

# **BANCA POPOLARE DEL CASSINATE**

**A CURA DELLA FUNZIONE ANTIRICICLAGGIO E DELLA FUNZIONE DI  
COMPLIANCE**

## **POLICY PER IL GOVERNO DEI RISCHI DI RICICLAGGIO E DI FINANZIAMENTO DEL TERRORISMO**

Approvazione - Consiglio di Amministrazione dell'8 settembre 2020

## ELENCO VERSIONI

NUMERO VERSIONE	DATA DI APPROVAZIONE C.d.A.	NOTE
1	11/02/2020	<p>1. Aggiornamento alle nuove disposizioni in materia di organizzazione procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo del 26 marzo 2019 emanate dalla Banca d'Italia;</p> <p>2. alle nuove disposizioni attuative in materia di adeguata verifica della clientela del 30 luglio 2019 emanate dalla Banca d'Italia, il cui adeguamento procedurale è stato in parte rilasciato ad inizio anno e proseguirà nel corso del corrente mese;</p> <p>3. alle nuove disposizioni di cui alla Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018, che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE (cosiddetta V direttiva);</p> <p>4. all'adeguamento dei termini massimi di aggiornamento dell'adeguata verifica</p> <p>5. alla formulazione del processo di adeguata verifica.</p>
2	08/09/2020	<p>1. Aggiornamento: paragrafo 4.1.4.2 relativo alle misure rafforzate da applicare agli intermediari bancari, finanziari o assicurativi.</p>

INDICE

1. PREMESSA.....	1
1.1. Definizioni.....	1
1.2. Contesto normativo di riferimento.....	9
1.3. Obiettivi del documento.....	10
1.4. Adozione e aggiornamento del documento .....	11
1.5. Destinatari.....	11
2. PRINCIPI GENERALI E LIMITI OPERATIVI .....	11
3. RUOLI E RESPONSABILITÀ.....	14
3.1. Ruoli e responsabilità degli Organi aziendali.....	14
3.1.1. Organo con funzione di supervisione strategica.....	14
3.1.2. Organo con funzione di gestione .....	15
3.1.3. Organo con funzione di controllo.....	16
3.2. Ruoli e responsabilità delle Funzioni aziendali.....	17
3.2.1. Funzione Antiriciclaggio.....	17
3.2.1.1. Responsabile Antiriciclaggio .....	17
3.2.1.2. Responsabile delle segnalazioni di operazioni sospette .....	18
3.2.2. Funzione Internal Audit.....	19
3.2.3. Funzione Commerciale.....	20
3.2.4. Funzioni aziendali di controllo .....	20
3.2.5. Altre Funzioni aziendali.....	20
3.2.6. Personale .....	20
4. GESTIONE DEI RISCHI DI RICICLAGGIO E DI FINANZIAMENTO DEL TERRORISMO .....	21
4.1. Principi generali in materia di adeguata verifica .....	22
4.1.1. Approccio basato sul rischio e profilatura della clientela .....	22
4.1.2. Adeguata Verifica della Clientela .....	23
4.1.3. Misure semplificate di adeguata verifica.....	25
4.1.4. Misure rafforzate di adeguata verifica.....	27
4.1.4.1 Persone Politicamente Esposte .....	29
4.1.4.2 Rapporti di corrispondenza transfrontalieri con intermediari bancari o finanziari rispondenti di un Paese terzo con regime non equivalente o Paese terzo ad alto rischio.....	30

## *Policy per il governo dei rischi di riciclaggio e di finanziamento del terrorismo*

4.1.4.3 Rapporti ed operazioni che coinvolgono Paesi Terzi ad alto rischio.....	31
4.1.4.4 Operazioni caratterizzate da importi insolitamente elevati o per le quali sussistono dubbi sulla finalità .....	32
4.1.5. Esecuzione da parte di terzi degli obblighi di adeguata verifica .....	32
4.1.6. Obbligo di astensione .....	33
4.1.7. Misure di contrasto al finanziamento del terrorismo.....	34
4.2. Principi generali in materia di conservazione dei dati e delle informazioni .....	35
4.3. Principi generali in materia di controlli interni.....	36
4.4. Principi generali in materia di segnalazione delle operazioni sospette .....	36
4.5. Comunicazioni oggettive.....	38
4.6. Gestione degli embarghi .....	38
4.7. Presidi in materia di trasferimento di fondi .....	39
4.8. Limitazioni all'uso del contante e dei titoli al portatore .....	40
4.9. Metodologia di valutazione del rischio .....	40
4.10. Formazione del personale e consulenza .....	40
4.11. Sistema interno di segnalazione delle violazioni.....	41
<b>5.ALLEGATI.....</b>	<b>41</b>

## 1. PREMESSA

La presente Policy, finalizzata al governo dei rischi di riciclaggio e di finanziamento del terrorismo (di seguito anche "Policy") è adottata dalla Banca Popolare del Cassinate

### 1.1. Definizioni

- **"Accordo di Garanzia"** o **"Accordo"**: indica il contratto redatto ai sensi dell'art. 37-bis, comma 4, TUB.;
- **"Accordo di Servizio"**: indica l'accordo disciplinante specifiche attività che impegna formalmente la Funzione aziendale erogatrice del servizio nei confronti della Funzione aziendale fruitrice;
- **"Agenti in attività finanziaria"**: gli agenti iscritti nell'elenco previsto dall'art. 128-quater, commi 2 e 6 del TUB;
- **"Archivio Unico Informatico (AUI)"**: l'archivio standardizzato, già istituito alla data di entrata in vigore del D. Lgs. n. 90/2017, mediante il quale sono resi disponibili i dati e le informazioni previsti dalle disposizioni di Banca d'Italia in materia di conservazione ed utilizzo dei dati e delle informazioni a fini antiriciclaggio e di contrasto al finanziamento del terrorismo;
- **"Attività istituzionale"**: l'attività per la quale i destinatari hanno ottenuto l'iscrizione ovvero l'autorizzazione da parte di un'Autorità Pubblica;
- **"Autorità competente"**: indica le Autorità che, a seconda dei casi e in coerenza con quanto previsto dalla normativa nazionale ed europea di settore, esercitano attività di vigilanza, quali, a titolo esemplificativo Banca Centrale Europea, Banca d'Italia, Consob, Ivass, Ministeri e Organi governativi;
- **"Autorità di vigilanza"**: la Banca d'Italia, la CONSOB e l'IVASS in quanto autorità preposte alla vigilanza e al controllo degli intermediari bancari e finanziari, dei revisori legali e delle società di revisione legale con incarichi di revisione legale su enti di interesse pubblico e su enti sottoposti a regime intermedio e la Banca d'Italia nei confronti degli operatori non finanziari che esercitano le attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, in presenza della licenza di cui all'articolo 134 TULPS, limitatamente all'attività di trattamento delle banconote in euro, in presenza dell'iscrizione nell'elenco di cui all'articolo 8 del decreto-legge 25 settembre 2001 n. 350, convertito, con modificazioni, dalla legge 23 novembre 2001, n. 409;
- **"Azione correttiva"**: indica un'azione la cui implementazione riduce il rischio rilevato nel corso delle verifiche eseguite dalle Funzioni aziendali di controllo;
- **"Banca"**: Banca Popolare del Cassinate
- **"Banca di comodo (shell bank)"**: la banca o l'ente che svolge funzioni analoghe ad una banca che non ha una struttura organica e gestionale significativa nel paese in cui è stato costituito e autorizzato all'esercizio dell'attività né è parte di un

gruppo finanziario soggetto a un'efficace vigilanza su base consolidata;

- **“Circolare 285”**: indica la Circolare di Banca d'Italia n. 285 del 17 dicembre 2013, recante le Disposizioni di Vigilanza per le Banche e successive modifiche ed integrazioni;
- **“Cliente”**: il soggetto che instaura rapporti continuativi, compie operazioni ovvero richiede od ottiene una prestazione professionale a seguito del conferimento di un incarico;
- **“Comitato per il Monitoraggio dei Rischi”**: il monitoraggio dei rischi indica il comitato endo-consiliare della Banca specializzato in tema di “rischi”, istituito ai sensi delle Disposizioni di vigilanza per le banche;
- **“Congelamento dei fondi”**: il divieto, in virtù dei regolamenti comunitari e della normativa nazionale, di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione di portafoglio;
- **“Congelamento delle risorse economiche”**: il divieto, in virtù dei regolamenti comunitari e della normativa nazionale, di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, utilizzo delle risorse economiche;
- **“Conti correnti di corrispondenza e rapporti ad essi assimilabili”**: i conti tenuti dalle banche per il regolamento dei servizi interbancari e gli altri rapporti comunque denominati, intrattenuti tra enti creditizi e istituti finanziari, utilizzati per il regolamento di transazioni per conto dei clienti degli enti corrispondenti;
- **“Conti di passaggio”**: i rapporti bancari di corrispondenza transfrontalieri, intrattenuti tra intermediari bancari e finanziari, utilizzati per effettuare operazioni in nome proprio e per conto della clientela;
- **“Dati identificativi”**: il nome e il cognome, il luogo e la data di nascita, la residenza anagrafica e il domicilio, ove diverso dalla residenza anagrafica, gli estremi del documento di identificazione e, ove assegnato, il codice fiscale o, nel caso di soggetti diversi da persona fisica, la denominazione, la sede legale e, ove assegnato, il codice fiscale;
- **“Decreto”**: il Decreto Legislativo 21 novembre 2007, n. 231 e successive modifiche e integrazioni;
- **“Denaro contante o contante”**: le banconote e le monete metalliche, in euro o in valute esteri, aventi corso legale;
- **“Embargo”**: misure di interruzione o riduzione, parziale o completa, delle relazioni economiche e finanziarie con uno o più paesi terzi;
- **“Esecutore”**: il soggetto delegato ad operare in nome e per conto del cliente o a cui siano comunque conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del Cliente;

