MODELLO DI ORGANIZZA-ZIONE E GESTIONE

Delibera del C.d.A. del 24.05.2022

BANCA DELLE TERRE VENETE
GRUPPO BCC ICCREA

INDICE

PARTE GENERALE

PREMESSA

Il presente documento descrive il Modello di Organizzazione e di Gestione di cui al D. Lgs. n. 231/2001 adottato dalla Banca delle Terre Venete, volto a prevenire la realizzazione dei reati previsti dal citato Decreto.

Si tratta di una rivisitazione del Modello esistente, sia nella Parte Generale che in quella Speciale, resasi necessaria sia alla luce delle sopravvenienze legislative (consistite soprattutto nell'ampliamento del catalogo dei reati-presupposto) sia a seguito delle modifiche regolamentari ed organizzative che hanno interessato il mondo del credito cooperativo, in particolare con la nascita del Gruppo Bancario Iccrea, costituito in seguito alla emanazione della Legge n. 49 del 2016 (e successive modifiche), che ha riformato il Sistema del Credito Cooperativo ed ha previsto l'obbligo di adesione delle Banche di Credito Cooperativo ad una Capogruppo formalmente autorizzata dall'Autorità di Vigilanza.

La Banca dal 4.3.2019 è parte del Gruppo Bancario Cooperativo Iccrea a capo del quale vi è la Capogruppo Iccrea Banca S.p.A., che esercita sulla Banca delle Terre Venete i poteri di direzione e coordinamento definiti dal contratto di coesione e garanzia sottoscritto.

Alla necessità di verificare la perdurante idoneità del modello esistente a prevenire i reati previsti anche nell'ambito del gruppo, si è unita l'esigenza di aggiornare ed adattare il modello previgente alla nuova realtà derivante dalla fusione per incorporazione del Credito Trevigiano Banca di Credito Cooperativo nella Cassa Rurale ed Artigiana di Brendola – Credito Cooperativo, intervenuta il 26 ottobre 2020, a seguito della quale l'incorporante ha modificato la propria denominazione sociale in Banca delle Terre Venete Credito Cooperativo – Società Cooperativa.

1. GLOSSARIO

Nel presente documento si intendono per:

- **D. lgs. 231**: 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;
- **Modello 231**: il Modello di Organizzazione e Gestione *ex* art. 6, c. 1, lett. a), del d. lgs. 231/2001, anche definito MOG;
- **Banca**: Banca delle Terre Venete;
- **Soggetti 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). Tali soggetti sono stati identificati nei membri del Consiglio di amministrazione e del Collegio sindacale, nonché nel Direttore;

- **Sottoposti:** le persone sottoposte alla direzione o alla vigilanza dei Soggetti apicali (art. 5, comma 1, lettera b) del d. lgs. n. 231/2001);
- **Destinatari:** Soggetti apicali e Sottoposti;
- **Ente:** soggetto fornito di personalità giuridica, società ed associazioni anche prive di personalità giuridica;
- **Organismo di Vigilanza:** l'organismo dotato di autonomi poteri di vigilanza e controllo cui è affidata la responsabilità di vigilare sul funzionamento e l'osservanza del modello avente i requisiti di cui all'art. 6, comma 1, lettera b) del d. lgs. n. 231/2001, di curarne l'aggiornamento e di ricevere le comunicazioni in forma anche riservata in relazione alle ipotesi di violazione normativa previste dal d. lgs.
- **Regolamento disciplinare:** documento contenente le norme disciplinari applicate dalla Banca;
- **Codice** o **Codice Etico:** Codice Etico adottato dalla Banca;
- **Attività Sensibile:** attività o atto che si colloca nell'ambito delle Aree a Rischio così come identificate nella Parte Speciale;
- **Organi Sociali:** il Consiglio di Amministrazione, il Comitato Esecutivo, il Collegio Sindacale, il Collegio dei Probiviri.

2. LA NORMATIVA DI RIFERIMENTO

2.1. Introduzione

In data 8 giugno 2001, in attuazione della delega di cui all'art. 11 della legge 29 settembre 2000, n. 300, è stato emanato il D. lgs. 231, con cui il legislatore ha dettato la disciplina della responsabilità degli enti per gli illeciti amministrativi dipendenti da reato.

La normativa prevede una responsabilità amministrativa (così testualmente denominata da legislatore) degli enti dotati di personalità giuridica, nonché delle società e delle associazioni prive di personalità giuridica in connessione con la commissione di taluni reati (cd. reati-presupposto), espressamente contemplati in un elenco di carattere tassativo.

Tale forma di responsabilità non è applicabile allo Stato, agli Enti pubblici territoriali, agli altri enti pubblici non economici, nonché agli enti che svolgono funzioni di rilievo costituzionale.

La responsabilità amministrativa degli enti è stata configurata dal legislatore come autonoma rispetto alla responsabilità penale della persona fisica che ha commesso il reato presupposto.

2.2. Gli autori del reato presupposto

La responsabilità in capo all'ente si configura quando il reato presupposto viene commesso da un soggetto che ricopre un ruolo formale all'interno dell'ente.

In particolare, il legislatore individua i seguenti autori:

- soggetti apicali di cui all'art. 5 lett. a): coloro che ricoprono all'interno dell'ente funzioni di rappresentanza, di amministrazione o di direzione o che ne esercitano (anche di fatto) il controllo o la gestione;
- soggetti sottoposti alla direzione o alla vigilanza dei soggetti di cui alla lettera a).

2.3. L'interesse o il vantaggio dell'ente

La normativa specifica che l'ente è responsabile per i reati commessi dai soggetti di cui sopra, solo laddove questi siano stati commessi nell' interesse o a vantaggio dell'ente.

L'interesse deve intendersi come la proiezione finalistica dell'azione realizzata ed è, dunque, un criterio valutabile *ex ante* mentre il vantaggio è il concreto risultato conseguito per effetto della condotta ed è verificabile *ex post*. Affinché possa configurarsi la responsabilità dell'Ente, è sufficiente che sussista uno dei due suddetti elementi.

L'ente, invece, non risponde, se gli autori del reato hanno agito nell'interesse esclusivo proprio o di terzi (art. 5, comma 2, D. Lgs. 231).

2.4. Le fattispecie di reato

La Sezione III del capo I del D. lgs. 231 individua i reati per i quali è configurabile la responsabilità amministrativa degli enti e per ciascuna forma di reato individua il relativo apparato sanzionatorio per l'ente.

Alla data di ultimo aggiornamento del presente documento le categorie di reati richiamate sono:

1. Delitti contro la Pubblica Amministrazione;
2. Reati Informatici;
3. Falsità in monete, in carte di pubblico credito e in valori di bollo;
4. Delitti contro l'industria e il commercio;
5. Reati societari;
6. Reati con finalità di terrorismo o di eversione dell'ordine democratico;
7. Delitti contro la personalità individuale e pratiche di mutilazione degli organi genitali femminili;
8. Reati e illeciti amministrativi di manipolazione del mercato e di abuso di informazioni privilegiate;
9. Reati transnazionali;
10. Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro;
11. Reati di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita;

12. Delitti in materia di strumenti di pagamento diversi dai contanti;
13. Delitti di criminalità organizzata;
14. Delitti in materia di violazione del diritto d'autore;
15. Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
16. Reati ambientali;
17. Reato di impiego di lavoratori con soggiorno irregolare;
18. Reati di razzismo e xenofobia;
19. Reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo apparecchi vietati;
20. Reati tributari;
21. Reati di contrabbando;
22. Reati contro il patrimonio culturale.

2.5. L'apparato sanzionatorio

Il D. lgs. 231 prevede, in caso di responsabilità dell'Ente derivante da reato, un catalogo di sanzioni:

A) sanzioni pecuniarie;

B) sanzioni interdittive, che si sostanziano in:

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

C) la confisca;

D) la pubblicazione della sentenza.

La sanzione pecuniaria, sempre applicata in caso di illecito amministrativo dipendente da reato, viene applicata per "quote in un numero non inferiore a cento né superiore a mille" (art. 10).

Il giudice determina il *quantum* in base alla gravità del fatto, al grado di responsabilità dell'Ente, all'attività svolta per eliminare o attenuare le conseguenze del fatto e prevenire la commissione di ulteriori illeciti.

L'importo della singola quota – variabile da € 258,00 ad € 1.549,00 – è fissato in relazione alle condizioni economiche e patrimoniali dell'Ente, in modo da assicurare efficacia alla sanzione comminata (artt. 10 co. 3 e 11 co. 2).

Per quanto attiene alle modalità di accertamento delle condizioni economiche e patrimoniali dell'Ente: *"Il giudice potrà avvalersi dei bilanci o delle altre scritture comunque idonee a fotografare tali condizioni. In taluni casi, la prova potrà essere conseguita anche tenendo in considerazione le dimensioni dell'Ente e la sua posizione sul mercato. [...] Il giudice non potrà fare a meno di calarsi, con l'ausilio di consulenti, nella realtà dell'impresa, dove potrà attingere anche le informazioni relative allo stato di solidità economica, finanziaria e patrimoniale dell'Ente"* (Relazione al Decreto, punto 5.1).

La sanzione pecuniaria può essere limitata e/o ridotta se:

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 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 ed è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.

Le sanzioni interdittive possono essere applicate anche in via cautelare, su richiesta del Pubblico Ministero, quando sussistono gravi indizi di responsabilità dell'Ente e vi sono fondati motivi per ritenere che sussista il pericolo di reiterazione del reato.

Ai sensi dell'art. 20, si ha reiterazione del reato quando a carico dell'Ente, già condannato in via definitiva almeno una volta, si configuri nuovamente un'ipotesi di responsabilità nei cinque anni successivi.

La confisca e sequestro preventivo in sede cautelare sono previste dall'art. art. 19: la sentenza di condanna ordina la confisca del prezzo o del profitto del reato, salvo per la parte che può essere restituita al danneggiato; quando ciò non è possibile, è disposta la confisca di somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato, salvo che per la parte che può essere restituita al danneggiato e fatti salvi i diritti acquisiti dai terzi in buona fede.

La pubblicazione della sentenza è prevista dall'art. 18 e può essere disposta, a spese dell'Ente, nei casi in cui viene applicata una sanzione interdittiva.

2.6. I delitti tentati

L'art. 26 del D. Lgs. n. 231 prevede che in caso di commissione nelle forme del tentativo dei delitti previsti dal Capo I del medesimo decreto (con eccezione di quelli che risultano insuscettibili di essere commessi nelle forme del tentativo, come ad esempio i reati colposi previsti dall'art. 25-*septies*), l'importo delle sanzioni pecuniarie e la durata delle sanzioni interdittive si riducono da un terzo alla metà.

L'erogazione di sanzioni è invece esclusa qualora l'Ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento.

2.7. I modelli di organizzazione e gestione

Il D.lgs. 231 prevede forme di esonero dalla responsabilità amministrativa degli enti; in particolare, ai sensi dell'art. 6, se il reato è stato commesso dai soggetti apicali l'ente non risponde se prova che:

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

Il legislatore, dunque, immagina nel caso di reato commesso da soggetti apicali una presunzione di responsabilità dovuta al fatto che tali soggetti esprimono e rappresentano la volontà dell'ente stesso.

Si tratta di una presunzione relativa che l'ente può superare dimostrando la sussistenza delle succitate quattro condizioni di cui all'art. 6 del D. Lgs. 231.

In tal caso, pur sussistendo la responsabilità personale in capo al Soggetto apicale, l'ente non è responsabile ai sensi del D. Lgs. 231.

Il D. Lgs. 231 attribuisce un valore esimente ai modelli di organizzazione e gestione nella misura in cui questi ultimi risultino idonei a prevenire i reati di cui al citato decreto e, al contempo, vengano efficacemente attuati da parte del Consiglio di amministrazione e dalla Direzione Generale.

Parimenti, l'art. 7 del D. Lgs. 231 stabilisce la responsabilità amministrativa dell'ente per i reati di Sottoposti, se la loro commissione è stata resa possibile dall'inosservanza degli obblighi di direzione o di vigilanza.

In ogni caso, l'inosservanza di detti obblighi di direzione o di vigilanza è esclusa se l'ente dimostra di aver adottato ed efficacemente attuato, prima della commissione del fatto, un modello di organizzazione e gestione idoneo a prevenire reati della specie di quello verificatosi.

Pertanto, nell'ipotesi prevista dal succitato art. 7 del D.Lgs. 231, l'adozione del modello di organizzazione e gestione da parte dell'ente costituisce una presunzione a suo favore, comportando, così, l'inversione dell'onere della prova a carico dell'accusa che dovrà, quindi, dimostrare la mancata adozione ed efficace attuazione del Modello 231.

Il Modello 231 deve rispondere ai seguenti requisiti:

a. individuare le attività nel cui ambito esiste la possibilità che vengano commessi reati previsti dal decreto;

b. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni della società in relazione ai reati da prevenire;

c. individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione di tali reati;

d. prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello 231;

e. introdurre un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello 231.

3. LA BANCA DELLE TERRE VENETE – CREDITO COOPERATIVO

3.1. La struttura della Banca delle Terre Venete e la sua collocazione all'interno del Gruppo Iccrea Banca

Come anticipato in premessa, la Banca nasce dalla fusione per incorporazione del Credito Trevigiano Banca di Credito Cooperativo nella Cassa Rurale ed Artigiana di Brendola – Credito Cooperativo, intervenuta il 26 ottobre 2020, a seguito della quale l'incorporante ha modificato la propria denominazione sociale in Banca delle Terre Venete Credito Cooperativo – Società Cooperativa.

Nell'esercizio della sua attività, la Banca si ispira ai principi dell'insegnamento sociale cristiano e ai principi cooperativi della mutualità senza fini di speculazione privata, ha lo scopo di favorire i soci e gli appartenenti alle comunità locali nelle operazioni e nei servizi di banca, perseguendo il miglioramento delle condizioni morali, culturali ed economiche degli stessi e promuovendo lo sviluppo della cooperazione, l'educazione al risparmio e alla previdenza, nonché la coesione sociale e la crescita responsabile e sostenibile del territorio nel quale opera.

Dal 4.3.2019 la Banca fa parte del Gruppo Bancario Cooperativo Iccrea ed è pertanto tenuta, in base al contratto di coesione cui essa aderisce, all'osservanza delle direttive emanate dalla Capogruppo ICCREA Banca S.p.A. nell'esercizio dell'attività di direzione e coordinamento ovvero per l'esecuzione delle istruzioni impartite dall'autorità competente nell'interesse della stabilità del Gruppo.

Il Gruppo Bancario Cooperativo Iccrea persegue una strategia finalizzata alla stabilità e allo sviluppo dello stesso, favorendo l'unità di direzione strategica e operativa delle proprie società, l'integrazione della *governance* e la coesione patrimoniale nel rispetto delle finalità mutualistiche delle Banche Affiliate.

3.2. Il ruolo della Capogruppo

Come previsto in apposito Contratto di coesione, la Capogruppo ICCREA Banca S.p.A. ha assunto verso la Banca i doveri e le responsabilità connessi al proprio ruolo di direzione strategica e operativa del gruppo e di interlocutore dell'Autorità di Vigilanza.

Nell'esercizio dei poteri di direzione e coordinamento la Capogruppo emana direttive aventi ad oggetto:

- il rispetto delle disposizioni in materia prudenziale e creditizia applicabili al gruppo e alle sue singole componenti;
- le disposizioni in materia di governo societario, politiche e prassi di remunerazione e incentivazione;
- il sistema dei controlli interni, sistema informativo e continuità operativa, partecipazioni detenibili, attività di rischio e conflitti d'interesse nei confronti di soggetti collegati;
- la trasparenza delle operazioni bancarie, usura e antiriciclaggio.

Le direttive della Capogruppo sono emanate dagli organi con funzioni di supervisione strategica, di gestione e di controllo della stessa, nonché dall'alta direzione della Capogruppo, e sono indirizzate ai competenti organi e funzioni della Banca.

La Banca, nel rispetto del Contratto di coesione, è tenuta a:

- approvare, recepire e dare esecuzione alle direttive;
- fornire alla Capogruppo ogni dato e informazione per l'emanazione e la verifica del rispetto delle stesse;
- collaborare con la Capogruppo per l'attuazione delle misure preventive, correttive e sanzionatorie eventualmente disposte dalla medesima.

La Banca può essere esclusa dal Gruppo, a fronte di una delibera motivata della Capogruppo e previa autorizzazione dell'Autorità di Vigilanza, se:

- ha commesso gravi o ripetute violazioni delle obbligazioni previste nel contratto di coesione, delle disposizioni di vigilanza afferenti al Gruppo o delle ulteriori disposizioni normative o regolamentari applicabili al Gruppo;
- non rispetta le direttive della Capogruppo;
- ostacola l'esercizio dell'attività di direzione e coordinamento da parte della Capogruppo;
- sono stati inutilmente esperiti, da parte della Capogruppo, gli appropriati poteri di intervento correttivo o di sostegno infragruppo.

Tali attività della Capogruppo, unitamente alle direttive ed ai controlli che questa emana nei confronti della Banca, concorrono e contribuiscono a favorire la *compliance* relativa a molteplici ambiti dell'attività della Banca stessa.

