvero l'uso della violenza o della minaccia.

Il reato può rilevare anche come "transnazionale", in presenza dei requisiti di cui alla L. n. 146/2006.

In relazione alle caratteristiche del reato-presupposto sopra descritto si possono ritenere potenzialmente a rischio tutte le aree di attività (in particolare l'attività inerente alla gestione dei contenziosi e degli accordi transattivi) essendo astrattamente possibile in ordine a ciascuna di esse la commissione di fatti da cui possano scaturire condotte di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci.

Circa il dettaglio delle fattispecie delittuose previste nelle Sezioni I, II e III si rimanda all'allegato "Elenco Reati".