- **“Esternalizzazione”**: indica l’accordo, in qualsiasi forma, tra una banca e le società e un fornitore di servizi in base al quale il fornitore realizza un processo, un servizio o un’attività della stessa banca;
- **“Finanziamento del terrorismo”**: qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all’intermediazione, al deposito, alla custodia o all’erogazione, in qualunque modo realizzate, di fondi e risorse economiche, destinati ad essere, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali ciò indipendentemente dall’effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte sopra riportate;
- **“Follow up”**: attività di controllo finalizzata a verificare che le azioni correttive previste in conseguenza della segnalazione di un rilievo siano effettivamente realizzate;
- **“Fondi”**: le attività ed utilità finanziarie di qualsiasi natura, inclusi i proventi da questi derivati, possedute, detenute o controllate, anche parzialmente, direttamente o indirettamente, o per interposta persona fisica o giuridica da parte di soggetti designati, ovvero da parte di persone fisiche o giuridiche che agiscano per conto o sotto la direzione di questi ultimi, compresi a titolo meramente esemplificativo:
  - a) i contanti, gli assegni, i crediti pecuniari, le cambiali, gli ordini di pagamento e altri strumenti di pagamento;
  - b) i depositi presso enti finanziari o altri soggetti, i saldi sui conti, i crediti e le obbligazioni di qualsiasi natura;
  - c) i titoli negoziabili a livello pubblico e privato nonché gli strumenti finanziari come definiti nell’articolo 1, comma 2, TUF;
  - d) gli interessi, i dividendi o altri redditi ed incrementi di valore generati dalle attività;
  - e) il credito, il diritto di compensazione, le garanzie di qualsiasi tipo, le cauzioni e gli altri impegni finanziari;
  - f) le lettere di credito, le polizze di carico e gli altri titoli rappresentativi di merci;
  - g) i documenti da cui risulti una partecipazione in fondi o risorse finanziarie;
  - h) tutti gli altri strumenti di finanziamento delle esportazioni;
  - i) le polizze assicurative concernenti i rami vita, di cui all’articolo 2, comma 1, CAP.;
- **“Funzione aziendale”**: indica l’insieme dei compiti e delle responsabilità assegnate per l’espletamento di una determinata fase dell’attività aziendale. Sulla base della rilevanza della fase svolta, la Funzione è incardinata presso una specifica unità organizzativa;
- **“Funzioni aziendali di controllo”**: indica la Funzione di conformità alle norme (Compliance), la Funzione di controllo dei rischi (Risk Management), la Funzione Antiriciclaggio e la Funzione di revisione (Internal Audit – attualmente esternalizzata

alla società Meta srl)) ;

- **“Funzioni di controllo”**: indica l’insieme delle funzioni che per disposizione legislativa, regolamentare, statutaria o di autoregolamentazione hanno compiti di controllo;
- **“Istituti di pagamento”**: le imprese, diverse dalle banche e dagli istituti di moneta elettronica, autorizzate a prestare i servizi di pagamento;
- **“Livelli di servizio” e o “Services Level Agreement - SLA”**: accordi tramite cui si definiscono le metriche di erogazione del servizio che devono essere rispettate dal fornitore;
- **“Mezzi di pagamento”**: il denaro contante, gli assegni bancari e postali, gli assegni circolari e gli altri assegni a essi assimilabili o equiparabili, i vaglia postali, gli ordini di accreditamento o di pagamento, le carte di credito e le altre carte di pagamento, le polizze assicurative trasferibili, le polizze di pegno e ogni altro strumento a disposizione che permetta di trasferire, movimentare o acquisire, anche per via telematica, fondi, valori, o disponibilità finanziarie;
- **Operazione**: attività consistente nella movimentazione, nel trasferimento o nella trasmissione di mezzi di pagamento o nel compimento di atti negoziali a contenuto patrimoniale; costituisce operazione anche la stipulazione di un atto negoziale, a contenuto patrimoniale, rientrante nell’esercizio dell’attività professionale o commerciale;
- **“Operazione frazionata”**: un’operazione unitaria sotto il profilo del valore economico, di importo pari o superiore ai limiti stabiliti dal decreto, posta in essere attraverso più operazioni, singolarmente inferiori ai predetti limiti, effettuate in momenti diversi ed in un circoscritto periodo di tempo fissato in sette giorni, ferma restando a sussistenza dell’operazione frazionata quando ricorrano elementi per ritenerla tale;
- **“Operazione occasionale”**: operazione non riconducibile a un rapporto continuativo in essere; costituisce operazione occasionale anche la prestazione intellettuale o commerciale, ivi comprese quelle ad esecuzione istantanea, resa in favore del cliente;
- **“Organi aziendali”**: indica il Consiglio di Amministrazione, il Collegio Sindacale;
- **“Organo con funzione di controllo”**: indica l’Organo aziendale cui, ai sensi del codice civile o per disposizione statutaria, spetta di vigilare sull’osservanza delle norme di legge, regolamentari e statutarie, sulla corretta amministrazione, sull’adeguatezza degli assetti organizzativi e contabili della Banca;
- **“Organo con funzione di gestione”**: indica l’Organo aziendale o i componenti di esso a cui, ai sensi del codice civile o per disposizione statutaria, spettano o sono delegati compiti di gestione, intesa come attuazione degli indirizzi deliberati nell’esercizio della funzione di supervisione strategica;
- **“Organo con funzione di supervisione strategica”**: indica l’Organo aziendale a cui,

ai sensi del codice civile o per disposizione statutaria, sono attribuite funzioni di indirizzo della gestione di impresa, mediante, tra l'altro, esame e delibera in ordine ai piani industriali o finanziari ovvero alle operazioni strategiche;

- **“Orientamenti congiunti”**: Orientamenti congiunti delle Autorità di Vigilanza europee, adottati il 26 giugno 2017, ai sensi degli articoli 17 e 18, paragrafo 4, della direttiva antiriciclaggio, in materia di fattori di rischio che gli intermediari dovrebbero prendere in considerazione nel valutare i rischi di riciclaggio e finanziamento del terrorismo associati alla clientela e in materia di misure di adeguata verifica da adottare;
- **“Paesi comunitari”**: paesi appartenenti allo Spazio economico europeo;
- **“Paesi terzi”**: Paesi non appartenenti allo Spazio Economico Europeo diversi da Paesi terzi ad alto rischio;
- **“Paesi terzi ad alto rischio”**: Paesi non appartenenti all'Unione Europea i cui ordinamenti presentano carenze strategiche nei rispettivi regimi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo, per come individuati dalla Commissione Europea nell'esercizio dei poteri di cui agli articoli 9 e 64 della direttiva nonché i Paesi classificati dal GAFI come “High-risk and other monitored jurisdictions”;
- **“Persone Politicamente Esposte (PEPs)”**: le persone fisiche che occupano o hanno cessato di occupare da meno di un anno importanti cariche pubbliche, nonché i loro familiari e coloro che con i predetti soggetti intrattengono notoriamente stretti legami, come di seguito elencate:
  - 1) sono persone fisiche che occupano o hanno occupato importanti cariche pubbliche coloro che ricoprono o hanno ricoperto la carica di:
    - 1.1 Presidente della Repubblica, Presidente del Consiglio, Ministro, Vice-Ministro e Sottosegretario, Presidente di Regione, assessore regionale, Sindaco di capoluogo di provincia o città metropolitana, Sindaco di comune con popolazione non inferiore a 15.000 abitanti nonché cariche analoghe in Stati esteri;
    - 1.2 deputato, senatore, parlamentare europeo, consigliere regionale nonché cariche analoghe in Stati esteri;
    - 1.3 membro degli organi direttivi centrali di partiti politici;
    - 1.4 giudice della Corte Costituzionale, magistrato della Corte di Cassazione o della Corte dei conti, consigliere di Stato e altri componenti del Consiglio di Giustizia Amministrativa per la Regione siciliana nonché cariche analoghe in Stati esteri;
    - 1.5 membro degli organi direttivi delle banche centrali e delle autorità indipendenti;
    - 1.6 ambasciatore, incaricato d'affari ovvero cariche equivalenti in Stati esteri, ufficiale di grado apicale delle forze armate ovvero cariche analoghe in Stati esteri;

1.7 componente degli organi di amministrazione, direzione o controllo delle imprese controllate, anche indirettamente, dallo Stato italiano o da uno Stato estero ovvero partecipate, in misura prevalente o totalitaria, dalle Regioni, da comuni capoluoghi di provincia e città metropolitane e da comuni con popolazione complessivamente non inferiore a 15.000 abitanti;

1.8 direttore generale di ASL e di azienda ospedaliera, di azienda ospedaliera universitaria e degli altri enti del servizio sanitario nazionale;

1.9 direttore, vicedirettore e membro dell'organo di gestione o soggetto svolgenti funzioni equivalenti in organizzazioni internazionali;

2) sono familiari di persone politicamente esposte: i genitori, il coniuge o la persona legata in unione civile o convivenza di fatto o istituti assimilabili alla persona politicamente esposta, i figli e i loro coniugi nonché le persone legate ai figli in unione civile o convivenza di fatto o istituti assimilabili;

3) sono soggetti con i quali le persone politicamente esposte intrattengono notoriamente stretti legami:

3.1 le persone fisiche che detengono, congiuntamente alla persona politicamente esposta, la titolarità effettiva di enti giuridici, trust e istituti giuridici affini ovvero che intrattengono con la persona politicamente esposta stretti rapporti d'affari;

3.2 le persone fisiche che detengono solo formalmente il controllo totalitario di un'entità notoriamente costituita, di fatto, nell'interesse e a beneficio di una persona politicamente esposta;

- **“Personale”**: i dipendenti e coloro che operano sulla base di rapporti che ne determinano l’inserimento nell’organizzazione del soggetto obbligato, anche in forma diversa dal rapporto di lavoro subordinato;
- **“Piano delle attività” o “Piano della Funzione Antiriciclaggio”**: indica il piano annuale delle attività per l’anno successivo, predisposto dal Responsabile della Funzione Antiriciclaggio all’interno della Relazione annuale della Funzione Antiriciclaggio presentata agli organi di supervisione strategica, gestione e controllo. Il Piano è basato sulle analisi dei rischi allo scopo di determinarne le priorità in linea con la metodologia e gli obiettivi della Funzione;
- **“Presidi”**: elementi strutturali e organizzativi atti a prevenire e/o eliminare/ridurre gli effetti degli eventi di rischio mitigando l’ipotesi di non conformità;
- **“Processo di gestione dei rischi”**: indica l’insieme delle regole, delle procedure, delle risorse (umane, tecnologiche e organizzative) e delle attività di controllo volte a identificare, misurare o valutare, monitorare, prevenire o mitigare nonché comunicare ai livelli gerarchici appropriati tutti i rischi assunti o assumibili nei diversi segmenti, cogliendone, in una logica integrata, anche le interrelazioni reciproche e con l’evoluzione del contesto esterno;
- **“Pubbliche Amministrazioni”**: le amministrazioni pubbliche di cui all’art. 1, comma 2,

del D. Lgs. 165/2001, e successive modificazioni, gli enti pubblici nazionali, le società partecipate dalle amministrazioni pubbliche e dalle loro controllate, ai sensi dell'art. 2359 del codice civile, limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o dall'Unione europea nonché i soggetti preposti alla riscossione dei tributi nell'ambito della fiscalità nazionale o locale, quale che ne sia la forma giuridica;