3.3. L'assetto organizzativo della Banca

L'assetto organizzativo della Banca, descritto compiutamente nell'organigramma, risente inevitabilmente dell'influenza della Capogruppo, verso la quale, come più innanzi specificato, sono state esternalizzate tutte le funzioni di controllo di primo e secondo livello.

La Struttura Organizzativa della Banca si compone di Aree funzionali, in linea e dipendenti dalla Direzione, e dai Servizi gerarchicamente in staff alla Direzione stessa.

Le Aree funzionali in cui è divisa la struttura della Banca sono le seguenti:

- Area Crediti;
- Area Amministrativa;

- Area Organizzazione di Sistemi;
- Area Finanza;
- Area Affari.

Le componenti organizzative utilizzate nella Struttura Organizzativa della Banca sono:

- le Unità Organizzative distinte in Aree, Servizi, Uffici, Filiali;
- le Funzioni (insieme omogeneo di attività, attribuito a una o più posizioni di lavoro);
- le posizioni di lavoro (l'elemento base della struttura organizzativa, costituita da un insieme di compiti e di responsabilità);
- le responsabilità per comparti (Responsabile di Area, Responsabile di Servizio, Responsabile Ufficio);
- gli Incarichi (compiti o attività attribuiti ad personam)
- gli Organi Sociali ed i loro esponenti;
- gli Organi di Coordinamento (Comitati con attività permanenti, ma discontinue).

3.4. Gli obiettivi del Modello 231

Con l'introduzione del Modello 231 la Banca si pone l'obiettivo di strutturare un sistema di elementi organizzativi e relative regole di funzionamento, attraverso l'individuazione delle "*attività sensibili ex D.Lgs. 231*" e la definizione di protocolli "*idonei a prevenire i reati*", volto a:

- rendere consapevoli tutte le persone facenti parte della struttura aziendale, sia di governo sia esecutiva, che eventuali comportamenti illeciti possono comportare sanzioni penali ed amministrative sia per il singolo che per l'azienda;
- garantire la correttezza dei comportamenti della Banca stessa e delle persone che la rappresentano, nel completo rispetto della normativa esterna e interna;
- rafforzare meccanismi di controllo, monitoraggio e sanzionatori atti a contrastare la commissione di reati;
- enfatizzare le scelte in materia di conformità, di etica, di trasparenza, di correttezza da sempre perseguite dal Credito Cooperativo e peraltro sancite anche dallo Statuto Sociale e dal Codice Etico della Banca.

3.5. Il sistema organizzativo

Ferma restando l'osservanza di quanto previsto dalle fonti normative primarie e secondarie, nonché dalle Linee Guida adottate dall'Associazione Bancaria Italiana, i principali riferimenti documentali che regolano l'organizzazione della Banca sono:

- <u>Lo Statuto sociale della Banca</u>

  Lo Statuto costituisce il documento fondamentale su cui è basato il sistema di governo societario della Banca: definisce la sede, l'oggetto sociale, il contratto di coesione e l'accordo

di garanzia, il capitale sociale, la composizione sia numerica che qualitativa degli Organi Sociali, nonché i compiti e le responsabilità dei Soggetti apicali.

- Il Codice Etico di Comportamento

  La Banca ha adottato un Codice Etico di Comportamento, che è parte integrante del Modello 231.

  Il Codice Etico di Comportamento rappresenta il compendio delle linee programmatiche e di condotta che guidano l'esistenza della Banca, fungendo da ausilio e supporto alla realizzazione ed implementazione di un valido modello di organizzazione e gestione.

- Il Regolamento interno

  Il Regolamento interno descrive la struttura e le competenze delle unità organizzative nelle quali si articola la Banca e fissa le principali attribuzioni e responsabilità delle unità organizzative, nonché quelle inerenti alla Direzione ed ai comitati, regolandone il reciproco coordinamento e le necessarie interazioni, al fine di conseguire in modo unitario gli scopi sociali.

- Politiche di gruppo

  Nell'ambito delle diverse attività poste in essere dalla Banca, la Capogruppo ha adottato ed emanato Politiche, che dettano principi generali in relazione a ciascuno dei profili tematici considerati (ad es. contabilità e bilancio, credito, finanza, organizzazione IT, etc.).

Oltre che sulla base del Regolamento Generale e delle Politiche della Capogruppo, l'attività della Banca è regolamentata da:

- ***I Regolamenti dei processi di lavoro:*** regolamenti che dettano le regole generali di funzionamento dell'operatività bancaria e sono emanati dal Consiglio di Amministrazione;
- ***Le Disposizioni attuative:*** danno concretezza ai regolamenti dei processi di lavoro e sono emesse dal Direttore Generale nella forma degli Ordini di Servizio;
- ***Note informative o Circolari:*** emesse dalle unità organizzative della Banca.

3.6. Le attività sensibili e la loro mappatura (ex art. 6 comma 2 lettera a)

Per mappare le attività sensibili, ai sensi e per gli effetti dell'art. 6 comma 2 lettera a) del D. Lgs. 231, si è proceduto ad analizzare la realtà aziendale, tenendo conto dei processi operativi e delle attività prevalentemente svolte, mettendo in evidenza le potenziali aree di rischio.

L'attività di analisi dei processi aziendali ha consentito di individuare quelle aree ove si è ritenuto potesse determinarsi il rischio di commissione dei reati previsti dal D. Lgs. 231, nonché i responsabili dei processi ad esse afferenti.

Per ogni processo sensibile sono state inoltre identificate le modalità operative e gestionali esistenti e gli elementi di controllo presenti, a presidio delle stesse.

È stata, quindi, valutata la congruità o meno delle norme e procedure attualmente in essere e, ove necessario, sono state elaborate o meglio precisate una serie di azioni di mitigazione in grado di prevenire o quantomeno ridurre sensibilmente il rischio di commissione di reati, attraverso sistemi di controllo sulle attività, di tracciabilità dei processi e di segregazione di responsabilità.

A tal fine sono state individuate cinque macro-aree:

- Area Crediti;
- Area Risorse Umane;
- Area Amministrativa;
- Area Organizzazione e Sistemi;
- Area Affari.

Sulla base di tale ripartizione, sono stati individuati i relativi *key-officers*, cui sono stati sottoposti dei questionari di autovalutazione ai fini della mappatura delle aree di rischio e della stima delle probabilità di commissione dei reati-presupposto nell'ambito delle aree di propria competenza.

In particolare, sono state raccolte le seguenti informazioni:

- lo svolgimento, o meno, dell'attività sensibile presso la Banca al fine di limitare l'analisi al perimetro di effettivo rischio aziendale;
- l'unità organizzativa responsabile dell'attività;
- informazioni relative al processo organizzativo (altre unità organizzative coinvolte, numero di risorse coinvolte nell'attività, normativa di riferimento) finalizzate a caratterizzarne le modalità di svolgimento;
- la descrizione delle modalità di svolgimento del processo anche in termini di livello di definizione delle procedure rispetto all'obiettivo di prevenire la commissione del reato;
- le contromisure adottate;
- l'indicazione delle criticità emerse e delle aree di miglioramento, sempre in ottica di prevenzione dei reati.

I processi che sono stati complessivamente presi in considerazione sono i seguenti:

- Contabilità e Bilancio;
- Credito;
- Estero;
- Finanza;
- Funzioni aziendali di controllo;
- Governo;
- Incassi e pagamenti;
- Legale;

- Mercato;
- Organizzazione – IT;
- Privacy;
- Risorse Umane;
- Tesoreria Enti;
- Trasparenza.

3.7. La formazione e l'attuazione del processo decisionale (ex art. 6 comma 2 lettera b)

Le varie fasi del processo decisionale della Banca, i poteri e le deleghe sono documentati e verificabili in appositi archivi documentali a cui il personale ed i collaboratori possono accedere per la loro consultazione e verifica. I poteri delegati ed i limiti autorizzativi attribuiti all'esecutivo sono definiti attraverso la fissazione di criteri, modalità e limiti di attribuzione, in materia di concessione di credito, classificazione del rischio creditizio e passaggio a perdita, applicazione di condizioni economiche ai rapporti con clientela, spendita della firma sociale e poteri di spesa ed erogazione beneficenza.

Il sistema dei controlli interni prevede la verifica sistematica circa il rispetto delle norme aziendali.

Nel corso dell'analisi effettuata ai fini del D. Lgs. 231 è stato espressamente individuato, per ogni attività sensibile, l'insieme delle regole, generali e di dettaglio, adottate dalla Banca, valutandone il grado di idoneità rispetto alla capacità di prevenzione dei comportamenti illeciti.

3.8. Le modalità di gestione delle risorse finanziarie (ex art. 6 comma 2 lettera c)

La Banca ha definito una modalità di gestione delle risorse finanziarie basata sulle seguenti regole:

- *in materia di erogazione del credito sono disciplinati i poteri di autonomia per organo deliberante e per ciascuna tipologia di affidamento (gruppi di forme tecniche omogenei per intensità di rischio);*
- *sono definiti precisi poteri di autonomia per la determinazione di tassi attivi e passivi e altre condizioni per la clientela della Banca (validi anche in caso di clientela rappresentata da enti pubblici).*

3.9. Il Sistema dei Controlli Interni

La Banca è dotata di un Sistema di Controlli Interni, ovvero l'insieme delle regole, delle procedure e delle strutture organizzative che mirano ad assicurare il rispetto delle strategie aziendali e il conseguimento dell'efficacia e dell'efficienza dei processi aziendali, della salvaguardia dei valori delle attività e protezione dalle perdite, dell'affidabilità e integrità delle informazioni contabili e gestionali, della conformità delle operazioni con la legge, la normativa di vigilanza nonché con le politiche, i piani, i regolamenti e le procedure interne.

Il Sistema di controlli e gestione dei rischi è articolato su tre livelli:

- *controlli di linea* (c.d. "controlli di I livello"), diretti ad assicurare il corretto svolgimento delle operazioni. Tali controlli sono effettuati dalle stesse strutture operative, ovvero eseguiti da altre strutture della Banca (es. uffici di sede). La Banca massimizza il ricorso a controlli di linea incorporati all'interno delle procedure informatiche;
- *controlli sui rischi e sulla conformità* (c.d. "controlli di II livello") assegnati a funzioni distinte da quelle produttive, che hanno l'obiettivo di assicurare tra l'altro:
  - la corretta attuazione del processo di gestione dei rischi;
  - il rispetto dei limiti operativi assegnati alle varie funzioni aziendali;
  - la conformità dell'operatività aziendale alle norme;
- *revisione* interna (c.d. "controlli di III livello) volta ad individuare la eventuale violazione delle procedure e della regolamentazione nonché a valutare la funzionalità e l'adeguatezza, in termini di efficienza e di efficacia, del Sistema dei Controlli.

I controlli di terzo livello sono oggi esternalizzati alla Capogruppo.

3.10. Il Consigliere con delega al Sistema dei Controlli Interni

Il Consigliere con delega al Sistema dei Controlli Interni supporta il Consiglio di Amministrazione in relazione alle materie attinenti alla gestione dei rischi e il sistema dei controlli della Banca, promuovendo il rispetto e l'integrazione con i principi definiti nell'ambito del sistema di controlli di Gruppo e favorendo la consapevolezza degli organi di amministrazione e controllo della Banca in ordine alle politiche e ai processi di gestione del rischio adottati nell'ambito del Gruppo.

Funge da collegamento tra Consiglio di Amministrazione e Funzioni Aziendali di Controllo, e rappresenta, altresì, il riferimento delle eventuali risorse individuate presso la Banca, siano esse inquadrate come referenti della funzione esternalizzata ovvero operanti nelle unità organizzative di supporto operativo.

Principali attività:

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

- rappresenta il riferimento delle eventuali risorse individuate presso la Banca, siano esse inquadrate come referenti della funzione esternalizzata ovvero operanti nelle unità organizzative di supporto operativo.

3.11. Funzioni aziendali di Controllo Esternalizzate alla Capogruppo

Come previsto dal Contratto di coesione, le Funzioni Aziendali di Controllo di Compliance, Internal Audit, Risk Management, Antiriciclaggio, così come definite dalla Circolare di Banca d'Italia n. 285/13, nonché la funzione DPO, sono state esternalizzate presso la Capogruppo secondo precisi accordi.

3.11.1 Compliance

Con il termine *compliance* si indica la funzione di conformità.

Il Servizio viene erogato da una Funzione Accentrata della Capogruppo coordinata e supervisionata da un presidio istituito a livello periferico. Per ciascun presidio periferico, è prevista la nomina di un "Responsabile UO Presidio Compliance" a cui sono assegnati compiti di coordinamento complessivo delle Funzioni di Conformità dell'area geografica di competenza e/o eventuali incarichi di responsabilità diretta della Funzione di Conformità delle singole Banche Affiliate, tra cui la Banca.

Tra il personale dei presidi Compliance periferici è nominato il Responsabile Compliance della Banca che svolge, sotto il coordinamento e la supervisione del Responsabile UO Presidio Compliance, le attività oggetto del Servizio di Compliance in linea con il *framework* di controllo definito dalla Capogruppo, nonché con quanto disciplinato nel contratto sottoscritto tra la Capogruppo e la Banca.

Alla funzione di Conformità sono assegnate le attività riportate principalmente all'interno della seguente documentazione recepita dalla banca tramite Direttiva:

- Politica di Gruppo in materia di assetto delle FAC;
- Contratto per l'esternalizzazione delle funzioni aziendali di controllo;
- Politica di Gruppo Governo e gestione del rischio di non conformità;
- Regolamento di Gruppo rischio Conformità;
- Metodologia di valutazione del Rischio di non conformità;
- Indirizzi per la pianificazione della Banca.

3.11.2 Internal Audit

Il Servizio viene erogato da una Funzione Accentrata della Capogruppo, governata dal "Responsabile della Funzione Accentrata" (RF), e da presidi organizzativi periferici all'interno dei quali è nominato il Responsabile Internal Audit della Banca – RIABCC – che svolge, sotto il coordinamento e la supervisione dell'Area Chief Audit Executive, le attività oggetto del Servizio di Internal Audit in linea con il *framework* di controllo definito dalla Capogruppo nonché con quanto disciplinato nel contratto.

Le principali attività della funzione di Internal Audit - le cui finalità, poteri e responsabilità sono definiti nel Mandato approvato dal Consiglio di Amministrazione - si declinano principalmente

nelle attività riportate all'interno della seguente documentazione recepita dalla banca tramite Direttiva:

- Politica di Gruppo in materia di assetto delle FAC;
- Contratto per l'esternalizzazione delle funzioni aziendali di controllo;
- Regolamento della Funzione Internal Audit.

3.11.3 Risk Management

Il Servizio viene erogato da una funzione accentrata della Capogruppo per il tramite di presidi periferici (per la Funzione Risk Management: Area 1, Area 2 e Area 3). Per ciascun presidio periferico, è prevista la nomina di un "Responsabile UO Coordinamento RM BCC" a cui sono assegnati compiti di coordinamento complessivo delle Funzioni Risk Management dell'area geografica di competenza del presidio. Nell'ambito del personale delle citate unità organizzative sono identificati e nominati:

- il Responsabile Risk Management della Banca, che guida lo svolgimento delle attività della Funzione in parola presso la Banca stessa;

- gli Specialisti Territoriali, che fungono da referenti specialistici e supportano il Responsabile Risk Manager della Banca nella declinazione e nell'adozione delle strategie, delle politiche e dei processi di rilevazione, valutazione e controllo dei rischi definiti a livello di Gruppo.

Alla funzione Risk Management sono assegnate le attività riportate principalmente all'interno della seguente documentazione recepita dalla banca tramite Direttiva:

- Politica di Gruppo in materia di assetto delle FAC;
- Contratto per l'esternalizzazione delle funzioni aziendali di controllo;
- Regolamento della Funzione Risk Management

3.11.4 AML - Antiriciclaggio

La Funzione Antiriciclaggio della Banca è esternalizzata alla Capogruppo ed incardinata principalmente nei Presidi Periferici della Capogruppo. Tali Presidi sono soggetti al coordinamento dell'Area Chief AML Officer di Capogruppo, collocata a diretto riporto del Consiglio di Amministrazione, che assicura, per mezzo delle UO AML BCC Affiliate e Metodologie e Reporting la definizione di indirizzi, principi organizzativi e politiche in materia di governo del rischio di riciclaggio e finanziamento del terrorismo e ne controlla l'attuazione da parte della Banca.

L'Unità organizzativa Presidio AML Periferico rappresenta la struttura Antiriciclaggio dislocata presso il Presidio Periferico, cui sono demandate l'esecuzione delle attività di supporto previste dal modello di controllo di secondo livello in materia di gestione del rischio di riciclaggio e finanziamento al terrorismo, e il coordinamento e la supervisione delle attività svolte dai Responsabili AML di BCC (RAMLBCC) dell'area geografica di riferimento. A questi è infine attribuita la responsabilità della Funzione Antiriciclaggio della Banca, al fine di garantire la realizzazione delle attività di competenza della Funzione Antiriciclaggio anche avvalendosi delle attività assicurate dalle strutture centrali.