- **“Rapporto continuativo”**: un rapporto di durata, rientrante nell'esercizio dell'attività istituzionale svolta dai soggetti obbligati, che non si esaurisce in un'unica operazione;
- **Responsabile del punto operativo o vice**: il soggetto responsabile della dipendenza, dell'ufficio, di altro punto operativo, unità organizzativa o struttura dell'intermediario o del soggetto cui compete l'amministrazione e la gestione concreta dei rapporti con la clientela o suo vice (rientrano in tale definizione anche i Settoristi) ove presente e in conformità delle attribuzioni allo stesso assegnate sulla base della regolamentazione interna della banca;
- **“Riciclaggio”**: a) la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni; b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; d) la partecipazione ad uno degli atti di cui alle lettere a), b) e c) l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolare l'esecuzione;
- **“Rischio di riciclaggio e finanziamento del terrorismo”**: il rischio derivante dalla violazione di previsioni di legge, regolamentari e di autoregolamentazione funzionali alla prevenzione dell'uso del sistema finanziario per finalità di riciclaggio, di finanziamento del terrorismo o di finanziamento dei programmi di sviluppo delle armi di distruzione di massa, nonché il rischio di coinvolgimento in episodi di riciclaggio e di finanziamento del terrorismo o di finanziamento dei programmi di sviluppo delle armi di distruzione di massa;
- **“Rischio inerente”**: indica il rischio che un'attività incorpora prescindendo dalla verifica dell'azione dei Presidi posti a mitigazione del rischio di non conformità. Il Rischio inerente si considera “lordo” qualora consideri esclusivamente la probabilità

teorica e l'impatto potenziale dell'evento di non conformità, mentre si considera "netto" qualora consideri inoltre la valutazione dell'esistenza dei Presidi effettuata in sede di Risk Assessment;

- **"Rischio residuo"**: indica il grado di esposizione al rischio a seguito della verifica sull'adeguatezza e/o sull'efficacia dei Presidi ritenuti funzionali alla mitigazione dei rischi;
- **"Risk Appetite Framework (RAF) - Sistema degli obiettivi di rischio"**: indica il quadro di riferimento che definisce – in coerenza con il massimo rischio assumibile, il business model e il piano strategico – la propensione al rischio, le soglie di tolleranza, i limiti di rischio, le politiche di governo dei rischi, i processi di riferimento necessari per definirli e attuarli;
- **"Risorse economiche"**: le attività di qualsiasi tipo, materiali o immateriali e i beni mobili o immobili, gli accessori, le pertinenze e i frutti, che non sono fondi ma che possono essere utilizzate per ottenere fondi, beni o servizi, possedute, detenute o controllate, anche parzialmente, direttamente o indirettamente, o per interposta persona fisica o giuridica, da parte di soggetti designati, ovvero da parte di persone fisiche o giuridiche che agiscano per conto o sotto la direzione di questi ultimi;
- **Settorista**: il soggetto incaricato dell'amministrazione e gestione concreta del rapporto con un determinato portafoglio di clienti; tali soggetti rientrano nella definizione di Responsabile del punto operativo;
- **"Sistema dei controlli interni"**: indica l'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, il conseguimento delle finalità previste dalla Circolare 285/2013;
- **"Sistema dei controlli interni integrato"**: indica l'interazione nell'esercizio dei compiti (di indirizzo, di attuazione, di verifica e di valutazione) fra gli Organi aziendali e le Funzioni aziendali di controllo; tale interazione implica la condivisione sia di aspetti operativi e metodologici alla base delle attività, sia delle Azioni correttive da intraprendere in caso di rilievi critici per evitare inefficienze e/o duplicazioni. In tale ottica sono stabiliti i diversi "parametri di integrazione" trasversali alle diverse fasi del processo di gestione dei rischi;
- **"Soggetti designati"**: le persone fisiche, le persone giuridiche, i gruppi e le entità designati come destinatari del congelamento sulla base dei regolamenti comunitari e della normativa nazionale;
- **"Statuto"**: indica l'atto contenente le norme relative al funzionamento della Banca Popolare del Cassinate così come previsto dall'art. 2328 c.c.;
- **"Titolare effettivo"**: la persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è

instaurato o l'operazione è eseguita;

- **“Trasferimento di fondi”**: i trasferimenti così come definiti all'art. 3, paragrafo 1, punto 9, del Regolamento (UE) n. 2015/847 del Parlamento europeo e del Consiglio. Ai sensi dell'art. 3, paragrafo 1, punto 9, del Regolamento (UE) n. 2015/847 del Parlamento Europeo e del Consiglio, con il termine «trasferimento di fondi» si intende un'operazione effettuata almeno parzialmente per via elettronica per conto di un ordinante da un prestatore di servizi di pagamento, allo scopo di mettere i fondi a disposizione del beneficiario mediante un prestatore di servizi di pagamento, indipendentemente dal fatto che l'ordinante e il beneficiario siano il medesimo soggetto e che il prestatore di servizi di pagamento dell'ordinante e quello del beneficiario coincidano, fra cui:
  - a) bonifico, quale definito all'articolo 2, punto 1), del regolamento (UE) n. 260/2012;
  - b) addebito diretto, quale definito all'articolo 2, punto 2), del regolamento (UE) n. 260/2012;
  - c) rimessa di denaro, quale definita all'articolo 4, punto 13), della direttiva 2007/64/CE, nazionale o transfrontaliera;
  - d) trasferimento effettuato utilizzando una carta di pagamento, uno strumento di moneta elettronica o un telefono cellulare o ogni altro dispositivo digitale o informatico prepagato o post pagato con caratteristiche simili.

## 1.2. Contesto normativo di riferimento

Di seguito si riportano i principali riferimenti normativi vigenti in ambito comunitario:

- Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018, che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE;
- Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che abroga le Direttive 2005/60/CE del Parlamento europeo e del Consiglio e 2006/70/CE della Commissione;
- Regolamento (UE) 2015/847 del Parlamento europeo e del Consiglio del 20 maggio 2015 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il Regolamento (CE) n. 1781/2006 del 15 novembre 2006;
- Orientamenti congiunti ai sensi dell'articolo 17 e 18, paragrafo 4, della direttiva (UE) 2015/849 sulle misure semplificate e rafforzate di adeguata verifica della clientela e sui fattori che gli enti creditizi e gli istituti finanziari dovrebbero prendere in considerazione nel valutare i rischi di riciclaggio e finanziamento del terrorismo associati ai singoli rapporti continuativi e alle operazioni occasionali (4 gennaio 2018);

- Orientamenti congiunti ai sensi dell'articolo 25 del regolamento (UE) 2015/847 sulle misure che i prestatori di servizi di pagamento dovrebbero adottare per individuare dati informativi mancanti o incompleti relativi all'ordinante o al beneficiario nonché sulle procedure che dovrebbero porre in essere per gestire un trasferimento di fondi non accompagnato dai dati informativi richiesti (16 gennaio 2018).

I principali riferimenti normativi nazionali sono:

- Decreto Legislativo 21 novembre 2007 n. 231 recante attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione e successive modifiche e integrazioni (di seguito anche "decreto" o "decreto antiriciclaggio");
- Decreto Legislativo 22 giugno 2007 n. 109 recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE e successive modifiche e integrazioni;
- Provvedimento della Banca d'Italia recante disposizioni su organizzazione, procedure e controlli in materia antiriciclaggio del 26 marzo 2019;
- Provvedimento della Banca d'Italia recante disposizioni attuative in materia di adeguata verifica della clientela del 30 luglio 2019;
- Provvedimento della Banca d'Italia recante disposizioni specifiche per la conservazione e l'utilizzo dei dati e delle informazioni ai fini antiriciclaggio e di contrasto al finanziamento del terrorismo (consultazione chiusa il 01.10.2018, in attesa dell'emanazione del Provvedimento in versione definitiva);
- Istruzioni UIF in materia di comunicazioni oggettive ai sensi dell'art. 47, comma 3, del Decreto del 28 marzo 2019;
- Provvedimento Banca d'Italia del 24 agosto 2010 ("decalogo SOS");
- Schemi e modelli di anomalia emanati dalla UIF ai sensi dell'art. 6, comma 7, lett. b) del D. Lgs. n. 231 del 2007 ante modifiche D. Lgs. n. 90/2017;
- Indicatori di anomalia emanati dalla UIF ai sensi dell'art. 35, comma 1, del Decreto;
- Regolamento IVASS del 12 febbraio 2019 n. 44 recante le disposizioni, attuative del d. Lgs. 21/11/2007 n. 231, in materia di organizzazione, procedure, controlli interni e adeguata verifica della clientela, e tiene conto degli Orientamenti congiunti delle Autorità Europee di Vigilanza sulle misure semplificate e rafforzate di adeguata verifica della clientela e sui fattori da considerare nel valutare il rischio di riciclaggio e di finanziamento del terrorismo associato ai rapporti continuativi e alle operazioni occasionali.

### **1.3. Obiettivi del documento**

La Policy definisce le linee guida per la prevenzione, la mitigazione e la gestione del rischio di riciclaggio e di finanziamento del terrorismo nella Banca, tenuto conto delle disposizioni normative e regolamentari vigenti e delle *best practice* di settore.

In particolare nella Policy sono formalizzati i principi generali inerenti:

- il processo di adeguata verifica della clientela, con riferimento anche alle misure di adeguata verifica semplificata e rafforzata;
- il sistema di conservazione dei dati e delle informazioni ai fini antiriciclaggio;
- il sistema dei controlli interni;
- il processo di segnalazione di operazioni sospette.

Inoltre nel documento risultano descritti:

- i ruoli e le responsabilità degli Organi e delle altre unità organizzative aziendali;
- i principi generali che caratterizzano la struttura organizzativa e le modalità di presidio del rischio di riciclaggio e di finanziamento del terrorismo.