Le principali attività attribuite alla funzione Antiriciclaggio, istituita presso il Presidio AML locale/ periferico si declinano nei compiti riportati principalmente all'interno della seguente documentazione recepita dalla banca tramite Direttiva:

- Politica di Gruppo in materia di assetto delle FAC;
- Contratto per l'esternalizzazione delle funzioni aziendali di controllo;
- Politica di Gruppo in materia di assetto delle FAC;
- Contratto per l'esternalizzazione delle funzioni aziendali di controllo;
- Politica di Gruppo AML governo e gestione rischio riciclaggio e finanziamento al terrorismo;
- Regolamento della Funzione AML.

3.11.5 Funzione *Data Protection Officer* (DPO)

La funzione Data Protection Officer (DPO) è stata esternalizzata alla Capogruppo; per la Banca è stato nominato un DPOBCC che costituisce l'articolazione sul territorio della Unità Operativa *Data Protection Officer*. Al DPO della Banca è demandata l'esecuzione delle attività collegate al servizio DPO per le Banche Affiliate di competenza.

3.11.6 Flussi informativi

Nell'ambito del Sistema dei controlli interni, in ossequio a quanto previsto dalle Disposizioni di Vigilanza, il Gruppo Iccrea ha disciplinato, nell'ambito della normativa interna, i principali flussi informativi, le aree di interazione nonché i meccanismi di coordinamento tra le diverse FAC e tra queste e gli Organi Aziendali. L'interazione ed il coordinamento si fonda su un sistema di flussi informativi che devono presentare caratteristiche di tempestività, chiarezza ed esaustività.

In particolare, le attività di *compliance* sono rendicontate agli Organi Aziendali attraverso appositi flussi informativi periodici, secondo quanto definito nella Politica di Gruppo in materia di *Coordinamento delle Funzioni Aziendali di Controllo e Schema dei flussi informativi verso gli Organi Aziendali e i Comitati endo-consiliari*.

La Funzione garantisce, attraverso la competente Unità Organizzativa, la predisposizione della reportistica e dei flussi informativi.

4. L'ORGANISMO DI VIGILANZA

In attuazione delle disposizioni dell'art 6, comma 1 lettera b), del D. Lgs. 231, il Consiglio di Amministrazione della Banca delle Terre Venete ha istituito uno specifico Organismo di Vigilanza, a composizione collegiale, nel quale siedono tre membri.

L'Organismo è composto da soggetti in grado di assicurare un adeguato livello di professionalità e continuità di azione e ha il compito di valutare l'adeguatezza dei modelli di organizzazione, gestione e controllo e del Codice Etico adottati dalla Banca, di vigilare sul loro funzionamento ed osservanza, per prevenire la commissione dei reati previsti dal D. Lgs. 231/01 e successive modifiche e integrazioni.

Il funzionamento dell'Organismo di Vigilanza è disciplinato dal Regolamento elaborato ed approvato in autoregolamentazione dallo stesso Organismo di Vigilanza in data 29.3.2021.

L'Organismo di Vigilanza è dotato di pieni ed autonomi poteri di iniziativa e di controllo sulle attività della Banca.

L'Organismo:

- vigila sull'osservanza, sull'attuazione e sull'adeguatezza del presente Modello;
- cura che ci sia un continuo monitoraggio ed adeguamento delle procedure di controllo e di prevenzione anche attraverso l'aggiornamento della mappatura dei rischi di reato, la verifica e la segnalazione da parte delle singole funzioni di nuove aree di rischio che potrebbero esporre la Banca alle conseguenze derivanti dal compimento dei suddetti reati;
- effettua proposte ed osservazioni relative ad aggiornamenti dell'impianto procedurale e verifica l'attuazione e l'efficacia delle soluzioni proposte, avvalendosi della collaborazione delle competenti funzioni della Banca;
- definisce le iniziative più idonee a diffondere tra il personale ed i consulenti la conoscenza dei modelli di organizzazione, gestione e controllo nonché del Codice Etico, tramite attività di formazione dei dipendenti e ne chiarisce, mediante pareri, il significato e l'applicazione;
- riferisce periodicamente al Consiglio di Amministrazione circa l'attività svolta e produce una relazione almeno annuale per il Consiglio di Amministrazione ed il Collegio Sindacale, sia quale consuntivo delle attività svolte, sia quale programma da svolgersi nel periodo successivo:
- attiva, tramite le funzioni preposte, gli eventuali procedimenti disciplinari ai sensi di legge e di contratto collettivo applicabile, idonei a sanzionare il mancato rispetto delle misure indicate nei modelli di organizzazione, gestione e controllo e nel Codice Etico.

4.2. Composizione

L'Organismo di Vigilanza, come detto, è formato da tre componenti di cui un Presidente, un membro ordinario e un Segretario che avrà il compito di provvedere alla verbalizzazione delle riunioni svolte.

I componenti dell'Organismo, una volta nominati dal Consiglio di Amministrazione, eleggono al loro interno il Presidente, laddove non vi abbia direttamente provveduto il Consiglio di Amministrazione.

Il Presidente dell'Organismo esercita i poteri e svolge le funzioni nei limiti previsti dal Regolamento, rappresenta l'Organismo nei confronti degli organi sociali, delle funzioni aziendali e dei terzi.

In caso di assenza o di impedimento temporaneo, i poteri e le funzioni del Presidente spettano al componente più anziano d'età. In caso di impedimento prolungato o definitivo l'Organismo, informato il Consiglio di Amministrazione, provvede non appena possibile a nominare un nuovo Presidente.

4.4. Flussi informativi

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

A tal fine, l'Organismo di Vigilanza:

- accede a tutti i documenti ed informazioni aziendali rilevanti per lo svolgimento delle funzioni ad esso attribuite;
- si avvale, previa richiesta al Consiglio di Amministrazione, di soggetti terzi di comprovata professionalità nei casi in cui ciò si renda necessario per l'espletamento delle attività di verifica e controllo ovvero di aggiornamento del Modello 231;
- richiede ai dipendenti della Banca di fornire tempestivamente le informazioni, i dati e/o le notizie necessarie per individuare aspetti connessi alle varie attività aziendali rilevanti ai sensi dei Modello 231 e per la verifica dell'effettiva attuazione dello stesso;
- riceve periodicamente i flussi informativi relativi al Modello 231 precedentemente definiti e comunicati alla struttura della Banca, nonché le comunicazioni inoltrate alla Banca stessa dai dirigenti e/o dai dipendenti di avvio di procedimento giudiziario a loro carico per i reati previsti dal D.Lgs. 231, i rapporti predisposti nell'ambito delle attività di controllo da funzioni interne e/o da soggetti esterni, nonché i verbali delle Autorità di Vigilanza, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto alle norme del D. Lgs. 231, le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del Modello 231, evidenzianti i procedimenti disciplinari svolti e le eventuali sanzioni irrogate (ivi compresi i provvedimenti assunti nei confronti dei dipendenti).

In particolare, l'Organismo di Vigilanza riceve:

- dal Consiglio di Amministrazione le delibere che abbiano attinenza con la 231/2001 ed operazioni con la Pubblica Amministrazione;
- dal Collegio dei Sindaci i verbali e le relazioni aventi attinenza con la 231/2001;
- dall'Area Internal Audit, Area Compliance, Area Risk Management, Comitato Controlli Interni e Dirigente Preposto le relazioni periodiche, i prospetti riepilogativi, i resoconti e i *report* delle singole verifiche su tematiche direttamente e indirettamente rilevanti ai fini della 231/01 (reati informatici, riciclaggio, abusi di mercato);
- dall'Area Affari Societari e Legali:
    a. ogni modifica dell'assetto di governance, del sistema delle deleghe e dell'organigramma;
    b. i provvedimenti e/o le notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati presupposto di cui al Decreto o in base ad altre leggi per cui esso è applicabile, nel caso in cui tali indagini coinvolgano la Banca o suoi dipendenti o collaboratori o comunque possano implicare la responsabilità dell'ente stesso;
    c. l'avvio di procedimenti giudiziari a carico di soggetti apicali, loro sottoposti collaboratori esterni dell'ente ove vengano contestati reati previsti dal Decreto o per cui esso è ritenuto applicabile in base ad altre norme;

d. le richieste di assistenza legale inoltrate da amministratori, sindaci, dirigenti e/o dipendenti in caso di avvio di procedimento giudiziario per i reati previsti dal Decreto;

- dalla Direzione gli appalti con la Pubblica Amministrazione;
- dal Servizio tecnica/sicurezza -RSPP:

  a. verbali delle riunioni periodiche di prevenzione e protezione dai rischi (ex art. 35, D.lgs. n. 81/2008 e successive modificazioni);

  b. incidenti occorsi sul luogo di lavoro; Modello Organizzativo D. Lgs. 231/2001; c. ogni modifica e aggiornamento della documentazione relativa al sistema di gestione della sicurezza sul lavoro (DVR, piano di intervento e di evacuazione in emergenza, procedure poste a presidio di funzioni connesse alla salute e sicurezza sul lavoro;

- dalla Direzione Human Resources:

  a. provvedimenti disciplinari adottati/adottandi in conseguenza di violazioni del codice di condotta ex 231/2001 e/o del codice etico;

  b. ogni variazione della struttura organizzativa;

- dal Responsabile area IT:

  a. relazioni su attività eventualmente a rischio di commissione di reati informatici ex 231/2001;

  b. relazione sulla business continuity.

Nello specifico, in materia di antiriciclaggio, l'Organismo di Vigilanza:

- in coordinamento con gli organi sociali e le funzioni di controllo, verifica l'efficacia dei presidi e l'osservanza delle procedure relative alla mitigazione e gestione dei rischi di riciclaggio e di finanziamento del terrorismo, promuovendo l'adozione delle misure correttive più idonee al superamento di eventuali carenze;
- riceve, con la cadenza periodica, i flussi informativi antiriciclaggio (Relazione Annuale della Funzione Antiriciclaggio, Report Consuntivo sulle attività svolte in materia di antiriciclaggio e i Report ordinari antiriciclaggio con giudizio "Parzialmente insoddisfacente e/ Insoddisfacente" o in presenza di rischi con *scoring* 3/4) per il consapevole espletamento delle responsabilità assegnate.
- le attività svolte dall'organismo sono documentate e i relativi atti, ove richiesti, sono prontamente forniti alle Autorità di vigilanza di settore e alla UIF.

4.4. Obblighi di informazione nei confronti dell'Organismo di Vigilanza

L'Organismo, al fine di consentire l'operatività degli obblighi di informazione di cui all'art. 6, comma 2, lett. d), predispone un efficace sistema di comunicazione interna che, garantendo la massima riservatezza e tutela del segnalante, permetta a tutti coloro che vengano a conoscenza di situazioni illecite nonché di situazioni non conformi ai modelli di organizzazione, gestione e

controllo ed al Codice Etico adottati, di segnalare allo stesso Organismo di Vigilanza ogni notizia rilevante ai fini del D.Lgs. 231, quali ad esempio:

- risultanze dell'attività di controllo (attività di monitoraggio, report riepilogativi, indici consuntivi);
- anomalie o atipicità riscontrate nello svolgimento delle varie attività;
- decisioni relative alla richiesta, erogazione ed utilizzo di finanziamenti pubblici;
- richieste di assistenza legale inoltrate da dirigenti e/o dipendenti per procedimenti relativi a reati previsti dal D.Lgs. 231;
- provvedimenti e/o notizie provenienti da organi di Polizia giudiziaria o altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al D.Lgs. 231;
- notizie relative ad appalti attribuiti da enti pubblici o soggetti che svolgono funzioni di pubblica utilità;
- modifiche organizzative/procedurali riferibili al D.Lgs. 231.

Fermo restando il rispetto di ogni tutela prevista dalla normativa o dai contratti collettivi vigenti e fatti salvi gli obblighi di legge, l'Organismo è legittimato a ricevere richieste di chiarimenti, reclami o notizie di potenziali o attuali violazioni del Modello. A tal fine è stato istituito un apposito recapito telematico (*organismodivigilanza@bancaterrevenete.it*) al fine di consentire la trasmissione di segnalazione all'organismo in attuazione di pratiche di *whistleblowing*.

Qualsiasi richiesta di chiarimenti, reclamo o notizia, sarà mantenuta strettamente riservata in conformità alle norme di legge applicabili.

Nel rispetto di quanto previsto dalla disciplina sulla protezione dei dati personali, il Responsabile dei Sistemi Interni di Segnalazione delle violazioni della Banca (il Consigliere con delega al Sistema dei Controlli interni) redige una relazione annuale sul corretto funzionamento dei sistemi interni di segnalazione delle violazioni, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute. Tale relazione comprende altresì le segnalazioni che hanno coinvolto il Direttore Generale e i membri degli Organi Aziendali.

5. IL SISTEMA SANZIONATORIO

5.1. Principi generali

L'osservanza delle disposizioni e delle regole comportamentali previste dal Modello 231 costituisce adempimento, da parte dei Soggetti sottoposti, degli obblighi previsti dall'art. 2104, comma 2, del codice civile; obblighi dei quali il contenuto del Modello 231 rappresenta parte sostanziale ed integrante.

La violazione delle misure indicate nel Modello 231 costituisce un inadempimento contrattuale censurabile sotto il profilo disciplinare ai sensi dell'art. 7 dello Statuto dei lavoratori (legge 20 maggio 1970 n. 300) e determina l'applicazione delle sanzioni previste dal vigente Contratto Collettivo Nazionale dei Lavoratori e dal Regolamento Disciplinare, su cui tra breve si tornerà.

Elemento essenziale per il funzionamento del Modello 231 e per la valenza scriminante del Modello rispetto alla responsabilità amministrativa degli enti. *è l'introduzione di un sistema disciplinare idoneo a sanzionare gli eventuali comportamenti ed attività contrastanti con le misure indicate dalla Banca.*

Al riguardo, infatti l'art. 6 comma 2 lett. e) del D.Lgs. 231 prevede che i modelli di organizzazione e gestione devono "*introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello*".

Per tutti i dipendenti della Banca il sistema sanzionatorio introdotto ai sensi dell'art. 6, comma 2, del Decreto è coerente con i principi di immediatezza e tempestività della contestazione della violazione, della concessione di termini per l'esercizio del diritto di difesa prima che la sanzione sia comminata, della proporzionalità della sanzione applicata in relazione alla gravità della violazione commessa ed al grado d'intenzionalità dell'azione o dell'omissione.

Il mancato rispetto delle misure, previste dal Modello 231, viene valutato sotto il profilo disciplinare in misura diversa in base a chi abbia posto in essere la violazione, ove si tratti "*soggetti sottoposti a direzione o vigilanza*" (art. 5, comma 1, lett. b) o di "*soggetti apicali*" (art. 5, comma 1, lett. a).

Le sanzioni irrogabili sono, come da disciplina di contrattazione collettiva, quelle previste dal regolamento disciplinare e saranno applicate ad ogni violazione delle disposizioni contenute nel Modello, a prescindere dalla commissione del reato e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria.

L'Organismo di Vigilanza, ricevuta la segnalazione e svolti gli opportuni accertamenti, formula una proposta in merito ai provvedimenti da adottare e comunica la propria valutazione agli organi aziendali competenti in base al sistema disciplinare, i quali si pronunceranno in merito all'eventuale adozione e/o modifica delle misure proposte dall'Organismo di Vigilanza, attivando le funzioni aziendali/unità organizzative di volta in volta competenti in ordine all'effettiva applicazione delle misure stesse.

5.2. Provvedimenti disciplinari

5.2.1. Personale appartenente alle aree professionali e quadri direttivi

I comportamenti tenuti dai dipendenti in violazione delle singole regole comportamentali dedotte dal Modello e dal Codice etico sono definiti come illeciti disciplinari.

L'Organismo di Vigilanza deve esserne tempestivamente informato e, con esso, la Direzione generale. Tale segnalazione deve pervenire dal soggetto (destinatario, a qualunque titolo, del presente documento) che abbia rilevato il comportamento illecito.

Fatti i riscontri del caso, l'OdV ne fornisce una relazione circostanziata alla Direzione generale e al responsabile delle Risorse umane, per l'avvio del procedimento disciplinare, secondo quanto previsto dall'art. 7 della legge 20 maggio 1970 n. 300 e dall'art. 40 del vigente "CCNL per i quadri direttivi e per il personale delle aree professionali delle imprese creditizie, finanziarie e strumentali".

Confermata la sussistenza della violazione, la Direzione generale fornirà, sul punto, debita informativa al Consiglio di amministrazione ed al Collegio dei sindaci, nella prima riunione consiliare utile a far data da quando la violazione sia stata accertata.

Decorsi i termini di legge a tutela del lavoratore, l'eventuale provvedimento sarà irrogato in maniera tempestiva, ispirandosi a criteri di:

- *gradualità* della sanzione in relazione al grado di pericolosità del comportamento messo in atto;

- *proporzionalità* fra la mancanza rilevata e la sanzione irrogata.

La recidiva costituisce aggravante ai fini della valutazione della sanzione da irrogare.

Il Modello fa riferimento alle categorie di fatti sanzionabili previste dall'apparato sanzionatorio esistente, contenuto nelle previsioni di cui al Contratto Collettivo Nazionale di Lavoro.

Tali categorie descrivono i comportamenti sanzionati a seconda del rilievo che assumono le singole fattispecie considerate e le sanzioni in concreto previste per la commissione dei fatti stessi a seconda della loro gravità.