La Policy è corredata da "Linee Guida", predisposte e applicabili principalmente per la Banca, che risultano parte integrante della stessa ed aventi ad oggetto l'adeguata verifica della clientela, la conservazione dei dati e delle informazioni, il sistema dei controlli interni e la segnalazione delle operazioni sospette.

#### **1.4. Adozione e aggiornamento del documento**

Il presente documento e i successivi aggiornamenti allo stesso sono approvati e adottati con delibera del Consiglio di Amministrazione, sentiti il Collegio Sindacale e il Comitato per il monitoraggio dei rischi.

La Funzione Antiriciclaggio cura l'aggiornamento della Policy nel caso in cui si verificano variazioni di rilievo nella disciplina di riferimento ovvero nell'organizzazione aziendale, sottoponendola all'approvazione di cui sopra.

La Policy ed i relativi aggiornamenti sono pubblicati nel Documentale aziendale sulla intranet e nella sezione del sito internet dedicata all'antiriciclaggio.

#### **1.5. Destinatari**

Il presente documento è applicabile alla Banca, che lo adotta con delibera del proprio Organo con funzione di supervisione strategica.

Il documento è reso disponibile e facilmente accessibile agli Organi aziendali, ai dipendenti e ai collaboratori della Banca.

## **2. PRINCIPI GENERALI E LIMITI OPERATIVI**

La Banca assicura un'azione di prevenzione e di contrasto al riciclaggio e al finanziamento del terrorismo coerente con l'articolazione societaria, la complessità e la dimensione aziendale, la tipologia dei servizi e prodotti offerti e le caratteristiche della clientela servita tramite:

- la definizione degli orientamenti strategici e della politica per la gestione complessiva del rischio di riciclaggio;
- i sistemi organizzativi e procedure idonei a garantire l'osservanza degli obblighi di adeguata verifica della clientela, di segnalazione delle operazioni sospette e di conservazione dei dati;
- la chiara definizione dei ruoli, dei compiti e delle responsabilità in capo a ciascun presidio organizzativo;
- l'istituzione della Funzione Antiriciclaggio quale Funzione di controllo specificatamente deputata a sovrintendere alla prevenzione e gestione dei rischi di riciclaggio;
- l'esercizio di un'attività costante di controllo sul rispetto, da parte del personale, delle procedure interne adottate e degli obblighi di legge e regolamentari in materia di antiriciclaggio.

La Banca si impegna a prevenire e mitigare il rischio di essere, anche inconsapevolmente, strumentalizzato per la realizzazione di attività di riciclaggio e di finanziamento del terrorismo e adotta misure proporzionate al rischio in relazione alla tipologia di clientela, al tipo di prodotto o servizio richiesto, all'area geografica di riferimento e ai canali di distribuzione utilizzati.

Al fine di evitare il coinvolgimento in attività di riciclaggio e di finanziamento del terrorismo, la Banca adotta i seguenti principi generali di comportamento, avuto riguardo, in primo luogo, ai divieti e agli adempimenti previsti dalla normativa esterna ed interna di riferimento e coerentemente con i valori dei codici etici aziendali.

In conformità alla normativa vigente, è fatto assoluto divieto di:

- instaurare rapporti, eseguire operazioni e mantenere rapporti continuativi già in essere con entità diverse da persona fisica di cui siano, direttamente o indirettamente, parte società fiduciarie, trust, società anonime<sup>1</sup> o controllate attraverso azioni al portatore aventi sede in un Paese terzo ad alto rischio (art. 42, comma 2, del Decreto);
- instaurare rapporti, eseguire operazioni e mantenere rapporti continuativi già in essere con entità diverse da persona fisica aventi sede in un Paese terzo ad alto rischio di cui non sia possibile identificare il titolare effettivo né verificarne l'identità (art. 42, comma 2, del Decreto);
- instaurare o mantenere, anche indirettamente, conti correnti di corrispondenza con Banche di comodo (art. 25, comma 3, del Decreto);
- avvalersi, qualora le attività di adeguata verifica della clientela siano demandate a terzi, di soggetti terzi con sede in Paesi terzi ad alto rischio (art. 29, comma 1, del

---

<sup>1</sup>Tipo di società, in cui i nominativi dei titolari delle partecipazioni societarie non sono resi pubblici (non risultano da pubblici registri).

Decreto);

- instaurare, in qualunque forma, conti o libretti di risparmio in forma anonima o con intestazione fittizia nonché l'utilizzo in qualunque forma di conti o libretti di risparmio in forma anonima o con intestazione fittizia aperti presso Stati esteri (art. 50, commi 1 e 2, del Decreto).

E' altresì fatto divieto di:

- eseguire operazioni ovvero instaurare o proseguire rapporti che coinvolgono soggetti inclusi nelle black lists dei soggetti designati dal Consiglio di Sicurezza dell'ONU, dall'Unione Europea e dai decreti del Ministero dell'Economia e delle Finanze; aprire conti di passaggio intrattenuti con un ente creditizio o istituto finanziario corrispondente di un Paese terzo che vengono utilizzati da clienti che hanno accesso diretto a tali conti per effettuare transazioni;
- instaurare rapporti o eseguire operazioni con compro oro, cambiavalute e prestatori di servizi relativi all'utilizzo di valuta virtuale, non debitamente registrati, offrire prodotti e servizi che:
  - favoriscano in qualunque modo l'anonimato;
  - favoriscano l'elusione delle limitazioni all'uso del contante e dei titoli al portatore;
  - ostacolino i processi di adeguata verifica della clientela e, in particolare, la raccolta di tutte le informazioni richieste dalla normativa esterna ed interna in materia;
  - ostacolino la tracciabilità e la conservazione dei dati inerenti i rapporti e l'operatività posta in essere dalla clientela;
  - ostacolino le attività di monitoraggio dell'operatività posta in essere dalla clientela.

L'apertura di rapporti con:

- trust insediati in Paesi terzi (cliente diretto);
- società fiduciarie insediate in Paesi terzi (cliente diretto);
- istituti di pagamento e agenti in attività finanziaria autorizzati a svolgere servizi di pagamento di rimessa di denaro (c.d. money transfer);
- intermediari bancari, finanziari e assicurativi insediati in Paesi terzi ad alto rischio;
- società anonime insediate in paesi terzi;
- società con azioni al portatore insediati in Paesi terzi;
- società partecipate da società anonime;
- società partecipate da società insediate in paesi terzi nel cui capitale sociale sono presenti azioni al portatore.

è subordinata ad apposita autorizzazione della Funzione Antiriciclaggio e/o di eventuali altri organi individuati dalla Banca e definiti nella normativa interna di riferimento.

La Banca presta inoltre particolare attenzione ai prodotti a duplice uso<sup>2</sup>, nonché ai nuovi prodotti o servizi che possano essere considerati suscettibili di essere utilizzati a fini di (i) finanziamento dei programmi di proliferazione di armi di distruzione di massa e movimentazione di sostanze chimiche pericolose, (ii) elusione di ulteriori restrizioni commerciali specifiche o generali (divieto di esportazione e di importazione) o restrizioni finanziarie (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti) previste verso territori a rischio e (iii) finanziamento di operazioni aventi per oggetto il commercio o la produzione di armi o sistemi di armamento.

La Funzione Antiriciclaggio può proporre ulteriori limitazioni di operatività, da formalizzare nella normativa interna, nei confronti di particolari soggetti, settori, prodotti, servizi e operazioni ad alto rischio, individuati sulla base delle comunicazioni e delle informazioni rese tempo per tempo disponibili dalle Autorità di Vigilanza e dagli organismi nazionali e internazionali.

### **3. RUOLI E RESPONSABILITÀ**

#### **3.1. Ruoli e responsabilità degli Organi aziendali**

Al fine di mitigare il rischio di riciclaggio e di finanziamento del terrorismo, risulta imprescindibile il coinvolgimento degli Organi aziendali ed il corretto adempimento degli obblighi previsti dalla normativa vigente. Nei seguenti capitoli si illustrano gli obblighi che ricadono su ciascun Organo aziendale.

##### **3.1.1. Organo con funzione di supervisione strategica**

Il Consiglio di Amministrazione, nella propria funzione di organo con funzione di supervisione strategica:

- approva e riesamina periodicamente gli orientamenti strategici e le politiche di governo dei rischi di riciclaggio e di finanziamento del terrorismo riportate nel presente documento;
- approva l'istituzione della Funzione Antiriciclaggio, di cui nomina e revoca il Responsabile, sentito il Collegio Sindacale, individuandone i compiti, le responsabilità e le modalità di coordinamento e collaborazione con le altre Funzioni aziendali di controllo. La nomina del Responsabile avviene previa individuazione e proposta da parte del Direttore Generale;
- nomina e revoca il Delegato SOS, sentito il Collegio Sindacale, individuandone i compiti, le responsabilità e le modalità di coordinamento e collaborazione con la Funzione Antiriciclaggio. La nomina del Delegato SOS avviene previa

---

<sup>2</sup> I prodotti a duplice uso sono i prodotti, inclusi il software e le tecnologie, che possono avere un utilizzo sia civile sia militare; essi comprendono tutti i beni che possono avere sia un utilizzo non esplosivo sia un qualche impiego nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari.

individuazione e proposta da parte del Direttore Generale;

- approva le linee di indirizzo di un sistema di controlli interni organico e coordinato, funzionale alla pronta rilevazione e alla gestione dei rischi di riciclaggio e di finanziamento del terrorismo, assicurandone l'efficacia nel tempo;
- assicura la chiara e appropriata distribuzione dei compiti e delle responsabilità in materia antiriciclaggio, dotando le Funzioni aziendali di controllo e le altre strutture operative aziendali di risorse qualitativamente e quantitativamente adeguate all'assolvimento dei loro compiti;
- assicura la predisposizione di un sistema di flussi informativi idoneo, adeguato, completo e tempestivo verso gli Organi aziendali e tra le Funzioni aziendali di controllo; in tale ambito, esamina e approva, con cadenza annuale, la Relazione della Funzione Antiriciclaggio, che riporta le attività svolte dalla Funzione nel corso dell'anno, unitamente alle risultanze emerse nell'esercizio di autovalutazione;
- approva i principi e gli orientamenti per la gestione dei rapporti con la clientela classificata ad alto rischio;
- valuta i rischi conseguenti all'operatività con Paesi terzi ad alto rischio, individuando i presidi antiriciclaggio atti a mitigarli e monitorandone l'efficacia;
- assicura la tutela della riservatezza nella segnalazione delle operazioni sospette;
- assicura che le carenze e le anomalie riscontrate in esito ai controlli siano portate tempestivamente a sua conoscenza, promuovendo l'adozione di idonee misure correttive e valutandone l'efficacia.