In particolare, in applicazione dei criteri di correlazione tra le mancanze dei lavoratori dipendenti e i provvedimenti disciplinari vigenti in Banca e richiamati dal CCNL, si prevede che **incorre**:

1) **nel provvedimento del "*rimprovero verbale o scritto*"**:

il lavoratore dipendente che violi le procedure interne previste dal presente Modello (ad esempio che non osservi le procedure prescritte, ometta di dare comunicazione all'OdV delle informazioni prescritte, etc.) o adotti, nell'espletamento della propria attività, un comportamento non conforme alle prescrizioni del Modello stesso, dovendosi ravvisare, in tali comportamenti, una non esecuzione degli ordini impartiti dall'azienda sia in forma scritta che verbale, correlandosi detto comportamento a una lieve (rimprovero verbale) o non grave (rimprovero scritto) inosservanza delle norme contrattuali o delle direttive ed istruzioni impartite dalla direzione o dai superiori;

2) **nel provvedimento della "*sospensione dal servizio e dal trattamento economico non superiore a 10 giorni*"**:

il lavoratore dipendente che, nel violare le procedure interne previste dal presente Modello o adottando nell'espletamento di attività nelle "aree a rischio" un comportamento non conforme alle prescrizioni del Modello stesso nonché compiendo atti contrari all'interesse della Banca, arrechi danno ad essa o la esponga a una situazione oggettiva di pericolo in relazione alla integrità dei beni aziendali, dovendosi ravvisare in tali comportamenti la non esecuzione degli ordini impartiti dalla Banca, sia in forma scritta sia verbale, correlandosi detto comportamento ad una inosservanza - ripetuta o di una certa gravità – delle norme contrattuali o delle direttive ed istruzioni impartite dalla direzione o dai superiori;

3) **nel provvedimento del "*licenziamento per notevole inadempimento degli obblighi contrattuali del prestatore di lavoro (giustificato motivo)*" o**, a seconda della gravità dei comportamenti posti in essere, dell'importanza delle prescrizioni violate nonché delle conseguenze dannose che ne discendano per la Banca, **nel provvedimento del "*Licenziamento per una mancanza così grave da non consentire la prosecuzione anche provvisoria del rapporto (giusta causa)*"**: il lavoratore che, nell'espletamento della propria attività, adotti un

comportamento palesemente in violazione delle prescrizioni del presente Modello e tale da determinare la concreta applicazione a carico della Società di misure previste dal Decreto, dovendosi ravvisare in tale comportamento una condotta orientata - dolosamente o per colpa grave - a provocare all'azienda grave nocumento reputazionale e/o materiale, correlandosi detto comportamento ad una violazione tale da configurare un inadempimento "notevole" degli obblighi relativi.

Il tipo e l'entità di ciascuna delle sanzioni sopra richiamate, saranno applicate, ai sensi di quanto previsto dal codice disciplinare vigente in Banca, in relazione:

- all'intenzionalità del comportamento o grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- al comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti provvedimenti disciplinari a carico del medesimo, nei limiti consentiti dalla legge;
- alle mansioni del lavoratore;
- alla posizione funzionale delle persone coinvolte nei fatti costituenti la mancanza;
- alle altre particolari circostanze che accompagnano la violazione disciplinare.

Per quanto riguarda l'accertamento delle suddette infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, alla relativa direzione aziendale.

Qualora la Direzione generale o il responsabile delle Risorse umane dovessero decidere di non procedere all'irrogazione della sanzione, essi dovranno darne motivazione scritta all'OdV.

5.2.2. Dirigenti

Nella contrattazione collettiva nazionale non è previsto per i dirigenti alcun codice disciplinare né alcuna sanzione disciplinare conservativa.

Nei casi in cui essi attuino, rispetto alle prescrizioni richiamate nel Modello, una condotta manchevole e gravemente pregiudizievole per la Banca, questa valuterà se, a fronte dei comportamenti riscontrati, permangano i presupposti per il mantenimento del vincolo fiduciario specificatamente insito nel rapporto di lavoro dirigenziale e procederà, in caso contrario, alla risoluzione del rapporto di lavoro ex art. 2118 c.c. e, nei casi accertati di comportamento doloso, ai sensi dell'art. 2119 c.c.

Il soggetto (a qualunque titolo destinatario del presente documento) che riscontri il comportamento illecito del dirigente, ai sensi del Modello 231/01, informa tempestivamente l'Organismo di Vigilanza. Fatti i riscontri del caso, l'OdV fornirà una relazione circostanziata al responsabile della direzione Human Resources e alla Direzione generale, la quale potrà chiedere gli opportuni chiarimenti al/ai dirigenti per via scritta, entro 7 giorni da quello in cui ne sia venuto a conoscenza. La Direzione generale, inoltre, fornirà debita e tempestiva informativa al Consiglio di amministrazione ed al Collegio dei sindaci nella prima riunione consiliare utile a far data da quando la violazione sia stata accertata.

Acclarata la violazione ed analizzatene le conseguenze, il Consiglio d'amministrazione applicherà la sanzione nei termini già descritti.

Qualora il Consiglio di amministrazione dovesse decidere di non procedere, esso dovrà darne motivazione scritta all'Organismo di Vigilanza.

5.2.3. Dirigenti con responsabilità strategiche

Valendo per i dirigenti in posizione apicale quanto già precedentemente enunciato per i dirigenti, in caso di violazione l'Organismo di Vigilanza dovrà informare il Collegio dei sindaci e tutti gli amministratori della notizia di una avvenuta violazione del Modello, commessa da parte del Direttore generale e/o del Vicedirettore generale. Il Consiglio, procedendo anche ad autonomi accertamenti e sentito il Collegio dei sindaci, procederà agli opportuni provvedimenti già previsti e descritti nel paragrafo precedente.

Qualora il Consiglio di amministrazione dovesse decidere di non procedere dovrà darne motivazione scritta all'Organismo di Vigilanza.

5.2.4. Amministratori

L'Organismo di Vigilanza dovrà informare il Collegio dei sindaci e tutti gli amministratori della notizia di una avvenuta violazione del Modello, commessa da parte di uno o più amministratori. Il Consiglio, procedendo anche ad autonomi accertamenti e sentito il Collegio dei sindaci, procederà agli opportuni provvedimenti previsti dal codice civile.

5.2.5. Sindaci

L'Organismo di Vigilanza dovrà informare tutti i Sindaci e il Consiglio di amministrazione della notizia di una avvenuta violazione del presente Modello commessa da parte di uno o più Sindaci.

Il Collegio dei sindaci, procedendo anche ad autonomi accertamenti e sentito il Consiglio di amministrazione, procederà agli opportuni provvedimenti previsti dal codice civile.

5.2.4. Consulenti, partners e fornitori

Ogni comportamento posto in essere da consulenti, *partners*, fornitori in contrasto con le linee di condotta indicate dal presente Modello e tale da comportare il rischio di commissione di un reato sanzionato dal Decreto potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali, la risoluzione del rapporto o ogni altra sanzione contrattuale appositamente prevista, fatta salva l'eventuale richiesta di risarcimento qualora dal comportamento derivino danni concreti alla Banca, come nel caso di applicazione da parte dell'Autorità giudiziaria delle sanzioni previste dal Decreto.

6. FORMAZIONE, RIESAME E AGGIORNAMENTO DEL MODELLO 231

Il Modello 231 è portato a conoscenza di tutti i Destinatari mediante appositi interventi di comunicazione e formazione al fine di garantire la massima diffusione dei principi ispiratori e delle regole di condotta. Esso è disponibile nell'area documentale dell'intranet aziendale, nonché pubblicato sul sito internet della Banca.

Il Modello 231 viene riesaminato periodicamente dall'Organismo di Vigilanza, al fine di verificarne l'effettività, l'adeguatezza, il mantenimento nel tempo dei requisiti di efficacia e funzionalità, curandone il relativo aggiornamento.

L'Organismo nello svolgimento dei suoi compiti si avvale delle competenti strutture della Banca attraverso il coordinamento della Direzione Generale.

Ai fini di un migliore e più efficace espletamento dei propri compiti e delle proprie funzioni, l'Organismo si avvale del Responsabile della funzione di Conformità alle norme.

L'Organismo riferisce periodicamente al Consiglio di amministrazione e al Direttore sullo stato di applicazione e sulle eventuali necessità di aggiornamento, proponendo le eventuali integrazioni e/o modifiche del Modello 231.

Gli aggiornamenti del Modello 231 sono realizzati con cadenza minima biennale salvo il caso in cui siano introdotti nel D.Lgs. 231 nuovi reati di rilievo per il settore bancario che rendano necessario un tempestivo aggiornamento, ovvero la Banca svolga nuove attività sensibili alla realizzazione del rischio – reato.

PARTE SPECIALE

PREMESSA

La parte speciale del MOG è suddivisa in ventuno sezioni, che corrispondono alle categorie di reati-presupposto indicati dal D.lgs. 231; in ciascuna sezione sono trattate le singole fattispecie di reato annoverate, le aree cd. sensibili, ovvero le attività in cui il livello di realizzazione delle fattispecie criminose risulta essere maggiore, nonché, infine, le norme di comportamento previste dalla Banca per prevenire la realizzazione di differenti categorie di reati, che si sostanziano in obblighi e divieti imposti ai dipendenti della Banca.

La realizzazione di tale parte speciale è stata preceduta dall'analisi dei reati previsti dal D. Lgs. 231 e dalla preliminare individuazione – attraverso lo svolgimento di colloqui e la somministrazione di specifici questionari ai *key-officers* – delle possibili modalità di realizzazione della condotta illecita all'interno dei processi aziendali della Banca (anche attraverso l'esemplificazione di alcune fattispecie concrete).

1. DELITTI CONTRO LA PUBBLICA AMMINISTRAZIONE

1.1. Le fattispecie di reato

Per quanto concerne i rapporti con la Pubblica Amministrazione, gli artt. 24 e 25 del Decreto prevedono quali reati presupposto le seguenti fattispecie di reato:

- Malversazione di erogazioni pubbliche (art. 316-bis c. p.)
- Indebita percezione di erogazioni pubbliche (art. 316-ter c. p.)
- Concussione (art. 317 c. p.)
- Corruzione per l'esercizio della funzione (art. 318 c. p.)
- Corruzione per un atto contrario ai doveri d'ufficio (art. 319 c. p.)
- Corruzione in atti giudiziari (art. 319-ter c. p.)
- Concussione, Induzione indebita a dare o promettere utilità (art. 319-quater c. p.)
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c. p.)
- Pene per il corruttore (art. 321 c. p.)
- Istigazione alla corruzione (art. 322 c. p.)
- Peculato, concussione, 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.)
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640, co.2 c. p.)
- Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c. p.)
- Frode informatica (art. 640-ter c. p.).

1.2. Le attività sensibili

Le attività, all'interno delle quali si realizzano contatti con rappresentanti di enti pubblici e che quindi possono essere identificate come potenzialmente sensibili per la realizzazione di delitti contro la Pubblica Amministrazione, sono di seguito riepilogate:

- predisposizione dei dati per la partecipazione alle procedure ad evidenza pubblica per l'aggiudicazione/rinnovo di servizi di tesoreria e cassa in favore di Enti Pubblici – Processo di Tesoreria Enti;
- concessione e gestione di finanziamenti agevolati alla propria clientela (contributi o garanzie dello Stato, crediti agrari agevolati) – Processo di Gestione del Credito;
- esecuzione dei mandati nell'ambito del servizio di tesoreria – Processo di Tesoreria Enti;
- gestione di finanziamenti pubblici ottenuti al fine di finanziare piani formativi del personale; gestione di tesorerie di enti pubblici – Processo di Gestione delle risorse umane;
- finanziamenti pubblici ottenuti per la ricostruzione e/o ristrutturazione dei punti operativi della Banca danneggiati in occasione di catastrofi naturali – Processo di Gestione delle Infrastrutture e Spese;
- finanziamenti pubblici concessi per le ristrutturazioni/restauri di sedi e/o edifici di proprietà o nella disponibilità della banca (leggi regionali) – Processo di Gestione delle Infrastrutture e Spese;
- contributi ricevuti dagli enti per i lavori di adeguamento antisismico delle infrastrutture (ad esempio anche dai singoli comuni) oppure finanziamenti pubblici ottenuti per la ricostruzione e/o ristrutturazione dei punti operativi della Banca danneggiati in occasione di catastrofi naturali – Processo di Gestione delle Infrastrutture e Spese;
- rendicontazione della destinazione dei finanziamenti agevolati – Processo di Gestione del Credito;
- predisposizione della documentazione per ottenere un finanziamento finalizzato al restauro di un immobile vincolato (tutela beni culturali) oppure nell'ambito della rendicontazione periodica – Processo di Gestione delle Infrastrutture e Spese;
- predisposizione della documentazione per ottenere un finanziamento finalizzato alla formazione del personale oppure nell'ambito della rendicontazione periodica – Processo di Gestione delle Risorse Umane;
- presentazione da parte della clientela delle domande di finanziamenti agevolati – Processo di Gestione del Credito;
- comunicazioni all'Ente in occasione della gestione del servizio di incasso pensioni – Processo di Gestione degli Incassi e Pagamenti;
- predisposizione della documentazione richiesta per le assunzioni agevolate o per i contratti di apprendistato e di inserimento e per la successiva verifica del rispetto dei presupposti e delle condizioni – Processo di Gestione delle Risorse Umane;

- predisposizione dei dati e della documentazione in occasione di versamenti obbligatori – Processo di Gestione delle Risorse Umane;
- predisposizione del bilancio d'esercizio da utilizzare nell'ambito della partecipazione a gara avente evidenza pubblica – Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- utilizzo delle deleghe di spesa attribuite – Processo di Gestione delle Infrastrutture e Spese;
- acquisizione di beni o servizi da parte di società o professionisti – Processo di Gestione delle Infrastrutture e Spese;
- assegnazione di beni a titolo di omaggio – Processo di Gestione delle Infrastrutture e Spese;
- assegnazione in godimento di un immobile non strumentale di proprietà della Banca – Processo di Gestione delle Infrastrutture e Spese;
- assunzione o avanzamento di grado di personale – processo di Gestione delle Risorse Umane;
- negoziazione titoli/collocamento prestiti obbligazionari emessi dalla Banca – Processo Finanza;
- concessione di linee di credito e cancellazione di posizioni debitorie – Processo di Gestione del Credito;
- trasmissione di dati in via telematica attraverso un database protetto oppure un software di proprietà della P.A. – Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- partecipazione in cause contro il personale – Processo di Gestione delle Risorse Umane;
- partecipazione in cause per recupero crediti o revocatorie fallimentari - Processo di Gestione del Credito.

1.3. Regole di comportamento

Tutti coloro che operano per conto della Banca a contatto con la Pubblica Amministrazione e con le Istituzioni Pubbliche, sono tenuti ad assolvere ai propri compiti con integrità, indipendenza, correttezza e trasparenza. Per essi è in particolare fatto divieto di:

- instaurare relazioni personali di favore, influenza, ingerenza idonee a condizionare, direttamente o indirettamente, l'esito del rapporto;
- operare, in caso di effettuazione di procedure ad evidenza pubblica, in violazione della legge e delle corrette prassi commerciali, creando accordi di cartello con altri partecipanti, ovvero inducendo la P.A. ad operare indebitamente a favore della Banca;
- destinare contributi/sovvenzioni/finanziamenti pubblici a finalità diverse da quelle per le quali sono stati ottenuti;
- esibire alla Pubblica Amministrazione documenti/dati falsi o alterati;
- omettere informazioni dovute al fine di orientare a proprio favore le decisioni della Pubblica Amministrazione;

- tentare in qualsivoglia modalità di influenzare le decisioni della Pubblica Amministrazione in favore della Banca;
- chiedere o indurre i soggetti della Pubblica Amministrazione a trattamenti di favore;
- promettere o effettuare erogazioni in denaro per finalità diverse da quelle istituzionali e di servizio;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;
- promettere o concedere omaggi/regalie che non siano coerenti con quanto previsto nel Codice Etico di Comportamento;
- effettuare pagamenti di parcelle maggiorate ai legali, ai professionisti o ad altri soggetti coinvolti in processi di rappresentanza legale della Banca al fine di costituire fondi per comportamenti corruttivi;
- adottare comportamenti contrari alle leggi e al Codice Etico di Comportamento, in tutte le fasi del procedimento anche a mezzo di professionisti esterni e soggetti terzi per favorire indebitamente gli interessi della Banca nei confronti della Pubblica Amministrazione;
- promettere o accordare somme di denaro, doni, prestazioni gratuite o vantaggi e utilità di qualsiasi natura a pubblici ufficiali o persone incaricate di pubblico servizio al fine di favorire interessi della Banca;
- promettere o accordare somme di denaro, doni, prestazioni gratuite o vantaggi e utilità di qualsiasi natura a parenti o affini entro il secondo grado di pubblici ufficiali o persone incaricate di pubblico servizio, al fine di favorire interessi della Banca;
- promettere o accordare a terzi soggetti somme di denaro, doni, prestazioni gratuite o vantaggi e utilità di qualsiasi natura per i quali ne sia conosciuta, o comunque ragionevolmente evidente, la condivisione con pubblici ufficiali o persone incaricate di pubblico servizio, al fine di favorire interessi della Banca;
- tenere condotte ingannevoli che possano indurre la Pubblica Amministrazione in errore nella valutazione tecnico-economica dei prodotti e servizi offerti/forniti.