### **3.1.2. Organo con funzione di gestione**

Il Direttore Generale, in qualità di organo con funzione di gestione:

- definisce un sistema di controlli interni funzionale alla pronta rilevazione e alla gestione del rischio di riciclaggio e ne assicura l'efficacia nel tempo in coerenza con le evidenze tratte dall'esercizio di autovalutazione dei rischi;
- cura l'attuazione degli indirizzi strategici e delle politiche di governo del rischio di riciclaggio approvati dall'organo con funzione di supervisione strategica;
- è responsabile dell'adozione di tutte le misure necessarie ad assicurare l'efficacia dell'organizzazione e del sistema dei controlli antiriciclaggio;
- definisce i flussi informativi volti ad assicurare la conoscenza dei fattori di rischio a tutte le Funzioni aziendali coinvolte nel sistema dei presidi antiriciclaggio e agli Organi competenti;
- definisce e cura l'attuazione delle procedure di gestione dei rapporti con la clientela classificata ad alto rischio in coerenza con i principi generali fissati dall'Organo con funzione di supervisione strategica;
- definisce e cura l'attuazione della procedura per la segnalazione delle operazioni sospette assicurando l'omogeneità dei comportamenti, il pieno utilizzo delle

informazioni rilevanti, la tracciabilità del processo, la tutela della riservatezza dei soggetti coinvolti nella procedura di segnalazione e l'adozione di adeguati strumenti, anche informatici, per la rilevazione delle operazioni anomale;

- definisce e cura l'attuazione delle iniziative e delle procedure per assicurare il tempestivo assolvimento degli obblighi di comunicazione alle autorità competenti in linea con le previsioni della normativa antiriciclaggio;
- assicura che le procedure e i sistemi informativi consentano il corretto adempimento degli obblighi di adeguata verifica della clientela, segnalazione delle operazioni sospette e conservazione dei documenti e delle informazioni;
- stabilisce i programmi di formazione del personale sugli obblighi previsti dalla disciplina in materia di antiriciclaggio. In tale ambito, l'attività deve rivestire carattere di continuità e di sistematicità, tenuto conto dell'evoluzione della normativa di riferimento e delle procedure interne e approva, annualmente, una relazione in ordine all'attività di addestramento e formazione in materia di normativa antiriciclaggio;
- stabilisce gli strumenti idonei a consentire la verifica dell'attività svolta dal personale.

### **3.1.3. Organo con funzione di controllo**

Il Collegio Sindacale, in qualità di organo con funzione di controllo, vigila sull'osservanza della normativa e sulla completezza, funzionalità e adeguatezza dei sistemi di controllo antiriciclaggio e di contrasto al finanziamento del terrorismo, avvalendosi delle strutture interne per lo svolgimento delle verifiche e degli accertamenti necessari e utilizza flussi informativi provenienti dal Responsabile Antiriciclaggio, dalle Funzioni aziendali di controllo e da altri Organi aziendali.

Il Collegio Sindacale:

- esprime parere sulle decisioni concernenti la nomina del Responsabile della Funzione Antiriciclaggio;
- esprime parere sulle decisioni concernenti la nomina del Delegato SOS;
- esprime parere sulla definizione delle politiche per il governo dei rischi di riciclaggio del denaro e di finanziamento del terrorismo;
- valuta l'idoneità delle procedure che consentono l'adempimento degli obblighi di adeguata verifica della clientela, conservazione delle informazioni e segnalazione delle operazioni sospette;
- analizza i motivi delle carenze, anomalie e irregolarità, promuovendo l'adozione di adeguate misure correttive;
- comunica tempestivamente al Responsabile delle segnalazioni di operazioni sospette le operazioni anomale di cui viene a conoscenza nell'esercizio delle proprie funzioni;

- informa tempestivamente l’Autorità di Vigilanza di tutti i fatti di cui venga a conoscenza nell’esercizio delle proprie funzioni quando costituiscano violazioni gravi o ripetute o sistematiche o plurime delle disposizioni di legge e delle relative disposizioni attuative.

### **3.2. Ruoli e responsabilità delle Funzioni aziendali**

Il sistema dei presidi di prevenzione, mitigazione e gestione dei rischi di riciclaggio e di finanziamento del terrorismo coinvolge gli Organi e le Funzioni aziendali, che allineano la propria operatività alla normativa tempo per tempo vigente.

#### **3.2.1. Funzione Antiriciclaggio**

La Funzione Antiriciclaggio presiede, secondo un approccio risk based, alla gestione dei rischi di riciclaggio e di finanziamento del terrorismo con riguardo all’attività aziendale attraverso la valutazione dell’adeguatezza delle procedure interne volte a prevenire la violazione di norme esterne (leggi e regolamenti) e di autoregolamentazione (ad esempio Statuto e Codici Etici) applicabili.

La Funzione Antiriciclaggio è indipendente e dotata di risorse qualitativamente e quantitativamente adeguate ai compiti da svolgere, attivabili in autonomia accedendo ad un budget messo a disposizione dall’Organo con funzione di supervisione strategica.

Nell’esercizio dei suoi compiti la Funzione Antiriciclaggio - che riferisce direttamente all’Organo con funzione di supervisione strategica- ha accesso, secondo le modalità ritenute più opportune, a tutte le attività e le informazioni da essa ritenute rilevanti ai fini dello svolgimento dei propri compiti.

I compiti della Funzione Antiriciclaggio previsti dalla normativa si traducono in molteplici attività riconducibili a:

- definizione delle politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo;
- autovalutazione dei rischi di riciclaggio e di finanziamento del terrorismo;
- consulenza e supporto agli organi aziendali;
- analisi di impatto delle normative;
- aggiornamento di regole interne e procedure;
- adeguata verifica;
- controlli interni;
- rapporti con UIF e Autorità di Vigilanza;
- obblighi formativi;
- reporting.

##### **3.2.1.1. Responsabile Antiriciclaggio**

Il Responsabile della Funzione Antiriciclaggio (Chief AML Officer o CAMLO o Responsabile della funzione) è nominato e revocato direttamente dal Consiglio di Amministrazione, sentito il Collegio Sindacale e su proposta del Direttore Generale.

La decisione di nomina o revoca del Responsabile della Funzione Antiriciclaggio è comunicata formalmente alla Banca d'Italia entro 10 giorni dalla delibera del Consiglio di Amministrazione.

Il Responsabile Antiriciclaggio, riferisce delle proprie attività direttamente al Consiglio di Amministrazione e informa il Collegio Sindacale e si relaziona con gli Organi Aziendali della Banca, rendendoli partecipi degli esiti delle attività svolte per quanto di loro competenza.

Il Responsabile della Funzione Antiriciclaggio deve essere in possesso dei requisiti di indipendenza, autorevolezza e professionalità necessari per assolvere efficacemente ai compiti conferiti; ricopre, nell'assetto organizzativo della Banca, una posizione gerarchico-funzionale adeguata all'incarico assegnato e non ha alcuna responsabilità diretta di aree operative, né dipende gerarchicamente da soggetti responsabili di dette aree.

### **3.2.1.2. Responsabile delle segnalazioni di operazioni sospette**

Il Responsabile del Servizio Segnalazioni operazioni Sospette è Delegato SOS ed è nominato e revocato direttamente dal Consiglio di Amministrazione, sentito il Collegio Sindacale e su proposta del Direttore Generale.

Il ruolo del Delegato SOS è adeguatamente formalizzato e reso pubblico all'interno della Banca e la nomina e la revoca del medesimo sono comunicate tempestivamente alla UIF con le modalità indicate dalla stessa Autorità ed all'Autorità di Vigilanza locale.

In caso di temporanea assenza e/o impedimento e/o necessità di supporto per lo smaltimento di carichi operativi il Delegato SOS viene sostituito o coadiuvato dal Responsabile della Funzione Antiriciclaggio.

Il Delegato SOS possiede adeguati requisiti di indipendenza, autorevolezza e professionalità, svolgendo la propria attività con autonomia di giudizio e riservatezza anche nei confronti delle altre Funzioni Aziendali. Il Delegato SOS non ha pertanto responsabilità dirette in aree operative, né dipende gerarchicamente da soggetti impiegati in dette aree.

Nell'esercizio delle funzioni che gli sono affidate, il Responsabile delle segnalazioni di operazioni sospette:

- valuta, alla luce di tutti gli elementi disponibili, le operazioni sospette provenienti dalle unità operative o di cui sia venuto altrimenti a conoscenza nell'ambito della propria attività;
- trasmette alla UIF le segnalazioni ritenute fondate, omettendo l'indicazione

dell'identità dei soggetti coinvolti nella procedura di segnalazione dell'operazione;

- comunica l'esito delle proprie valutazioni al responsabile di primo livello che ha dato origine alla segnalazione, assicurando la tutela della riservatezza;
- mantiene evidenza delle valutazioni effettuate nell'ambito della procedura, anche in caso di mancato invio della segnalazione alla UIF.

Il Responsabile delle segnalazioni di operazioni sospette svolge le proprie attività con autonomia di giudizio e riservatezza anche nei confronti delle altre Funzioni aziendali. Ai fini dello svolgimento dei propri compiti, egli:

- ha libero accesso, direttamente o per il tramite di strutture organizzative da lui coordinate, ai flussi informativi concernenti la prevenzione del riciclaggio e del finanziamento del terrorismo diretti agli Organi aziendali e alle unità organizzative coinvolte a vario titolo nell'assetto dei presidi organizzativi antiriciclaggio;
- acquisisce ogni informazione utile dalle unità operative che svolgono il primo livello di analisi delle operazioni anomale;
- utilizza, ai fini di valutazione, anche eventuali elementi desumibili da fonti informative liberamente accessibili;
- è tenuto a conoscere ed applicare con rigore ed efficacia le istruzioni, gli schemi e gli indicatori emanati di volta in volta dalla UIF nell'ambito delle sue prerogative;
- svolge un ruolo di interlocuzione unitaria con le Autorità<sup>3</sup> e risponde tempestivamente alle eventuali richieste di approfondimento provenienti dalla UIF.