Normativa aziendale di riferimento: Al fine di prevenire la commissione dei suddetti reati, oltre alle previsioni contenute nel Codice etico, rilevano le previsioni di cui al Regolamento credito, alla Politica di gruppo in materia di concessione e perfezionamento del credito, al Sistema delle deleghe e dei poteri deliberativi in materia creditizia Banca delle Terre Venete, in base ai quali vengono delimitati i poteri di firma e di spesa per le singole operazioni contemplate da tali fonti. Rileva altresì il Sistema dei Controlli Interni che si è sopra descritto nella Parte Generale.

2. REATI INFORMATICI

2.2. Le fattispecie di reato

La Legge n. 48 del 18 marzo 2008, in particolare con l'articolo 7, introducendo nel D.Lgs. 231 l'art. 24-bis, ha esteso la responsabilità amministrativa dell'ente (al ricorrere di un vantaggio o di un interesse per quest'ultimo) alle seguenti fattispecie di reato:

- Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter c.p.);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (Art. 615-quater c.p.);
- Diffusione 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.);
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617-quinquies c.p.);
- Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis c.p.);
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico 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.);

  (Le ultime due disposizioni si aggiungono al preesistente art. 640-ter c.p., Frode informatica, anch'esso richiamato nel D.Lgs. 231 qualora sia commesso a danno di un ente pubblico, che punisce la condotta di chi procura a sé o ad altri un ingiusto profitto con altrui danno alterando informazioni o programmi contenuti in un sistema informativo o telematico o ad esso pertinenti);
- Documenti informatici (Art. 491-bis c.p.).

2.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei delitti informatici sono seguito riepilogate:

- gestione degli strumenti informatici – Processo Disposizioni normative;
- predisposizione di documenti informatici pubblici o privati aventi efficacia probatoria – Processo Contabilità, bilancio e segnalazioni di vigilanza e Processo del risparmio.

2.3. Regole di comportamento

Ai destinatari del presente Modello, è fatto divieto, in generale, di porre in essere comportamenti o concorrere alla realizzazione di condotte che possano rientrare nelle fattispecie di reato innanzi indicate; sono altresì proibite le violazioni ai principi ed alle regole previste nel Codice Etico di Comportamento, nonché alle norme aziendali regolamentari sopra richiamate.

In particolare, per ciò che concerne i servizi informatici è fatto divieto di:

a) utilizzare le risorse informatiche assegnate dalla Banca (es. personal computer fissi o portatili o altri dispositivi mobili) per finalità diverse da quelle lavorative;

b) effettuare download illegali o trasmettere a soggetti terzi contenuti protetti dal diritto d'autore;

c) alterare documenti elettronici, pubblici o privati, con finalità probatoria;

d) accedere, senza averne la autorizzazione, ad un sistema informatico o telematico o trattenersi contro la volontà espressa o tacita di chi ha diritto di escluderlo (il divieto include sia l'accesso ai sistemi informativi interni che l'accesso ai sistemi informativi di enti concorrenti, pubblici o privati, allo scopo di ottenere informazioni su sviluppi commerciali o strategici);

e) procurarsi, riprodurre, diffondere, comunicare, ovvero portare a conoscenza di terzi codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui protetto da misure di sicurezza;

f) procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti, ovvero di favorire l'interruzione, totale o parziale, l'alterazione del suo funzionamento (il divieto include la trasmissione di virus con lo scopo di danneggiare i sistemi informativi di enti concorrenti);

g) intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;

h) distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici (il divieto include l'intrusione non autorizzata nel sistema informativo di società concorrente, con lo scopo di alterare informazioni e dati di quest'ultima);

i) distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;

j) distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ostacolarne gravemente il funzionamento;

k) distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ostacolarne gravemente il funzionamento;

l) aggirare o tentare di aggirare i sistemi di sicurezza aziendali (es: Antivirus, Firewall, Proxy server, etc.);

m) lasciare il proprio Personal Computer incustodito e senza protezione password.

Ai destinatari del Modello 231 è fatto altresì obbligo di:

a) utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;

b) custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi della Banca, evitando che terzi soggetti possano venirne a conoscenza;

c) aggiornare periodicamente le password, secondo le regole aziendali;

d) installare software/programmi aggiuntivi rispetto a quelli esistenti o che verranno installati per esigenze aziendali, previa verifica del contenuto da parte del Responsabile della funzione di sicurezza informatica;

e) garantire la tracciabilità dei documenti prodotti;

f) assicurare meccanismi di protezione dei file, quali, ad esempio, password;

g) utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste.

I provider di servizi inerenti ai sistemi informativi, coerentemente con le previsioni contrattuali vigenti, devono:

a) installare a tutti gli utenti esclusivamente software originali, debitamente autorizzati o licenziati;

b) verificare la sicurezza della rete e dei sistemi informativi aziendali;

c) monitorare i cambiamenti organizzativi o tecnici che potrebbero determinare l'esposizione del sistema informativo a nuove minacce, rendendo inadeguato il sistema di controllo accessi;

d) valutare l'opportunità di chiedere informazioni e chiarimenti a tutte le funzioni aziendali e a tutti coloro che si occupano o si sono occupati dell'operazione sensibile;

e) verificare, per quanto di loro competenza, il rispetto delle norme aziendali;

f) informare tempestivamente l'Organismo di fatti o circostanze significative riscontrate nello svolgimento delle attività sensibili con espresso riferimento ai delitti informatici.

Nella gestione dei sistemi informativi, le norme aziendali danno attuazione ai seguenti principi:

a) eventuali server applicativi centralizzati siano ospitati in locali dedicati e messi in sicurezza;

b) l'accesso logico ai sistemi informativi sia protetto da user-id e password utente con scadenza periodica;

c) le credenziali di accesso ai sistemi siano prontamente eliminate per il personale dimesso e ogni utente disponga di una user-id e password personale;

d) la rete sia protetta da firewalls e da software antivirus/antispam, ripetutamente aggiornati;

e) i backup dei dati residenti su eventuali server siano salvati con frequenza giornaliera ed i supporti adeguatamente conservati.

Eventuali integrazioni delle suddette Aree di attività a rischio potranno essere disposte dall'Organismo e successivamente sottoposte all'approvazione del Consiglio di Amministrazione.

Normativa aziendale di riferimento: Al fine di prevenire la commissione dei suddetti reati, oltre alle previsioni contenute nel Codice etico, rilevano le previsioni di cui alla Politica di gruppo in

materia di Funzioni Aziendali e Servizi ICT Critici, Politica di gruppo per la Sicurezza delle Informazioni, Politica di Gruppo in materia di utilizzo delle risorse informatiche aziendali, Regolamento generale, Norme operative di processo - Internet Banking, Deleghe operative poteri di spesa, Regolamento Privacy. Rileva altresì il Sistema dei Controlli Interni che si è sopra descritto nella Parte Generale.

Si precisa comunque che la rete dati, *i firewall*, l'antivirus e tutti i sistemi di sicurezza sono gestiti in *outsourcing* dalla società BCC SI.

3. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

3.1. Le fattispecie di reato

L'art. 15, comma 7 della legge 23 luglio 2009, n. 99 recante disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia introduce modifiche all'articolo 25-bis del decreto legislativo n. 231 e prevede l'inserimento nel decreto dell'articolo 25-bis.1, riguardante la responsabilità amministrativa degli enti per delitti contro l'industria e il commercio nonché dell'articolo 25-novies, riguardante la responsabilità amministrativa degli enti per delitti in materia di violazione del diritto d'autore.

L'art. 25-bis prevede ora anche i seguenti reati:

- contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

L'art. 25-bis.1 prevede i seguenti reati:

- Turbata libertà dell'industria o del commercio (art. 513 c.p.);
- Frode nell'esercizio del commercio (art. 515 c.p.);
- Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
- Vendita di prodotti industriali con segni mendaci (Art. 517 c.p.);
- Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-ter c.p.);
- Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-quater. c.p.);
- Illecita concorrenza con minaccia o violenza (art. 513-bis. c.p.);
- Frodi contro le industrie nazionali (art. 514 c.p.).

3.2. Le attività sensibili

Con riguardo ai delitti contro l'industria e il commercio si precisa che non si ravvisano attività sensibili alla realizzazione di questa categoria di reati.

3.3. Regole di comportamento

I delitti contro l'industria ed il commercio sono certamente attinenti all'attività delle società industriali e commerciali, mentre non risultano rientrare nella casistica delle attività propriamente bancarie.

4. FALSITÀ IN MONETE, CARTE DI PUBBLICO CREDITO E VALORI DI BOLLO

4.1. Le fattispecie di reato

I reati indicati nell'art. 25-bis del Decreto in tema di falsità in monete, carte di pubblico credito e valori di bollo, sono i seguenti:

- 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 dei 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.).

4.2. Le attività sensibili

Le attività che prevedono la gestione di banconote e monete che possono essere identificate come potenzialmente sensibili per la realizzazione dei reati di falsità in monete, in carte di pubblico credito e in valori di bollo sono di seguito riepilogate:

- attività di sportello, in relazione alle operazioni effettuate per cassa – Processo di sportello (gestione del contante e altri valori di cassa);
- caricamento degli ATM – Processo di sportello (gestione del contante e altri valori di cassa).

4.3. Regole di comportamento

Le strutture della Banca, nonché le strutture esterne da essa incaricate, a qualsiasi titolo coinvolte nella gestione dei valori, sono tenute ad osservare le modalità esposte nel presente modello organizzativo, le disposizioni di legge esistenti in materia, la normativa interna, ivi incluso quanto previsto nel Codice Etico di Comportamento.

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

- devono essere appositamente incaricati;
- sono tenuti ad operare con onestà, integrità, correttezza e buona fede;
- 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 quelli sospetti di falsità. L'attività di identificazione può avvenire anche attraverso l'utilizzo di apparecchiature (omologate in conformità alla normativa vigente) 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;
- in particolare, in presenza di banconote sospette di falsità, gli addetti sono tenuti ad effettuare le segnalazioni previste dalla normativa interna di riferimento sopra richiamata;
- 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. 231 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. 231 e, più in particolare, a titolo meramente esemplificativo e non esaustivo, di:

- mettere in circolazione, in concorso o meno con terzi, valori falsi;

  si sottolinea che 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; 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 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 modello organizzativo.

Normativa aziendale di riferimento: Al fine di prevenire la commissione dei suddetti reati, rilevano le Procedure interne gestione valori e contante e segnalazione sospetti di falsità.

5. REATI SOCIETARI

5.1. Le fattispecie di reato

Si provvede di seguito ad elencare i reati societari indicati all'art. 25-ter del Decreto.

- False comunicazioni sociali (art. 2621 c. c.);
- Impedito controllo (art. 2625, co. 2, c. c.);
- Indebita restituzione dei conferimenti (art. 2626 c. c.);
- Illegale ripartizione degli utili o 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 di interessi (art. 2629-bis c. c.);
- Formazione fittizia del capitale (art. 2632-bis c. c.);
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c. c.);
- Corruzione tra privati (art. 2635 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, co. 1 e co. 2, c. c.).

5.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei reati societari sono quelle in cui operano i soggetti apicali e relative a:

- gestione dei dati contabili presenti nel sistema informatico – Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- applicazione dei criteri dettati dalla legge e dei principi contabili di riferimento – Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- predisposizione dei prospetti richiesti per la sollecitazione all'investimento – Processo di Governo e Processo Finanza;
- messa a disposizione dei dati e delle informazioni oggetto della revisione legale dei conti affidata a soggetto esterno – Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- messa a disposizione di documenti per le verifiche da parte del Collegio Sindacale, della Società di Revisione o dei Soci – Processo di Governo, Processo di Disposizioni normative e Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;

- restituzione dei conferimenti – Processo: di Disposizioni normative e Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- ripartizione di utili o acconti sugli utili e ripartizione delle riserve – Processo di Disposizioni normative e Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- acquisto o sottoscrizione di azioni – Processo di Disposizioni normative e Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- esposizione di dati in occasione di operazioni straordinarie (riduzioni del capitale sociale, fusione, scissione) – Processo di Disposizioni normative e Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- deliberazione di operazioni da parte del Consiglio di Amministrazione nelle quali è presente un conflitto di interesse da parte dell'amministratore – Processo del Credito e processo di Gestione delle infrastrutture e spese;
- aumento del capitale sociale – Processo di Disposizioni normative e Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- liquidazione della Banca – Processo di Disposizioni normative e Processo di Contabilità Bilancio e Segnalazioni di Vigilanza;
- utilizzo delle deleghe di spesa attribuite – Processo di Gestione delle Infrastrutture e Spese;
- acquisizione di beni o servizi da parte di società o professionisti – Processo di Gestione delle Infrastrutture e Spese;
- assegnazione di beni a titolo di omaggio – Processo di Gestione delle Infrastrutture e Spese;
- assegnazione in godimento di un immobile non strumentale di proprietà della Banca – Processo di Gestione delle Infrastrutture e Spese;
- assunzione o avanzamento di grado di personale – processo di Gestione delle Risorse Umane;
- negoziazione titoli/collocamento prestiti obbligazionari emessi dalla Banca – Processo Finanza;
- concessione di linee di credito e cancellazione di posizioni debitoria – Processo del Credito;
- predisposizione di progetti, prospetti e documentazione da sottoporre all'approvazione dell'Assemblea – Processo di Disposizioni normative;
- rappresentazione e diffusione di informazioni relative alla situazione economica patrimoniale e finanziaria della Banca e/o di propri Clienti – Processo Finanza e Processo di Gestione del Credito;
- comunicazioni previste da norma di legge (ad esempio: segnalazioni di vigilanza, legge sull'usura, norme sulla privacy, norma in materia di riciclaggio, normative Consob, etc.), regolamenti o in occasione di ispezioni o verifiche delle Autorità di Vigilanza (Consob, Banca d'Italia) – Processo di Contabilità Bilancio e Segnalazioni di Vigilanza – Processo Finanza – Processo Disposizioni normative.

5.3. Regole di comportamento

Il sistema di organizzazione della Banca deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione dei ruoli, e in particolare, per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative. Gli strumenti organizzativi della Banca (organigramma, circolari interne, comunicazioni e ordini di servizio, regolamenti e procedure, ecc.) devono essere improntati a principi generali di:

a) conoscibilità all'interno della Banca;

b) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;

c) chiara descrizione delle linee di riporto (flussi informativi, ivi inclusi quelli verso l'Organismo).

Tutti coloro che, per posizione e ruolo ricoperto, assumono singolarmente o collegialmente decisioni e deliberazioni relative alla gestione della Banca e al relativo governo, e tutti i dipendenti che a qualunque titolo collaborino in tali attività, sono tenuti alle seguenti condotte:

- osservanza delle norme di legge, dello Statuto Sociale, dei Regolamenti e delle normative interne relative al funzionamento degli organi sociali;
- correttezza, liceità ed integrità nella formazione e nel trattamento dei dati, dei documenti contabili, delle segnalazioni alle Autorità di Vigilanza e del bilancio della Banca (situazione economica, patrimoniale e finanziaria), nonché nella loro rappresentazione all'esterno, anche ai fini di garantire i diritti dei Soci;
- rispetto dei principi di lealtà, correttezza, collaborazione e trasparenza nelle attività e nelle relazioni con le funzioni ed autorità di controllo e di revisione;
- applicazione dei principi della riservatezza, della correttezza, della trasparenza, della chiarezza della veridicità e della completezza nelle attività afferenti la circolazione e la diffusione di notizie che riguardano la Banca, sia all'interno che all'esterno;
- chiarezza, veridicità e conformità alle politiche ed ai programmi aziendali, delle comunicazioni della Banca verso l'esterno.