Ferma la tutela della riservatezza dell'identità dei soggetti che prendono parte alla procedura di segnalazione delle operazioni, il Responsabile fornisce, anche attraverso l'utilizzo di idonee basi informative, informazioni sui nominativi dei clienti oggetto di segnalazione di operazioni sospette ai responsabili delle strutture competenti ai fini dell'attribuzione o aggiornamento del profilo di rischio dei clienti stessi.

### **3.2.2. Funzione Internal Audit**

La Funzione di Internal Audit verifica in modo continuativo il grado di adeguatezza dell'assetto organizzativo aziendale e la sua conformità rispetto alla disciplina di riferimento e vigila sulla funzionalità del complessivo sistema dei controlli interni.

La funzione, attraverso controlli sistematici anche di tipo ispettivo, verifica tra l'altro:

- il costante rispetto degli obblighi di adeguata verifica, sia nella fase di instaurazione del rapporto continuativo, sia nel corso del rapporto stesso;
- l'effettiva acquisizione e l'ordinata conservazione dei dati e dei documenti secondo quanto prescritto dalla normativa;

---

<sup>3</sup> Si fa riferimento agli Organi istituzionali quali, ad esempio, la Magistratura, la Guardia di Finanza e il Nucleo speciale di Polizia Valutaria che possono essere coinvolti nelle fasi di investigazione e di approfondimento a seguito di segnalazioni di operazioni sospette provenienti dal sistema finanziario.

- l'effettivo grado di coinvolgimento del personale e dei responsabili delle strutture centrali e periferiche nell'attuazione degli obblighi di comunicazione e segnalazione.

Gli interventi, sia a distanza che ispettivi, devono essere oggetto di pianificazione per consentire che tutte le strutture operative periferiche e centrali siano sottoposte a verifica in un congruo arco di tempo e che le iniziative siano più frequenti nei confronti delle strutture maggiormente esposte ai rischi di riciclaggio nonché con riferimento ai rapporti a profilo di rischio "alto".

La Funzione Internal Audit svolge interventi di follow-up per assicurarsi dell'avvenuta adozione degli interventi correttivi delle carenze e irregolarità riscontrate e della loro idoneità a evitare analoghe situazioni.

La Funzione riporta, almeno annualmente, agli organi aziendali informazioni sull'attività svolta e sui suoi esiti, fermo restando il rispetto degli obblighi di riservatezza previsti dal decreto antiriciclaggio.

### **3.2.3. Funzione Commerciale**

La Funzione Commerciale coinvolge la Funzione Antiriciclaggio in merito a progetti innovativi compresa l'operatività in nuovi prodotti o servizi (o in caso di modifiche significative a prodotti / servizi già esistenti) collaborando all'identificazione dei rischi potenziali e fornendo, ove applicabili, valutazioni quantitative.

### **3.2.4. Funzioni aziendali di controllo**

La Funzione Antiriciclaggio collabora con le altre Funzioni aziendali di controllo per sviluppare le proprie metodologie di gestione del rischio tenuto conto delle strategie e dell'operatività aziendale, disegnando processi conformi alla normativa vigente e prestando attività di consulenza.

### **3.2.5. Altre Funzioni aziendali**

Le altre Funzioni aziendali, ciascuna per le aree di propria competenza, sono tenute a:

- segnalare le novità intervenute nelle prassi operative;
- comunicare situazioni di non conformità alle norme di cui vengano a conoscenza;
- collaborare nell'individuazione degli interventi di mitigazione necessari per la risoluzione delle anomalie eventualmente riscontrate;
- attivare prontamente gli interventi di adeguamento necessari, comunicando i relativi stati di avanzamento.

### **3.2.6. Personale**

Il Personale, ciascuno nell'ambito delle proprie attribuzioni e competenze, è tenuto ad operare nel rispetto degli obblighi di legge e ad assicurare la corretta attuazione delle politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo. Il Personale è responsabile, per quanto di propria competenza, nell'ambito delle mansioni attribuite:

- della corretta identificazione della clientela ai fini antiriciclaggio;
- della corretta esecuzione degli obblighi di adeguata verifica della clientela e dei controlli antiterrorismo;
- della corretta conservazione dei dati identificativi dei soggetti e delle informazioni raccolte in sede di adeguata verifica della clientela;
- della segnalazione tempestiva ai soggetti competenti, secondo la procedura di segnalazione stabilita nella normativa interna, di ogni circostanza per la quale sa, sospetta, ha ragionevoli motivi per sospettare che siano state compiute, tentate o siano in corso operazioni di riciclaggio, di finanziamento del terrorismo o che i fondi, indipendentemente dalla loro entità, provengano da un'attività criminosa;
- della segnalazione, attraverso i canali dedicati, delle possibili violazioni, potenziali o effettive, delle disposizioni dettate in materia di prevenzione del riciclaggio e del finanziamento del terrorismo (c.d. *whistleblowing*);
- della comunicazione ai soggetti competenti delle eventuali violazioni alle disposizioni in materia di limitazioni all'uso del contante e dei titoli al portatore e di divieto di conti e libretti di risparmio in forma anonima o con intestazione fittizia, per le quali sussiste l'obbligo di comunicazione al Ministero dell'Economia e delle Finanze;
- della collaborazione attiva con la Funzione Antiriciclaggio, in particolare fornendo risposte tempestive ed esaurienti alle eventuali richieste di informazioni e approfondimenti.

In ogni caso, il Personale si attiene alle indicazioni impartite dalla documentazione interna in materia di antiriciclaggio ed antiterrorismo e partecipa ai programmi di formazione definiti dalla Funzione Antiriciclaggio.

#### **4. GESTIONE DEI RISCHI DI RICICLAGGIO E DI FINANZIAMENTO DEL TERRORISMO**

In questo capitolo sono riportati i principi generali della normativa antiriciclaggio per la gestione dei rischi di riciclaggio e di finanziamento del terrorismo:

- adeguata verifica;
- conservazione dei dati e delle informazioni;
- controlli interni;
- segnalazione delle operazioni sospette.

Gli specifici ambiti di applicazione e i criteri per l'adempimento dei suddetti obblighi normativi risultano dettagliati nei rispettivi documenti di "Linee Guida".

## 4.1. Principi generali in materia di adeguata verifica

### 4.1.1. Approccio basato sul rischio e profilatura della clientela

In base al principio dell'approccio basato sul rischio<sup>4</sup>, l'intensità e l'estensione degli obblighi di adeguata verifica della clientela sono modulati secondo il grado di rischio associato a ciascun cliente.

Al fine di valutare il rischio di riciclaggio e di finanziamento del terrorismo, si considerano i seguenti criteri<sup>5</sup>:

- criteri generali di valutazione concernenti il cliente: nell'identificare i fattori di rischio, si valuta, con riferimento al cliente, all'eventuale titolare effettivo e, ove rilevante, all'esecutore, la tipologia di soggetto e le sue caratteristiche, il paese o l'area geografica di provenienza (anche dei fondi), le relazioni d'affari, l'attività svolta e i paesi con i quali vi siano collegamenti significativi<sup>6</sup>, il profilo economico e finanziario (in termini reddituali e patrimoniali), nonché l'inclusione nelle liste delle persone e degli enti associati ad attività di finanziamento del terrorismo previste dai Regolamenti comunitari o dai Regolamenti ministeriali adottati ai sensi del D. Lgs. n. 109/2007; il personale considera altresì il comportamento tenuto al momento dell'apertura del rapporto o del compimento dell'operazione;
- criteri generali di valutazione concernenti il rapporto o l'operazione: nell'identificare i fattori di rischio inerenti al prodotto o al servizio offerti, si prendono in considerazione la tipologia di prodotto o servizio, la loro struttura (valutata in termini di complessità e trasparenza), i canali utilizzati per la loro distribuzione, l'eventuale coinvolgimento di più parti, le tecnologie e i metodi di pagamento che li contraddistinguono, l'ammontare, la frequenza e il volume delle transazioni, la ragionevolezza del rapporto continuativo o dell'operazione in relazione all'attività svolta e al complessivo profilo economico del cliente (e dell'eventuale titolare effettivo) e l'area geografica di destinazione dei fondi; il personale è tenuto a prestare maggiore attenzione ad eventuali prodotti e ai servizi nuovi o innovativi e a quelli che permettono il ricorso frequente al denaro contante o che consentono l'esecuzione di operazioni di importo particolarmente elevato.

La valutazione del rischio di riciclaggio rileva nelle seguenti fasi:

- in fase iniziale, per l'assolvimento degli obblighi di adeguata verifica, mediante la valutazione degli elementi di identificazione del cliente, dell'esecutore e del titolare effettivo per l'instaurazione del rapporto continuativo o l'esecuzione di

---

<sup>4</sup> L'approccio basato sul rischio può essere esercitato nei limiti fissati dall'ordinamento. In nessun caso esso può essere applicato in violazione di obblighi puntualmente definiti da previsioni di legge o regolamentari.

<sup>5</sup> Cfr. art. 17, comma 3 del Decreto.

<sup>6</sup> Qualora si tratti di rapporti od operazioni che coinvolgono un Paese terzo, la Banca valuta la robustezza complessiva dei presidi antiriciclaggio in essere in quel paese, verificando altresì se esso è soggetto a sanzioni finanziarie, embargo o misure correlate al finanziamento del terrorismo o alla proliferazione delle armi di distruzione di massa.

un'operazione occasionale;

- per tutta la durata del rapporto con il cliente, attraverso l'esame della complessiva operatività, la verifica e l'aggiornamento dei dati e delle informazioni acquisite nello svolgimento delle attività di adeguata verifica.

Alla luce di tali criteri, la Banca adotta un modello di profilatura che consente di assegnare automaticamente un profilo di rischio.

La Banca attribuisce un profilo di rischio alla clientela, avvalendosi di procedure informatiche volte ad assicurare che il profilo di rischio proposto in automatico dal sistema sia coerente con la conoscenza del cliente.

Le fasce del profilo di rischio sono quattro (irrelevante, basso, medio, alto).

A ciascuna fascia di rischio i destinatari associano un coerente livello di profondità, estensione e frequenza delle misure di adeguata verifica, affinché sia sempre assicurata l'adeguatezza della loro portata all'entità dello specifico rischio di riciclaggio o di finanziamento del terrorismo.