Tutti coloro che, per posizione e ruolo ricoperto, assumono singolarmente o collegialmente decisioni e deliberazioni relative alla gestione dei rapporti che la Banca intrattiene con soggetti terzi privati, e tutti i dipendenti che a qualunque titolo collaborino in tali attività, sono tenuti alle seguenti condotte:

- rispettare la distinzione dei ruoli e delle inerenti responsabilità nei rapporti con i soggetti terzi;
- adottare decisioni responsabili nella definizione del prezzo di offerta e delle condizioni e tempi di pagamento (e relative penali);
- adottare decisioni responsabili nella scontistica e nella definizione di eventuali risoluzioni transattive in caso di contestazioni;
- rispettare i principi di lealtà, correttezza, collaborazione e trasparenza nelle attività e nella gestione dei rapporti contrattuali con soggetti terzi privati;

- selezionare i soggetti terzi, con cui intrattenere rapporti contrattuali e/o societari, attraverso criteri identificativi e valutativi che consentano di "accreditare" gli stessi soggetti presso la Banca (corredo informativo-istruttorio, eventuale rating di legalità ex art. 5-ter del D.L. n. 1/2012, così come modificato dall'art. 1, comma 1-quinquies, del D.L. n. 29/2012, convertito, con modificazioni, dalla Legge n. 62/2012, presenza di modello organizzativo ai sensi del D.Lgs. 231);
- considerare e valutare specifici "indici di anomalia" dei rapporti contrattuali con soggetti terzi, a titolo esemplificativo (non esaustivo): 1. l'intermediario opera normalmente in una diversa linea di business da quello per cui è stato impegnato; 2. l'intermediario è legato o è in stretta collaborazione con un funzionario pubblico; 3. proposta dell'intermediario di operazioni da effettuarsi con modalità, frequenza o dimensioni che risultano illogiche, inusuali o tali da denotare intenti dissimulatori, soprattutto se non vi sono plausibili giustificazioni economiche o finanziarie; 4. operazioni con controparti insediate in aree geografiche appartenenti a Paesi blacklist;
- effettuare controlli preventivi e riferire gerarchicamente sull'operatività in relazione alle citate anomalie;
- rispettare i blocchi dell'operatività eventualmente disposti dalla Banca in relazione alle citate anomalie;
- includere il rispetto del Modello 231 della Banca nei contratti con "Soggetti Terzi";
- non effettuare il pagamento delle spettanze di soggetti terzi attraverso sistemi inusuali, artatamente elaborati e/o triangolazioni con ulteriori soggetti;
- segnalare all'Organismo gli scostamenti e le deroghe alla policy aziendale, ed alle disposizioni di servizio in materia;
- segnalare all'Organismo le infrazioni al Codice Etico di Comportamento della Banca.

L'Organismo verifica periodicamente, con il supporto delle altre funzioni competenti, il sistema di deleghe e procure in vigore e la loro coerenza con tutto il sistema delle comunicazioni organizzative, raccomandando eventuali modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

Normativa aziendale di riferimento: Al fine di prevenire la commissione dei suddetti reati, oltre alle previsioni contenute nel Codice Etico, rilevano le seguenti fonte interne: Politiche di Governo societario del Gruppo Iccrea, Regolamenti di gestione dei rapporti con i soci, Politica in materia di Trasparenza, Regolamento Credito, Poteri delegati credito, Regolamento finanza, Regolamento flussi informativi, Regolamento generale, Politiche remunerazione, Poteri delegati, Deleghe operative poteri di spesa, Statuto, Politiche e procedure deliberative operazioni con soggetti collegati, Statuto sociale.

Per la prevenzione dei reati societari, rileva altresì il Sistema dei Controlli Interni che si è sopra descritto nella Parte Generale, oltre alla più generale attività di *compliance* affidata alla Capogruppo ed ai controlli da parte del Collegio Sindacale, nonché da parte della Società di Revisione.

6. REATI CON FINALITÀ DI TERRORISMO O EVERSIONE DELL'ORDINE DEMOCRATICO

6.1. Le fattispecie di reato

Di seguito sono elencati i delitti con finalità di terrorismo o di eversione dell'ordine democratico indicati all'art. *25-quater* del Decreto.

- Associazioni sovversive (art. 270 c. p.);
- Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordinamento democratico (art. 270-bis c. p.);
- Assistenza agli associati (art. 270- ter c. p.);
- Arruolamento con finalità di terrorismo anche internazionale (art. 270-quater c. p.);
- Addestramento ad attività con finalità di terrorismo anche internazionale (art. 270-quinquies c. p.);
- Condotte con finalità di terrorismo (art. 270-sexies c. p.);
- Banda armata e formazione e partecipazione e assistenza ai partecipi di cospirazione o di banda armata (artt. 306 e 307 c. p.);
- Reati diversi da quelli indicati nel Codice Penale e nelle leggi speciali, previsti dall'art. 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo di New York del 9.12.1999.

6.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei delitti con finalità di terrorismo o di eversione dell'ordine democratico sono di seguito elencate:

- finanziamenti – Processo del credito;
- gestione delle liberalità – Processo Relazioni esterne;
- gestione degli immobili non strumentali di proprietà della Banca – Processo di gestione delle infrastrutture e delle spese;
- operatività di sportello con la clientela (apertura C/C – bonifici) – Processo incassi e pagamenti, Processo Risparmio.

6.3. Regole di comportamento

Tutti coloro che sono coinvolti nell'attività bancaria di raccolta del risparmio, erogazione del credito e servizi di pagamento, in occasione dell'instaurarsi di rapporti con clienti, sono tenuti ad attivarsi per una esaustiva conoscenza e adeguata verifica del cliente, di chi opera per conto di quest'ultimo e dell'eventuale titolare effettivo, in modo che sia possibile una ricostruzione il più

possibile approfondita delle modalità con cui l'operazione viene effettuata e delle ragioni per cui viene richiesta.

In particolare, essi sono tenuti alle seguenti condotte:

- osservanza delle norme di legge e della normativa interna riguardante gli obblighi di identificazione, registrazione e adeguata verifica della clientela e di segnalazione delle operazioni sospette;
- osservanza delle norme di lotta contro il terrorismo riguardanti il divieto di finanziare soggetti che compiono o sono sospettati di compiere reati contro la libertà delle persone (come ad esempio, reato di tratta di persone, riduzione in schiavitù, sfruttamento della prostituzione, favoreggiamento, sfruttamento di minori, ecc.) o di collaborare o concedere liberalità ad associazioni terroristiche o persone sospette di terrorismo.

Normativa aziendale di riferimento: Al fine di prevenire la commissione dei suddetti reati, oltre alle previsioni contenute nel Codice Etico, rilevano le seguenti fonte interne: Politica di Gruppo Governo e gestione del rischio di riciclaggio e finanziamento al terrorismo, Regolamento generale, Poteri delegati, Deleghe operative in materia di spesa, Regolamento funzione AML Capogruppo, Politica di Gruppo in materia di Operazioni di Maggior Rilievo.

7. DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE E PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI

7.1. Le fattispecie di reato

Di seguito sono elencati i delitti contro la personalità individuale di cui all'art. 25-quinquies del Decreto:

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.);
- Prostituzione minorile (art. 600-bis c.p.);
- Pornografia minorile (art. 600-ter c.p.);
- Detenzione di materiale pornografico (600-quater c.p.);
- Pornografia virtuale (art. 600-quater.1 c. p.);
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.);
- Tratta di persone (art. 601 c.p.);
- Acquisto e alienazione di schiavi (art. 602 c.p.).

All'art. 25-quater.1, poi, il Decreto prevede la responsabilità dell'ente per la commissione di pratiche di mutilazione degli organi genitali femminili (art. 583 - bis c.p.).

7.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei delitti contro la personalità individuale sono di seguito elencate:

- finanziamenti – Processo del credito;
- gestione delle liberalità – Processo Relazioni esterne;
- gestione degli immobili non strumentali di proprietà della Banca – Processo di gestione delle infrastrutture e delle spese.

Quanto alle pratiche di mutilazione, esse all'evidenza non incontrano un fattore di rischio nello svolgimento dell'attività bancaria.

7.3. Regole di comportamento

Tutti coloro che sono coinvolti nell'attività bancaria di raccolta del risparmio, erogazione del credito, servizi di pagamento, in occasione dell'instaurarsi di rapporti con clienti, sono tenuti ad attivarsi per una esaustiva conoscenza ed adeguata verifica del cliente, di chi opera per conto di quest'ultimo e dell'eventuale titolare effettivo, in modo che sia possibile una ricostruzione il più possibile approfondita delle modalità con cui l'operazione viene effettuata e delle ragioni per cui viene richiesta.

In particolare, essi sono tenuti alla seguente condotta:

- osservanza delle norme di legge e della normativa interna riguardante gli obblighi di identificazione, registrazione e adeguata verifica della clientela e di segnalazione delle operazioni sospette di cui alla normativa antiriciclaggio (D.Lgs. n. 231/2007);
- osservanza delle norme di lotta contro il terrorismo riguardanti il divieto di finanziare soggetti che compiono o sono sospettati di compiere reati contro la libertà delle persone (come ad esempio, reato di tratta di persone, riduzione in schiavitù, sfruttamento della prostituzione, favoreggiamento, sfruttamento di minori, ecc.) o di collaborare o concedere liberalità ad associazioni terroristiche o persone sospette di terrorismo.

Normativa aziendale di riferimento: Al fine di prevenire la commissione dei suddetti reati, oltre alle previsioni contenute nel Codice Etico, rilevano le seguenti fonte interne: Politiche di gestione del rischio di riciclaggio e di finanziamento al terrorismo, Regolamento generale, Regolamento credito, Poteri delegati, Deleghe operative in materia di spesa.

8. REATI E ILLECITI AMMINISTRATIVI DI MANIPOLAZIONE DEL MERCATO E DI ABUSO DI INFORMAZIONI PRIVILEGIATE

8.1. Le fattispecie di reato

Di seguito sono elencati i reati di abuso di mercato indicati all'art. 25-sexies del Decreto.

I reati in esame, unitamente all'art. 25-sexies del D.Lgs. 231, sono stati introdotti dalla Legge n. 62 del 18 aprile 2005 – c.d."Legge Comunitaria 2004":

- Abuso di informazioni privilegiate (art. 184 TUF);
- Manipolazione del mercato (art. 185 TUF).

La Legge Comunitaria 2004 ha altresì introdotto le due fattispecie di illecito amministrativo di abuso di informazione privilegiata e di manipolazione del mercato, caratterizzate dal fatto che le medesime condotte (disciplinate dai richiamati artt. 184 e 185 TUF) sono tenute con colpa e non con dolo:

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

Le sanzioni pecuniarie previste per le suddette fattispecie di illecito amministrativo sono applicate sia al soggetto che ha materialmente commesso il fatto, sia alla Banca, in virtù del rinvio effettuato dall'art. 187-quinquies TUF alle norme del D.Lgs. 231 in quanto applicabili.

8.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei reati e gli illeciti amministrativi di manipolazione del mercato e di abuso di informazioni privilegiate sono quelle relative a:

- consulenza e negoziazione per la clientela di strumenti finanziari – Processo Finanza;
- acquisto o vendita di prodotti finanziari nell'ambito della gestione del portafoglio di proprietà della Banca – Processo Finanza;
- consulenza e negoziazione di strumenti finanziari per la clientela affidata – Processo del Credito.

8.3. Regole di comportamento

Ai soggetti coinvolti nell'emissione e nell'intermediazione di strumenti finanziari è fatto obbligo di:

1. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione e comunicazione verso l'esterno di informazioni privilegiate, di notizie riservate, di operazioni sul capitale sociale;
2. evitare di pubblicare o divulgare notizie false o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio aventi ad oggetto strumenti finanziari quotati o non quotati ed idonei ad alterarne sensibilmente il prezzo.

Tutti i destinatari del presente Modello 231 sono tenuti alla osservanza:

- del vigente "Regolamento Finanza";
- della vigente "Policy operazioni personali dei soggetti rilevanti";
- della procedura del *Market Abuse*.

Normativa aziendale di riferimento: Al fine di prevenire la commissione dei suddetti reati, oltre alle previsioni contenute nel Codice Etico, rilevano le seguenti fonte interne: Politica di Gruppo in materia di gestione dei conflitti di interesse e incentivi nella presentazione dei servizi di investimento e accessori e nella distribuzione di prodotti assicurativi, Regolamento generale, Regolamento operativo in materia di Finanza Retail, Regolamento credito, Limiti e deleghe finanza di proprietà, procedura market abuse, Policy operazioni personali titoli. Rileva altresì il Sistema dei Controlli Interni, che si è sopra descritto nella Parte Generale.

9. REATI TRANSNAZIONALI

9.1. Le fattispecie di reato

La normativa contro il crimine organizzato transnazionale (legge 16 marzo 2006 n. 146) prevede che, a seguito del compimento dei reati di seguito descritti, l'ente possa essere ritenuto amministrativamente responsabile e, quindi, passibile di sanzioni.

I reati transnazionali sono:

- Associazione per delinquere (art. 416 c.p.);
- Associazione di tipo mafioso (art. 416-bis c.p.);
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del Testo Unico di cui al Presidente della Repubblica del 23 gennaio 1973 n. 43);
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del Testo Unico del Presidente della Repubblica del 9 ottobre 1990, n. 309);
- Disposizioni contro le immigrazioni clandestine (art. 12, comma 3, 3-bis, 3-ter e 5, del Testo Unico di cui al D.Lgs. 25 luglio 1998, n. 286).

Si definisce "reato transnazionale", a norma dell'art. 3 della Legge 16 marzo 2006 n. 146, *«il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:*

a) sia commesso in più di uno Stato;

b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;

c) ovverosia commesso in uno Stato ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;

d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.»

9.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei reati transnazionali sono quelle connesse alla gestione dei rapporti della clientela - Processo del Credito e Processo del risparmio.

Per la prevenzione dei reati transnazionali, il rischio maggiore è rappresentato dalla "controparte". In concreto, la principale attività di prevenzione per questa categoria di reati è rappresentata dalla verifica che la persona fisica o giuridica con la quale la Banca intrattiene rapporti commerciali sia in possesso di adeguati requisiti di professionalità e di onorabilità.

Alla luce della struttura e della natura delle condotte punite dalle fattispecie criminose in parola, si ritiene che esse non abbiano un impatto significativo sulla Banca e che, comunque, i rischi residuali di commissione di tali reati trovino adeguata copertura nei presidi già attualmente in essere, in particolare in materia di rispetto della normativa antiriciclaggio e delle misure di contrasto al terrorismo.

9.3. Regole di comportamento

Normativa aziendale di riferimento: Al fine di prevenire la commissione dei suddetti reati, oltre alle previsioni contenute nel Codice Etico, rilevano le seguenti fonte interne: Regolamento generale, Regolamento credito, Poteri delegati. Rileva altresì il Sistema dei Controlli Interni, che si è sopra descritto nella Parte Generale.

10. REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORMA ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO

10.1. Le fattispecie di reato

La legge delega n. 123/2007, in materia di "Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa", ha avviato una riforma sulla sicurezza del lavoro, attuata poi attraverso il D.Lgs n. 81/2008.

Tale provvedimento ha introdotto nel D.Lgs. 231 l'art. 25-septies, che ha esteso la responsabilità amministrativa dell'ente a due nuove fattispecie di reato:

- Omicidio colposo (art. 589 c.p.);
- Lesioni personali colpose gravi o gravissime (art. 590 c.p.).

Tale responsabilità, peraltro, è subordinata alla condizione che tali reati si realizzino in conseguenza della violazione delle norme poste a tutela della salute e della sicurezza sul lavoro.

10.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro sono quelle relative alla gestione dei luoghi e degli spazi in cui si svolge l'attività lavorativa e dei mezzi e degli strumenti materiali in essa adoperati – Processo Disposizioni normative.

10.3. Regole di comportamento

La politica aziendale in tema di salute e sicurezza sul lavoro deve essere diffusa, compresa, applicata ed aggiornata a tutti i livelli organizzativi. 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.

Le Strutture della Banca, a qualsiasi titolo coinvolte nella gestione dei rischi in materia di salute e sicurezza sul lavoro, come pure tutti i dipendenti, 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 di Comportamento.

In particolare, tutte le Strutture/figure sono tenute - nei rispettivi ambiti - a:

- definire gli obiettivi per la sicurezza e la salute dei lavoratori e l'identificazione in continuo dei pericoli;
- garantire un adeguato livello di informazione/formazione dei dipendenti e dei fornitori, sul sistema di gestione della sicurezza e salute definito dalla Banca e sulle conseguenze derivanti da un mancato rispetto delle norme di legge, nonché delle regole di comportamento e controllo definite dalla Banca medesima;
- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro, ai fini della protezione collettiva ed individuale, anche in ordine all'utilizzo degli strumenti lavorativi;
- segnalare immediatamente al Datore di Lavoro, le deficienze degli strumenti ovvero dei mezzi forniti dallo stesso, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente, nell'ambito delle loro competenze, per eliminare o ridurre tali deficienze, dandone notizia al Rappresentante dei Lavoratori per la Sicurezza (RLS);
- sottoporsi ai controlli sanitari previsti;
- definire e aggiornare (in base a cambiamenti nella struttura organizzativa ed operativa della Banca) le procedure specifiche per la prevenzione di infortuni, malattie e delle emergenze;
- adeguare le risorse umane in termini di numero e qualifiche professionali e materiali, necessarie al raggiungimento degli obiettivi prefissati dalla Banca per la sicurezza e la salute dei lavoratori;
- provvedere alla manutenzione ordinaria e straordinaria degli strumenti, degli impianti, dei macchinari e, in generale, delle strutture aziendali;

- applicare i provvedimenti disciplinari nel caso di violazione dei principi comportamentali, delle regole di cui al Codice Etico di Comportamento della Banca, dei protocolli e delle procedure aziendali tempo per tempo vigenti.

In ambito aziendale, dovrà essere portata a conoscenza dell'Organismo, a cura del Responsabile del Servizio di Prevenzione e Protezione dai rischi (RSPP), la comunicazione di ogni modifica e/o aggiornamento della documentazione relativa al sistema di gestione della sicurezza sul lavoro, ed in particolare:

- il Documento di Valutazione dei Rischi;
- il Piano di intervento e di evacuazione in emergenza;
- le procedure poste a presidio di funzioni connesse alla salute e sicurezza sul lavoro.