La frequenza di aggiornamento degli obblighi di adeguata verifica viene svolta nella Banca nei tempi massimi di seguito indicati:

- profilo alto ogni 6 mesi;
- profilo medio ogni anno;
- profilo basso ogni 2 anni;
- profilo irrilevante ogni 4 anni.

Il profilo di rischio è assegnato o aggiornato in occasione:

- dell'apertura di un rapporto continuativo;
- dell'esecuzione di un'operazione che rilevi ai fini antiriciclaggio;
- dell'elaborazione mensile eseguita dal sistema di profilatura;

#### **4.1.2. Adeguata Verifica della Clientela**

La Banca adempie agli obblighi di adeguata verifica della clientela in relazione ai rapporti e alle operazioni che rientrano nella propria attività istituzionale quando:

- il cliente richiede l'instaurazione di un rapporto continuativo;
- il cliente dispone l'esecuzione di un'operazione occasionale che comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro<sup>7</sup>, indipendentemente dal fatto che sia effettuata con un'operazione unica o con più operazioni che appaiono collegate per realizzare un'operazione frazionata. Nell'ambito della normativa interna, la soglia di importo per l'effettuazione dell'adeguata verifica è definita in 5.000 euro, ed è coincidente

---

<sup>7</sup> Rientrano tra le operazioni occasionali i casi in cui la banca agisce da tramite nei trasferimenti di denaro contante o titoli al portatore effettuati a qualsiasi titolo tra soggetti diversi, di importo complessivamente pari o superiore a quello previsto dall'art. 49, comma 1 del Decreto.

con il limite fissato nelle disposizioni delle Autorità di vigilanza in materia di conservazione dei dati;

- il cliente effettua operazioni di prelievamento / versamento di contanti per importi pari o superiori alla soglia di 10.000 €;
- il cliente dispone l'esecuzione di un'operazione occasionale che consista in un trasferimento di fondi<sup>8</sup> superiore a 1.000 euro;
- ogni volta vi sia un sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile;
- quando vi sono dubbi sulla completezza, l'attendibilità o la veridicità delle informazioni o della documentazione acquisiti ai fini di adeguata verifica della clientela.

Al fine di assicurare il corretto adempimento degli obblighi di adeguata verifica della clientela, le strutture competenti effettuano:

- l'identificazione del cliente e, ove presenti, l'esecutore e il titolare effettivo, attraverso l'acquisizione dei dati identificativi e delle informazioni, nonché la raccolta di copia dei documenti identificativi<sup>9</sup>;
- la ricostruzione, secondo un approccio basato sul rischio, dell'assetto proprietario e di controllo della clientela diversa da persona fisica, al fine di riscontrare, con ragionevole certezza, l'identità del titolare effettivo dichiarato dall'esecutore all'atto dell'identificazione;
- la verifica dei dati relativi al cliente e, ove presenti, all'esecutore e al titolare effettivo, mediante il riscontro della veridicità dei dati identificativi e delle informazioni acquisite all'atto dell'identificazione valutando, secondo un approccio basato sul rischio, l'estensione e la profondità dei controlli da effettuare;
- l'acquisizione e la valutazione delle informazioni sullo scopo e sulla natura prevista del rapporto continuativo<sup>10</sup>, sulle relazioni intercorrenti tra il cliente e l'esecutore e tra il cliente e il titolare effettivo, nonché in merito all'attività lavorativa ed economica svolta e, in generale, alle relazioni d'affari del cliente e del titolare effettivo;
- la conservazione della documentazione acquisita in sede di adeguata verifica della clientela in conformità alle disposizioni tempo per tempo vigenti in materia di trattamento dei dati personali;

---

<sup>8</sup> Così come definiti all'art. 3, paragrafo 1, punto 9, del Regolamento (UE) n. 2015/847 del Parlamento europeo e del Consiglio.

<sup>9</sup> L'identificazione del cliente è sempre effettuata in presenza del cliente. Ove il cliente sia un soggetto diverso da una persona fisica, l'identificazione del cliente è effettuata attraverso le dichiarazioni e le informazioni fornite dall'esecutore dotato di formale potere di rappresentanza. L'identificazione del titolare effettivo è effettuata, senza che sia necessaria la sua presenza fisica, contestualmente all'identificazione del cliente e sulla base dei dati identificativi da questi forniti.

<sup>10</sup> La Banca richiede e valuta anche le informazioni sullo scopo e sulla natura delle operazioni occasionali, quando rilevano, secondo un approccio basato sul rischio, elementi che potrebbero configurare un elevato rischio di riciclaggio e di finanziamento del terrorismo.

- l'esercizio di un controllo costante nel corso del rapporto continuativo attraverso:
  - o l'individuazione, mediante l'esame della complessiva operatività del cliente e l'eventuale acquisizione di ulteriori informazioni significative ai fini della valutazione del rischio di riciclaggio, di elementi di incongruenza con il profilo economico e finanziario del cliente;
  - o l'aggiornamento periodico dei dati identificativi e delle informazioni inerenti alla clientela, tramite la raccolta di un questionario di adeguata verifica, secondo la frequenza determinata dal profilo di rischio, nonché in occasione dell'acquisizione di particolari qualifiche (es. cariche rilevanti a fini PEP).

#### **4.1.3. Misure semplificate di adeguata verifica**

In presenza di un basso rischio di riciclaggio e di finanziamento del terrorismo, determinato sulla base di specifici indici di basso rischio disciplinati nella normativa di riferimento esterna - relativi a clientela, prodotti, servizi, operazioni o canali di distribuzione, area geografica di riferimento - la Banca applica misure semplificate di adeguata verifica connotate da una riduzione dell'estensione e della frequenza degli adempimenti rispetto alle misure ordinarie di adeguata verifica, adempiendo in ogni caso a tutte le fasi di cui consta il processo di adeguata verifica della clientela.

Le misure di adeguata verifica semplificata identificate dalle disposizioni normative consistono nella possibilità di:

- modulare i tempi di esecuzione delle attività ai fini dell'identificazione del cliente, dell'esecutore o del titolare effettivo;
- verificare i dati relativi al titolare effettivo limitandosi ad acquisire una dichiarazione di conferma dei dati sottoscritta dal cliente, sotto la propria responsabilità;
- presumere lo scopo e la natura del rapporto continuativo, in relazione alla tipologia di prodotto o servizio offerto e alla tipologia di cliente servito, laddove siano destinati ad uno specifico utilizzo;
- aggiornare le informazioni e i dati raccolti per l'adeguata verifica al ricorrere di specifiche circostanze - quali ad esempio l'apertura di un nuovo rapporto o l'effettuazione di un'operazione di importo superiore ad una determinata soglia;
- ridurre la frequenza e la profondità della analisi effettuate nell'ambito del controllo costante del rapporto monitorando, ad esempio, solamente le operazioni che abbiano un importo al di sopra di una certa soglia definita internamente coerentemente con lo scopo e la natura del rapporto e la tipologia di cliente.

L'adeguata verifica non può essere condotta in forma semplificata laddove sussistano dubbi, incertezze o incongruenze in relazione ai dati identificativi e alle informazioni acquisite in sede di identificazione del cliente, dell'esecutore ovvero del titolare effettivo.

In particolare, le misure di adeguata verifica semplificata non trovano applicazione

quando:

- vengono meno le condizioni per l'applicazione delle misure semplificate, in base agli indici di rischio previsti dalla normativa in materia esterna ed interna;
- le attività di monitoraggio sulla complessiva operatività del cliente e le informazioni acquisite nel corso del rapporto inducono a escludere la presenza di una fattispecie a basso rischio;
- vi sia comunque il sospetto di riciclaggio o di finanziamento del terrorismo.

In funzione di un approccio basato sul rischio e della connessione tra gli indici di basso rischio relativi alla clientela e all'area geografica disciplinati dalla normativa di riferimento, la Banca applica misure di adeguata verifica in maniera semplificata in presenza di:

- intermediari bancari comunitari o con sede in un paese terzo con un efficace regime di contrasto al riciclaggio e al finanziamento del terrorismo;
- intermediari finanziari e imprese assicurative comunitarie o con sede in un paese terzo con un efficace regime di contrasto al riciclaggio e al finanziamento del terrorismo;
- società ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che includono quelli di assicurare un'adeguata trasparenza della titolarità effettiva;
- pubbliche amministrazioni (di cui all'articolo 1, comma 2, del D. Lgs. 165/2001, e s.m.i.)<sup>11</sup>.

Nel caso in cui la Persona Politicamente Esposta agisca in veste di organo della Pubblica Amministrazione, la Banca adotta misure di adeguata verifica della clientela commisurate al rischio in concreto rilevato, tenuto conto anche che a dette Pubbliche Amministrazioni si rendono applicabili le citate misure di adeguata verifica semplificata.

Le misure semplificate di adeguata verifica applicate dalla Banca sono diversificate sulla base della tipologia di controparte - intermediario bancario, intermediario finanziario o impresa assicurativa, società quotata, pubblica amministrazione - ed in termini di:

- contenuto e modalità di raccolta del Questionario di adeguata verifica ai fini dell'identificazione del cliente, dell'esecutore e del titolare effettivo (es. per le Banche è previsto un Questionario dedicato cartaceo mentre per le società quotate, le pubbliche amministrazioni e gli intermediari bancari, finanziari e imprese assicurative è raccolto il Questionario standard procedurale);
- modalità di conservazione dei dati e della documentazione acquisiti, con particolare riferimento all'alimentazione dell'Archivio Unico Informatico aziendale

---

<sup>11</sup>Per le Pubbliche Amministrazioni diverse da quelle ricomprese all'art. 1, comma 2, del D. Lgs. 165/2001 e s.m.i. - (i) enti pubblici nazionali ; (ii) società (non quotate) partecipate dalle amministrazioni pubbliche e dalle loro controllate, ai sensi dell'articolo 2359 del codice civile, limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o dall'Unione europea ; (iii) soggetti preposti alla riscossione dei tributi nell'ambito della fiscalità nazionale o locale, quale che ne sia la forma giuridica - le Banche aderenti applicano misure ordinarie di adeguata verifica.

(es. per le società quotate è prevista la registrazione dei rapporti e delle operazioni in Archivio Unico Informatico mentre per le banche e gli intermediari bancari, finanziari e imprese assicurative le registrazioni di rapporti e operazioni sono conservate nei sistemi gestionali).