È inoltre previsto l'invio all'Organismo, da parte dell'RSPP, dei verbali relativi alle riunioni periodiche di prevenzione e protezione dai rischi (art. 35, D.Lgs. n. 81/2008), delle analisi ambientali e dei sopralluoghi negli uffici, nonché dei dati in merito agli eventuali infortuni verificatisi sul luogo di lavoro, ovvero a provvedimenti assunti dall'Autorità giudiziaria o da altre autorità in merito alla materia della sicurezza e salute sul lavoro.

L'Organismo svolge inoltre le attività di seguito indicate:

- esame delle segnalazioni riguardanti presunte violazioni del Modello ex D.Lgs.231, incluse le segnalazioni, non riscontrate con tempestività dai soggetti competenti, in merito ad eventuali carenze e inadeguatezze dei luoghi, delle attrezzature di lavoro e dei dispositivi di protezione, ovvero riguardanti una situazione di pericolo correlato alla salute ed alla sicurezza sul lavoro;
- monitoraggio della funzionalità del complessivo sistema preventivo adottato dalla Banca con riferimento al settore della salute e della sicurezza sul lavoro, in quanto organismo idoneo ad assicurare l'obiettività, l'imparzialità e l'indipendenza dal settore di lavoro sottoposto a verifica;
- segnalazione al Consiglio di Amministrazione, ovvero alle funzioni aziendali competenti, in merito agli aggiornamenti del Modello ex D.Lgs. 231, del sistema preventivo adottato dalla Banca ovvero delle procedure vigenti, che si rendessero necessari o opportuni in considerazione di carenze rilevate e a seguito di significativi cambiamenti intervenuti nella struttura organizzativa.

L'Organismo comunica annualmente al Consiglio di amministrazione, al Collegio sindacale e al Direttore i risultati della propria attività di vigilanza e controllo.

Normativa aziendale di riferimento: Al fine di prevenire il rischio di commissione dei suddetti reati, oltre al Codice Etico rilevano il Regolamento generale ed il Documento Valutazione dei Rischi; quest'ultimo, in particolare, contiene l'analisi dettagliata dei rischi per la salute e la sicurezza dei lavoratori e le relative misure volte a prevenirli e contrastarli.

11. REATI DI RICETTAZIONE, RICICLAGGIO, AUTORICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA

11.1. Le fattispecie di reato

Il D.Lgs. 21 novembre 2007, n. 231 (c.d. "Decreto Antiriciclaggio"), attuativo della III Direttiva Antiriciclaggio, ha introdotto nel D.Lgs. 231 l'art. 25-*octies* che disciplina le seguenti fattispecie di reato:

- 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.).

I reati di Riciclaggio e di Impiego di denaro, beni o utilità di provenienza illecita, precedentemente contemplati dalla legge 16 marzo 2006 n. 146 contro il crimine organizzato di carattere "transnazionale", vengono, con l'entrata in vigore del Decreto Antiriciclaggio, inseriti nel corpus del Decreto Antiriciclaggio stesso (con l'aggiunta del reato di ricettazione), andando a coinvolgere in tal modo la responsabilità amministrativa dell'ente anche in conseguenza di condotte poste in essere all'interno del territorio dello Stato e con effetti rilevanti nell'ambito dello stesso.

Il reato di autoriciclaggio è stato introdotto con l'art. 3 della Legge 15/12/2014 n. 186, pubblicata in G.U. n.292 del 17-12-2014, che ha modificato anche l'art. 25-octies del D.Lgs. 231.

11.2. Le attività sensibili

Le attività, identificate come potenzialmente sensibili per la realizzazione dei reati di ricettazione, riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita, sono di seguito riepilogate e prevedono la gestione dei rapporti della clientela:

- apertura e gestione dei conti correnti, dei dossier titoli e di altri rapporti continuativi – Processo Disposizione normative;
- erogazione del credito – Processo del Credito;
- collocamento di prestiti obbligazionari – Processo Finanza;
- registrazione di operazioni in AUI – Processo Disposizione normative;
- obblighi relativi alle singole operazioni bancarie (es.: "accertamenti bancari") – Processo Disposizione normative;
- segnalazioni antiriciclaggio – Processo Disposizione normative;
- esecuzione di operazioni "estero".

Vengono, inoltre, prese in considerazione tutte le attività bancarie che siano o possano essere caratterizzate dall'uso di denaro contante, quali:

- prelievo e versamento – Processo Disposizione normative;
- pagamento di utenze, bonifici o rate di mutuo – Processo Disposizione normative;
- cambio assegni – Processo Disposizione normative.

Con specifico riferimento al reato di autoriciclaggio, le attività sensibili sono quelle che possono determinare occultamento di proventi derivanti da crimini propri, quali ad esempio: l'evasione fiscale, la corruzione e l'appropriazione di beni sociali.

11.3. Regole di comportamento

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

In particolare, gli operatori, nell'ambito dell'assolvimento degli obblighi previsti dalla normativa antiriciclaggio (D.Lgs. 231/2007), 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, tramite l'acquisizione agli atti di fotocopia di un documento di identificazione in corso di validità e del codice fiscale, previa verifica dell'eventuale presenza del nominativo nelle versioni aggiornate delle liste antiterrorismo;
  - 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;
  - procedere alla profilatura della clientela in ottemperanza ai parametri oggettivi e soggettivi, dettati dalle disposizioni di legge e regolamentari, secondo quanto stabilito dalle disposizioni interne tempo per tempo vigenti;
  - mantenere aggiornati tutti i dati relativi ai rapporti continuativi al fine di consentire una costante valutazione del profilo economico e finanziario del cliente;
  - procedere all'adeguata verifica e all'aggiornamento della profilatura della clientela quando, indipendentemente da qualsiasi soglia di importo o di esenzione applicabile, vi sia il sospetto di riciclaggio o di finanziamento del terrorismo o sorgano dubbi sulla veridicità o sull'adeguatezza dei dati identificativi già acquisiti;
  - inoltrare al Responsabile Antiriciclaggio una segnalazione conformemente alla normativa interna quando sanno o sospettano che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo;
  - valutare se inoltrare la segnalazione predetta in presenza di indici di anomalia emanati e diffusi dalle Autorità di Vigilanza recepiti dalla normativa interna;
  - inoltrare le predette segnalazioni nei casi in cui risulti impossibile rispettare gli obblighi di adeguata verifica;
  - bloccare o, comunque, non dare esecuzione ad operazioni che vedano coinvolti soggetti/Paesi/merci oggetto di restrizioni di natura finanziaria (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) e/o commerciale (sanzioni commerciali generali o specifiche, divieti di importazione e di esportazione - ad esempio embargo sulle armi) o per

le quali sussista comunque il sospetto di una relazione con il riciclaggio o con il finanziamento del terrorismo;

- inoltrare, nel rispetto della normativa interna, 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 (Archivio Unico Informatico) e di conservazione della documentazione.

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 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;
- eseguire le operazioni per le quali si sospetta vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo;
- 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, titoli, 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.

Tutti coloro che sono coinvolti nei processi relativi ad attività che sono regolate da norme in materia di antiriciclaggio, sono perciò tenuti alla seguente condotta:

- osservanza di quanto previsto dal D.Lgs. n. 231/2007;
- osservanza delle normative interne e delle procedure;
- osservanza degli obblighi relativi alla frequentazione dei corsi di formazione obbligatori per i dipendenti della Banca.

Si precisa che l'utilizzo di sistemi informatici di ausilio alla gestione delle attività rivolte alla prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento al terrorismo non deresponsabilizza l'operatore dagli obblighi di conoscenza della clientela e di ogni connessa valutazione di rischio delle operazioni svolte.

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.

L'art. 52 del D.Lgs. n. 231/2007 - Organi di controllo - introduce a carico dell'Organismo di Vigilanza alcuni obblighi specifici relativi alla materia recata dal decreto. In particolare, l'art. 52 del D.Lgs. n. 231/2007 prevede:

a) l'attribuzione all'Organismo dell'obbligo di vigilare sull'osservanza delle norme contenute nel decreto (art. 52, comma 1);

b) l'assegnazione di specifici obblighi di comunicazione, a rilevanza sia meramente interna che esterna in capo all'Organismo (e agli altri organi di cui al comma 1).

Avendo riguardo agli obblighi specifici, il D.Lgs. n. 231/2007 (art. 52, comma 2, lett. a – d) prevede che l'Organismo debba:

1. comunicare, senza ritardo, all'Autorità di Vigilanza di settore, tutti gli atti e i fatti di cui venga a conoscenza nell'esercizio dei propri compiti, che possano costituire una violazione delle disposizioni emanate ai sensi dell'art. 7, comma 2, del D.Lgs. n. 231/2007;

2. comunicare, senza ritardo, al titolare dell'attività o al legale rappresentante o a un suo delegato, le infrazioni alle disposizioni di cui all'art. 41, di cui ha notizia;

3. comunicare, entro trenta giorni, al Ministero dell'Economia e delle Finanze infrazioni relative: (i) alle limitazioni all'uso del contante e dei titoli al portatore e (ii) al divieto di conti e libretti di risparmio anonimi o con intestazione fittizia di cui ha notizia;

4. comunicare, entro trenta giorni, all'UIF le infrazioni alle disposizioni contenute nell'art. 36 di cui ha notizia (le violazioni degli obblighi di registrazione).

Il mancato rispetto degli obblighi di comunicazione di cui all'art. 52, comma 2, è espressamente sanzionato dalla previsione contenuta nel comma 5 del successivo art. 55 D.Lgs. n. 231/2007, che recita: "*chi, essendovi tenuto, omette di effettuare la comunicazione di cui all'art. 52, comma 2, è punito con la reclusione fino ad un anno e con la multa da 100 a 1.000 euro*".

Tale disposizione è stata in parte modificata con un successivo intervento legislativo che ha chiarito che i compiti ed i doveri posti a carico dei soggetti menzionati dall'art. 52 non possono che essere svolti "*nell'ambito delle proprie attribuzioni e competenze*".

Come ha affermato l'ABI, con propria circolare serie Legale n. 14 – 8 giugno 2011, "*nonostante la specificazione che tale attività debba essere svolta nell'ambito delle proprie attribuzioni e competenze, l'art. 52 permane una disposizione fortemente critica perché sembra attribuire all'organismo di vigilanza un potere-dovere di prevenzione delle fattispecie illecite che è eccentrico rispetto ai compiti che l'art. 6 del D.Lgs. 231 intende attribuirgli*".

Sicché, prosegue la circolare, "*l'organismo di vigilanza, vigilerà sul rispetto nel contesto aziendale delle sole previsioni del decreto funzionali ad escludere il rischio di un coinvolgimento della banca in "fenomeni di riciclaggio", segnalando eventuali infrazioni di cui venga a conoscenza nello svolgimento dei propri compiti*".

Sul punto, la Banca d'Italia, nel Provvedimento 10 marzo 2011, capitolo I, Seziona IV, penultimo capoverso (entrato in vigore l'1°settembre 2011), precisa che le segnalazioni che l'Organismo di Vigilanza è tenuto ad effettuare nell'ambito delle proprie attribuzioni e competenze, "*possono essere effettuate congiuntamente con altri organi o funzioni aziendali*".

Normativa aziendale di riferimento: Al fine di prevenire i suddetti reati, oltre al Codice Etico rilevano le seguenti fonti interne: Politica di Gruppo Governo e gestione del rischio di riciclaggio e di finanziamento al terrorismo, Regolamento Funzione AML Capogruppo, Politica in materia di Adeguata verifica per le banche Affiliate, Disposizioni operative SOS Banche Affiliate.

Rileva altresì il Sistema dei Controlli Interni, che si è descritto nella Parte Generale.

12. REATI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

12.1. Le fattispecie di reato

Il D.lgs. n. 184 dell'8 novembre 2021 "Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio" ha introdotto l'art. 25-octies.1., rubricato *delitti in materia di strumenti di pagamento diversi dai contanti*.

La nuova disposizione prevede l'estensione della responsabilità amministrativa degli enti alla commissione dei delitti previsti dal codice penale in materia di strumenti di pagamento diversi dai contanti, ovvero:

- 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 (493- *quater* c.p.);
- frode informatica nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale (art. 640-ter c.p.).

12.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei reati in materia di strumenti di pagamento diversi dai contanti sono di seguito specificate:

- gestione dei sistemi di *home banking*;
- attività legate alla gestione delle carte di credito e carte prepagate.

12.3. Regole di comportamento

Le strutture della Banca, nonché le strutture esterne da essa incaricate, a qualsiasi titolo coinvolte nella gestione dei valori, sono tenute ad osservare le modalità esposte nel presente modello organizzativo, le disposizioni di legge esistenti in materia, la normativa interna, ivi incluso quanto previsto nel Codice Etico di Comportamento.

In particolare, tutti i soggetti che, nell'espletamento delle attività di propria competenza, a qualunque titolo si trovino a dover trattare strumenti di pagamento diversi dai contanti:

- devono essere appositamente incaricati;
- sono tenuti ad operare con onestà, integrità, correttezza e buona fede;
- devono attenersi alle norme operative di processo "gestione contante e valori";

- in particolare, in presenza di carte di credito di sospette di falsità, gli addetti sono tenuti ad effettuare le segnalazioni previste dalla normativa interna di riferimento;
- 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. 231 e di impegno al suo rispetto.

Normativa aziendale di riferimento: Normativa aziendale di riferimento: Al fine di prevenire i suddetti reati, oltre al Codice Etico rilevano le Norme operative di processo – *Internet banking*.

13. DELITTI DI CRIMINALITÀ ORGANIZZATA

13.1. Le fattispecie di reato

L'articolo 2, comma 29 della legge 15 luglio 2009, n. 94 recante disposizioni in materia di sicurezza pubblica prevede l'inserimento nel decreto legislativo n. 231 dell'articolo *24-ter* riguardante la responsabilità amministrativa degli enti per i delitti di criminalità organizzata.

Tale articolo amplia le fattispecie di reato suscettibili di determinare la responsabilità dell'ente alle seguenti fattispecie:

- delitti di associazione a delinquere (art. 416, sesto c.p.);
- associazioni di tipo mafioso, anche straniere (art. 416-bis c.p.);
- scambio elettorale politico-mafioso (art. 416 ter c.p.);
- sequestro di persona a scopo di estorsione (art. 630 c.p.);
- associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope (art. 74 DPR n. 309/90);
- delitti concernenti la fabbricazione ed il traffico di armi da guerra, esplosivi ed armi clandestine (art. 407, comma 2, lettera a) n. 5 c.p.p.).

13.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei delitti di criminalità organizzata sono legate alla concessione di affidamenti – Processo del credito.

13.3. Regole di comportamento

Alla luce della struttura e della natura delle condotte punite dalle fattispecie criminose in esame, si ritiene che tali disposizioni non abbiano un impatto significativo sulla Banca e che, comunque, i rischi residuali di commissione di tali reati trovino adeguata copertura nei presidi già attualmente in essere, in particolare in materia di rispetto della normativa antiriciclaggio e delle misure di contrasto al terrorismo.

Normativa aziendale di riferimento: Al fine di prevenire i suddetti reati, oltre al Codice Etico rilevano le seguenti fonti interne: Regolamento generale, Regolamento del credito, Poteri delegati credito.

14. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE

14.1. Le fattispecie di reato

L'art. 25-*novies* prevede i seguenti delitti in materia di violazione del diritto di autore:

- messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa art. 171, l. 633/1941 comma 1 lett a) bis);
- reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, l. 633/1941 comma 3);
- abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis l. 633/1941 comma 1);
- riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis l. 633/1941 comma 2);
- abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter l. 633/1941);
- mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies l. 633/1941);
- fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies l. 633/1941).

14.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei delitti in materia di violazione del diritto d'autore sono di seguito riepilogate:

- gestione dei programmi e dei sistemi informatici – Processo di gestione dei sistemi informativi
- attività di comunicazione e marketing – Processo Relazioni esterne
- gestione di siti intranet ed internet – Processo di gestione dei sistemi informativi.

14.3. Regole di comportamento

Per ciò che concerne le regole di comportamento in materia di violazione del diritto di autore si veda quanto stabilito al paragrafo 2.3 in materia di reati informatici.

15. REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI

15.1. Le fattispecie di reato

Con l'art. 4, comma 1, della legge 3 agosto 2009, n. 116 "Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale" il legislatore ha introdotto il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (articolo 25-decies).

15.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione del reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci sono state identificate nella partecipazione della Banca o di un dipendente della stessa ad un procedimento penale – Processo di Governo.

15.3. Regole di comportamento

Per la prevenzione del reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria la Banca ha previsto i seguenti obblighi e divieti di condotta.

La Banca vieta espressamente:

a) a chiunque di costringere o indurre, in qualsiasi forma e con qualsiasi modalità, nel malinteso interesse della Banca medesima, i destinatari a rispondere all'Autorità giudiziaria o ad avvalersi della facoltà di non rispondere;

b) nei rapporti con l'Autorità giudiziaria, ai destinatari del Modello di accettare denaro o altra utilità, anche attraverso consulenti eventualmente incaricati dalla Banca stessa;

c) nei rapporti con l'Autorità giudiziaria, ogni forma di condizionamento che induca il destinatario a rendere dichiarazioni non veritiere.

Tutti i destinatari devono tempestivamente avvertire l'Organismo di ogni violenza o minaccia, pressione, offerta o promessa di danaro o altra utilità, ricevuta al fine di alterare le dichiarazioni da non rendere all'Autorità giudiziaria.

Normativa aziendale di riferimento: Al fine di prevenire i suddetti reati, oltre al Codice Etico, rilevano le previsioni del Regolamento Generale.

16. REATI AMBIENTALI

16.1. Le fattispecie di reato

Il D.Lgs. n. 121 del 7 luglio 2011 "Attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni" ha introdotto l'art. 25 *undecies* (reati ambientali) nell'ambito del D. Lgs. 231.

L'art. 25 *undecies* individua le seguenti fattispecie di reato:

- Inquinamento ambientale (art. 452- bis c.p.);
- Morte o lesioni come conseguenza del delitto di inquinamento ambientale (art. 452- quater c.p.);
- Disastro ambientale (art. 452- quinquies c.p.);
- Delitti associativi aggravati ai sensi dell'articolo 452-octies c.p.;
- Delitto di traffico e abbandono di materiale ad alta radioattività (art. 452- sexies c.p.);
- Abbandono di animali (art. 727- bis c.p.)
- Distruzione o deterioramento di habitat all'interno di un sito privato (art. 733-bis c.p.);
- Scarico di acque reflue industriali contenenti le sostanze pericolose (art. 137, comma 5, d.lgs. 152/2006);
- Scarico nelle acque del mare da parte di navi od aeromobili contiene sostanze o materiali per i quali è imposto il divieto assoluto di sversamento (art. 137, comma 13, d.lgs. 152/2006);
- Violazione divieti di scarico si cui agli art. 103 e 104 d.lgs. 152/2006 (art. 137, comma 11, d. lgs. 152/2006);
- Attività di gestione di rifiuti non autorizzata (art. 256 d.lgs. 152/2006);
- Violazione dell'obbligo di bonifica di cui all'art. 257 d.lgs. 152/2006;

- Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari di cui all'art. 258, d.lgs. 152/2006;
- Traffico illecito di rifiuti (art. 259, d.lgs. 152/2006);
- Attività organizzate per il traffico illecito di rifiuti (art. 452 - *quaterdecies* c.p.) anche se il richiamo all'interno della l. 231 è ancora all'articolo 260 d.lgs. 152/2006);
- Violazione, nell'esercizio di uno stabilimento, dei valori limite di emissione stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla parte quinta del d.lgs. 152/2006, dai piani e dai programmi o dalla normativa di cui all'articolo 271, d.lgs. 152/2006 (art. 279, d.lgs. 152/2006);
- Importazione, esportazione senza autorizzazione di specie animali e vegetali in via di estinzione di cui alla L. 07/02/1992, n. 150;
- Violazione degli obblighi relativi alla cessazione e riduzione dell'impiego delle sostanze lesive di cui all'art. 3, L. 28/12/1993, n. 549;
- Inquinamento doloso e colposo di cui al D.Lgs. 06/11/2007, n. 202.

16.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei reati ambientali sono di seguito specificate:

- raccolta, trasporto, smaltimento rifiuti in mancanza di autorizzazione – Processo di gestione delle infrastrutture e delle spese;
- gestione degli obblighi di comunicazione, tenuta dei registri obbligatori e dei formulari, gestione delle comunicazione al Sistema Informatico di controllo della tracciabilità dei rifiuti (SISTRI) – Processo di gestione delle infrastrutture e delle spese;
- la concessione di credito ad aziende che si occupano di raccolta, trasporto, smaltimento rifiuti in mancanza di autorizzazione – Processo del Credito;
- gestione immobili di proprietà della Banca - Processo di gestione delle infrastrutture e delle spese.

16.3. Regole di comportamento

La materia dei reati ambientali interessa la Banca limitatamente allo smaltimento dei rifiuti (carta, toner, apparecchiature elettroniche dismesse, materiali d'uso corrente per la pulizia dei locali, ecc.), tipici dell'ordinaria attività aziendale.

Sul punto, è fatto obbligo al responsabile dell'ufficio Economato di vigilare sull'adeguatezza delle procedure interne adottate nel rispetto della normativa vigente, e di comunicare all'Organismo ogni eventuale comportamento difforme rispetto ad esse.

Nell'ambito delle attività di concessione del credito ad aziende che si occupano di raccolta, trasporto e smaltimento rifiuti, è fatto obbligo agli operatori di acquisire ogni informazione

necessaria a verificare il possesso delle necessarie autorizzazioni, in capo al richiedente, allo svolgimento delle predette attività.

Per ciò che concerne le attività di gestione degli immobili di proprietà della Banca è fatto obbligo al momento dell'acquisizione del bene di acquisire informazioni dettagliate rispetto ai materiali utilizzati per la costruzione, ai terreni su cui questi sono edificati, verificando il possesso delle eventuali autorizzazioni.

Normativa aziendale di riferimento: Al fine di prevenire i suddetti reati, oltre al Codice Etico, la Banca ha conferito specifico incarico di consulenza al fine di uniformare le procedure in essere nei due istituti di credito anteriormente alla fusione ed ha altresì conferito incarico di redigere specifiche linee guida e/o procedure operative in materia ambientale destinate agli operatori: di tali documenti risulta imminente l'adozione.

17. REATO DI IMPIEGO DI LAVORATORI CON SOGGIORNO IRREGOLARE

17.1. Le fattispecie di reato

Il D.Lgs. n. 109 del 16 luglio 2012 "Attuazione della direttiva 2009/52/CE che introduce norme minime relative a sanzioni e provvedimenti nei confronti di datori di lavoro che impiegano cittadini di Paesi terzi il cui soggiorno è irregolare" ha introdotto l'art. 25 duodecies nell'ambito del D.Lgs. 231.

La nuova disposizione prevede l'estensione della responsabilità amministrativa degli enti alla commissione del delitto di cui all'art. 22 comma 12-bis D.Lgs. 286/1998 (TU sull'immigrazione) relativo all'impiego di cittadini provenienti da paesi terzi privi del regolare permesso di soggiorno ovvero il cui permesso di soggiorno sia scaduto e del quale non sia stato chiesto, nei termini di legge, il rinnovo, ovvero il cui permesso di soggiorno sia stato revocato o annullato.

17.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione del reato di impiego di lavoratori con soggiorno irregolare sono di seguito specificate:

- Impiego, alle dirette dipendenze della Banca, di lavoratori provenienti da paesi terzi privi di regolare permesso di soggiorno – Processo gestione risorse umane;
- impiego, tramite soggetti terzi (agenzie di somministrazione, appaltatori), di lavoratori provenienti da paesi terzi privi di regolare permesso di soggiorno – Processo di gestione delle infrastrutture e spese.

17.3. Regole di comportamento

Le strutture della Banca, a qualsiasi titolo coinvolte nella gestione di lavoratori assunti alle dirette dipendenze, sono tenute ad osservare le disposizioni di legge esistenti in materia, la normativa

interna, ivi incluso quanto nel Codice Etico di Comportamento vi sia di pertinente con la materia in discorso.

Le strutture della Banca, a qualsiasi titolo coinvolte nella stipula di nuovi contratti ove essa risulti nella qualità di committente di forniture, servizi, opere, lavori e manutenzioni, sono tenute ad accertare ed a far constare che le controparti contrattuali, anche non dirette come nel caso di subappalti, rendano atto di aver adottato misure organizzative adeguate al rispetto della normativa in materia di impiego di lavoro di cittadini di paesi terzi il cui soggiorno è irregolare e, più in generale, delle disposizioni previste dal Testo Unico concernente la disciplina dell'immigrazione e la condizione dello straniero.

In relazione ai contratti di durata già in corso, in particolare per i cd. "servizi in outsourcing", le strutture della Banca preposte alla loro gestione sono tenute ad integrarli, ove lacunosi in materia, acquisendo le dichiarazioni delle controparti, anche non dirette come nel caso di subappalti, di aver adottato misure organizzative adeguate al rispetto della normativa in materia di impiego di lavoro di cittadini di paesi terzi il cui soggiorno è irregolare e, più in generale, delle disposizioni previste dal Testo Unico concernente la disciplina dell'immigrazione e la condizione dello straniero.

Le strutture della Banca che se ne occupano sono tenute ad acquisire il DURC di tutte le società cui vengono conferiti appalti.

Normativa aziendale di riferimento: Al fine di prevenire i suddetti reati, oltre al Codice Etico, rilevano le previsioni del Regolamento Generale. Rileva altresì il Sistema dei Controlli Interni, che si è descritto nella Parte Generale.

18. REATO DI RAZZISMO E XENOFOBIA

18.1. Le fattispecie di reato

La l. n. 167 del 20 novembre 2017, "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017" ha introdotto l'art. 25 terdecies nell'ambito del D.Lgs. 231.

La nuova norma estende la responsabilità amministrativa degli enti alla commissione del delitto di propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa, di cui oggi all'art. 604 – bis del c.p. (già all'art. 3, comma 3-bis, l. n. 654/1975, abrogato dall' art. 7, comma 1, lett. *c*), D.Lgs. 1° marzo 2018, n. 21).

18.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione del reato di propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa, sono astrattamente le attività di comunicazione e marketing e gestione di siti internet.

18.3. Regole di comportamento

Per la prevenzione di tali reati, occorre in ogni caso che tutti i dipendenti:

- operino nelle proprie attività di competenza con onestà, integrità, correttezza e buona fede;
- rispettivo i criteri di imparzialità, merito, competenza e professionalità nelle decisioni legate alla gestione del personale (progressione di carriera, incarichi etc.);
- stigmatizzino qualsiasi pratica discriminatoria;
- segnalino all'Organismo qualsiasi pratica discriminatoria posta in essere all'interno della Banca;

Normativa aziendale di riferimento: Codice Etico di Comportamento.

Per la prevenzione dei reati in materia di razzismo e xenofobia, tutti gli organi della Banca ed i dipendenti sono tenuti ad osservare le modalità esposte nel presente modello organizzativo, le disposizioni di legge esistenti in materia, la normativa interna, ivi incluso quanto previsto nel Codice Etico di Comportamento.

19. REATO DI FRODE IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O DI SCOMMESSA E GIOCHI D'AZZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI

19.1. Le fattispecie di reato

La legge n. 39 del 3 maggio 2019, "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla manipolazione di competizioni sportive, fatta a Magglingen il 18 settembre 2014" ha introdotto nel corpo del D.lgs. 231 l'art. Art. 25-quaterdecies.

La norma prevede l'estensione della responsabilità amministrativa degli enti all'ipotesi di commissione dei reati di frode in competizioni sportive ed esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (di cui agli articoli 1 e 4 l. 401/1989).

19.2. Le attività sensibili

Con riguardo ai delitti di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati, non si ravvisano attività sensibili alla realizzazione di questa categoria di reati.

19.3. Regole di comportamento

I delitti di frode in competizione sportive, esercizio abusivo di gioco o di scommessa e giochi di azzardo non risultano rientrare nella casistica delle attività bancarie.

20. REATI TRIBUTARI

20.1. Le fattispecie di reato

Il D.L. n. 124 del 26 ottobre 2019 – convertito, con modificazioni, dalla l. n. 157 del 19 dicembre 2019 – "Disposizioni urgenti in materia fiscale e per esigenze indifferibili" ha introdotto l'art. 25-quinquiesdecies nel D.lgs. n. 231.

La nuova disposizione estende la responsabilità amministrativa degli enti alla commissione dei reati tributari previsti dal d.lgs. n. 74/2004, ed in particolare:

- delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1, d.lgs. n. 74/2004);
- delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 2-bis, d.lgs. n. 74/2004);
- delitto di dichiarazione fraudolenta mediante altri artifici (art. 3, d.lgs. n. 74/2004);
- delitto di emissione di fatture o altri documenti per operazioni inesistenti (art. 8, comma 1, d.lgs. n. 74/2004);
- delitto di emissione di fatture o altri documenti per operazioni inesistenti (art. 8, comma 2- bis, d.lgs. n. 74/2004);
- delitto di occultamento o distruzione di documenti contabili (art. 10, d.lgs. n. 74/2004);
- delitto di sottrazione fraudolenta al pagamento di imposte (art. 11, d.lgs. n. 74/2004);
- delitto di dichiarazione infedele (art. 4, d.lgs. n. 74/2004);
- delitto di omessa dichiarazione (art. 5, d.lgs. n. 74/2004);
- delitto di indebita compensazione (art. 10- quater, d.lgs. n. 74/2004).

20.2. Le attività sensibili

Le attività identificate come potenzialmente sensibili per la realizzazione dei reati tributari sono:

- Processo Finanza
- contabilità generale;
- tenuta delle scritture contabili;
- redazione del bilancio;
- gestione delle operazioni contabili;
- gestione dei pagamenti delle imposte dirette ed indirette;
- gestione delle attività di versamento tasse per cui l'istituto bancario è sostituto d'imposta.

20.3. Regole di comportamento

Tutti gli organi della Banca ed i dipendenti sono tenuti ad osservare le modalità esposte nel presente modello organizzativo, le disposizioni di legge esistenti in materia, la normativa interna, ivi incluso quanto previsto nel Codice Etico di Comportamento.

In particolare, al pari dei reati societari, anche per i reati tributari, tutti coloro che per posizione e ruolo ricoperto assumono collegialmente decisioni e deliberazioni relative alla gestione della Banca e al relativo governo e tutti i dipendenti che collaborino in tali attività, tra cui anche l'elaborazione di dati e documenti contabili, nonché la gestione di pagamenti di imposte dirette o indirette sono tenuti a:

- osservare le norme di legge, dello Statuto Sociale, dei Regolamenti e delle normative interne relative al funzionamento degli organi sociali;
- operare nel rispetto dei principi di verità, accuratezza, completezza, chiarezza e trasparenza del dato registrato;
- rappresentare in modo corretto, completo e tempestivo i dati di gestione nella contabilità e nei documenti aziendali;
- fare in modo che qualsiasi transazione commerciale sia tracciabile e adeguatamente documentata, nel rispetto delle normative e delle procedure;
- garantire che qualsiasi operazione sia agevolmente ricostruibile nel più breve tempo possibile;
- segnalare tempestivamente agli organi di controllo gli eventuali errori, omissioni o falsificazioni;
- segnalare all'Organismo le infrazioni del Codice Etico di Comportamento della Banca

Normativa aziendale di riferimento: Al fine di prevenire i suddetti reati, oltre al Codice Etico, rilevano le seguenti fonti interne: Regolamento Gruppo IVA, Politica di gestione del Rischio di non conformità fiscale, Regolamento Interno, Politica di Gruppo in materia di Concessione e perfezionamento del Credito, Poteri e deleghe. Rileva altresì il Sistema dei Controlli Interni, che si è descritto nella Parte Generale.

21. REATO DI CONTRABBANDO

21.1. Le fattispecie di reato

Il D.lgs. 14 luglio 2020, n. 75 "Attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" ha introdotto l'art. 25-sexiesdecies nell'ambito del D.Lgs. 231.

La nuova disposizione prevede l'estensione della responsabilità amministrativa degli enti alla commissione dei reati previsti dal D.P.R. 23 gennaio 1973, n. 43, ovvero il Testo Unico in materia doganale.

21.2. Le attività sensibili

Con riguardo al delitto di contrabbando, non si ravvisano attività sensibili alla realizzazione di questa categoria di reati.

21.3. Regole di comportamento

I delitti di contrabbando non risultano rientrare nella casistica delle attività bancarie.

22. REATI CONTRO IL PATRIMONIO CULTURALE

22.1. Le fattispecie di reato

La Legge 9 marzo 2022, n. 22 (pubblicata in Gazzetta Ufficiale del 22 marzo 2022) "Disposizioni in materia di reati contro il patrimonio culturale" ha introdotto nell'ambito del D.Lgs. 231 l'art. 25-septiesdecies e l'art. 25-octiesdecies.

Le nuove disposizioni prevedono l'estensione della responsabilità amministrativa degli enti alla commissione dei seguenti reati, contestualmente introdotti nel corpo del codice penale dalla L. n. 22/2022:

- violazioni in materia di alienazione di beni culturali (art. 518-nonies c.p.);
- appropriazione indebita di beni culturali (art. 518-ter c.p.);
- importazione illecita di beni culturali (c.p. art. 518-decies.);
- uscita o esportazione illecite di beni culturali (art. 518-undecies c. p.);
- distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies c.p.);
- contraffazione di opere d'arte (art. 518-quaterdecies);
- furto di beni culturali (art. 518-bis c.p.);
- ricettazione di beni culturali (art. 518-quater c.p.);
- falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.);
- riciclaggio di beni culturali (art. 518-sexies c.p.);
- devastazione e saccheggio di beni culturali e paesaggistici (art. 518-terdecies c.p.).

22.2. Le attività sensibili

Con riguardo ai delitti contro il patrimonio culturale, non si ravvisano attività sensibili alla realizzazione di questa categoria di reati.

22.3. Regole di comportamento

I delitti contro il patrimonio non risultano rientrare nella casistica delle attività bancarie.