Nella valutazione della sussistenza di un effettivo basso rischio, la Banca considera:

- i casi in cui l'intermediario bancario, finanziario o impresa assicurativa sia interessato da commissariamento o interventi sanzionatori o altri provvedimenti da parte delle Autorità di Vigilanza o giudiziarie;
- i casi in cui la pubblica amministrazione sia sottoposta a provvedimenti di commissariamento o di infiltrazione criminale;
- le società quotate ammesse alla quotazione su un mercato regolamentato non sottoposte ad obblighi di comunicazione che impongono un'adeguata trasparenza della titolarità effettiva.

In ogni caso, non si rendono applicabili le misure semplificate di adeguata verifica per tutti i soggetti considerati a "basso rischio", qualora ricorrano i fattori di rischio elevato definiti dalla normativa primaria e secondaria di riferimento (es. presenza nella compagine societaria di società anonime con azioni al portatore / trust / fiduciarie, residenza in un Paese Terzo ad alto rischio).

Qualora una Banca rifiuti l'apertura o revochi un rapporto con un Istituto di Pagamento è tenuta a darne comunicazione preventiva alla Funzione Antiriciclaggio al fine di adempiere agli obblighi di cui all'art. 114-octiesdecies del TUB e alla Comunicazione di Banca d'Italia "Apertura e mantenimento di conti di pagamento presso una banca a favore di istituti di pagamento. Provvedimento di attuazione dell'art. 114-octiesdecies del D.Lgs.: 1° settembre 1993, N. 385.

Per il dettaglio sulle specifiche misure di adeguata verifica semplificata previste per ciascuna fattispecie si rimanda alle "Linee guida per l'adeguata verifica della clientela".

#### **4.1.4. Misure rafforzate di adeguata verifica**

In presenza di un elevato rischio di riciclaggio e di finanziamento del terrorismo, determinato sulla base di specifiche previsioni normative ovvero di un'autonoma valutazione del profilo di rischio del cliente, sono previste misure rafforzate di adeguata verifica della clientela connotate da una maggiore profondità, estensione e frequenza rispetto alle misure ordinarie.

In applicazione del principio dell'approccio basato sul rischio, tali misure consistono:

- nell'acquisizione di maggiori informazioni - anche esterne al patrimonio aziendale - relative a:
  - o l'identità del cliente e, ove presenti, dell'esecutore e del titolare effettivo nonché, in caso di cliente diverso da persona fisica, l'assetto proprietario e di controllo

del cliente ai fini della determinazione della titolarità effettiva; tali informazioni possono riguardare, a titolo esemplificativo ma non esaustivo, notizie reputazionali, presenza di atti pregiudizievoli, legami familiari - indagando anche la situazione lavorativa, economica e patrimoniale di familiari e conviventi - e relazioni d'affari;

o l'origine del patrimonio e dei fondi impiegati dal cliente nel rapporto, ricavati ad esempio da bilanci d'esercizio, dichiarazioni IVA e dei redditi e documenti forniti dal datore di lavoro o da altri intermediari;

o il rapporto continuativo, come ad esempio il volume, l'entità e la frequenza dell'operatività attesa sul rapporto, la destinazione dei fondi, la natura dell'attività svolta dal cliente e dall'eventuale titolare effettivo, le relazioni d'affari e i rapporti con altri intermediari;

- nella possibilità che il cliente effettui, al momento dell'apertura del rapporto, un bonifico da un conto a lui intestato presso un'altra banca comunitaria o con sede in uno dei Paesi terzi con adeguati presidi antiriciclaggio tra quelli individuati dalla Funzione Antiriciclaggio;
- nell'acquisizione dell'autorizzazione del Direttore Generale o suo delegato per l'avvio o la prosecuzione del rapporto continuativo nei casi previsti dal Decreto antiriciclaggio e dalle disposizioni delle Autorità di vigilanza in materia di adeguata verifica;
- nella maggiore frequenza degli aggiornamenti delle informazioni acquisite.

La Banca applica sempre misure rafforzate di adeguata verifica della clientela, in presenza di:

- fattispecie di adeguata verifica rafforzata ex legge definite dal legislatore ed in particolare nei casi di:
  - o rapporti continuativi o operazioni occasionali che coinvolgono paesi terzi ad alto rischio
  - o rapporti di corrispondenza transfrontalieri con un intermediario bancario o finanziario corrispondente con sede in un Paese terzo
  - o rapporti continuativi o operazioni occasionali con clienti e relativi titolari effettivi che rivestono la qualifica di persone politicamente esposte
  - o clienti che compiono operazioni caratterizzate da importi insolitamente elevati ovvero rispetto alle quali sussistono dubbi circa la finalità cui le medesime sono, in concreto, preordinate;
- un rischio di riciclaggio alto risultante dalla combinazione degli elementi di rischio - di tipo anagrafico, di rapporto e di operatività - del sistema di profilatura.

Le misure di adeguata verifica si sostanziano in:

- **informazioni integrative** che è necessario acquisire sul cliente (elementi aggiuntivi del Questionario rispetto alle informazioni già richieste – es. reddito e patrimonio);
- **documentazione aggiuntiva**, a supporto delle attività di verifica, richiesta al cliente o reperita in autonomia da ciascuna Banca (es. documentazione attestante il reddito e il patrimonio dichiarato);
- **workflow autorizzativi differenziati** che possono coinvolgere cumulativamente o alternativamente, in aggiunta al Responsabile di Punto Operativo, le seguenti figure: (ii) Direttore Generale o suo Delegato; (iii) Funzione AML.
- **tempistiche di aggiornamento / controllo costante differenziate**, al fine di effettuare con una frequenza più ravvicinata l'aggiornamento del set informativo e documentale a disposizione e l'analisi della complessiva operatività del cliente.

Per il dettaglio sulle specifiche misure di adeguata verifica rafforzata previste per ciascuna fattispecie si rimanga alle *"Linee guida per l'adeguata verifica della clientela"*.

#### 4.1.4.1 Persone Politicamente Esposte

L'utilizzo di fondi ottenuti illecitamente da soggetti che ricoprono - o hanno ricoperto da meno di un anno - cariche pubbliche, nonché i loro familiari diretti o coloro che non detti soggetti intrattengono notoriamente stretti legami, a seguito di reati quali la corruzione, la concussione o il peculato può tradursi in riciclaggio.

La Banca pertanto verifica, sulla base dell'approccio basato sul rischio, se il cliente e l'eventuale titolare effettivo rientrano nella definizione di Persona Politicamente Esposta, commisurando l'intensità e l'estensione delle misure di rafforzata verifica al grado di rischio associato.

A tal fine sono eseguiti, per mezzo di procedure automatizzate, controlli anagrafici mirati a verificare la potenziale presenza, tra la clientela, di nominativi inclusi nelle liste fornite da appositi *provider* esterni<sup>12</sup>. Nella consapevolezza che l'utilizzo esclusivo di *database* commerciali non pone al riparo da errori o incompletezze correlate alla difficoltà di mantenere le liste di riferimento complete e aggiornate, La Banca utilizza in maniera integrata tutte le informazioni a cui possa avere accesso o di cui sia a disposizione a livello aziendale ed extra aziendale nell'ambito del rapporto.

L'acquisizione della qualifica di PEP ovvero eventuali variazioni occorse allo *status* di PEP - del cliente e del titolare effettivo - nel corso del rapporto continuativo sono verificate nel continuo.

Qualora il cliente ed il titolare effettivo rientrino nella definizione di PEP, la Banca:

- raccoglie e valuta le informazioni inerenti all'origine del complessivo patrimonio dei PEPs e degli specifici fondi impiegati nel rapporto o nell'operazione occasionale<sup>13</sup>;

---

<sup>12</sup> Le Liste ad oggi utilizzate sono le liste *World-Check* fornite da *Thomson Reuters*. La Funzione Antiriciclaggio assicura che le procedure informatiche dedicate a tali controlli utilizzino liste costantemente aggiornate.

<sup>13</sup> La raccolta di informazioni deve consentire di acquisire un apprezzabile grado di certezza che i fondi

in tale ambito, in caso di rapporti continuativi, è necessario acquisire un'attestazione del cliente e verificare le informazioni contenute sulla base dei documenti pubblicamente disponibili;

- autorizza, a cura del Direttore Generale o di soggetto delegato, l'avvio o la prosecuzione di un rapporto ovvero l'esecuzione di un'operazione occasionale con un PEP, valutando l'effettiva esposizione al rischio di riciclaggio del PEP e il grado di efficacia dei presidi aziendali;

Nei confronti di soggetti originariamente individuati come PEPs, che abbiano cessato di rivestire le relative cariche pubbliche da oltre un anno, in presenza di un elevato rischio, si continua ad applicare misure di adeguata verifica rafforzata.

#### **4.1.4.2 Rapporti di corrispondenza transfrontalieri con intermediari bancari o finanziari rispondenti di un Paese terzo con regime non equivalente o Paese terzo ad alto rischio**

In base all'approccio basato sul rischio, le misure di adeguata verifica rafforzata applicate nei confronti dell'intermediario rispondente con sede in un Paese terzo con regime non equivalente o Paese terzo ad alto rischio con cui si instauri un conto corrente di corrispondenza transfrontaliero sono modulate, ponendo particolare attenzione, nella valutazione del rischio, al Paese terzo in cui l'ente è insediato.

Accertandosi che l'ente rispondente (rispondente diretto) non sia una Banca di comodo o un intermediario che consenta l'accesso ai rapporti di corrispondenza con banche di comodo, le Banche aderenti:

- formalizzano con il rispondente un accordo scritto recante i termini, gli obblighi, le attività e le responsabilità antiriciclaggio che le parti si impegnano reciprocamente a rispettare;
- acquisiscono ulteriori informazioni sul rispondente, anche mediante informazioni pubblicamente disponibili, al fine di individuare gli assetti proprietari, la natura delle attività svolte e dei servizi offerti e di valutare la sua reputazione e la qualità della vigilanza a cui è sottoposto. In particolare, è necessario acquisire un'espressa attestazione del rispondente circa l'inesistenza di impedimenti normativi o contrattuali in merito alla tempestiva trasmissione delle informazioni richieste;
- valutano il sistema dei controlli interni antiriciclaggio dell'ente mediante l'acquisizione della documentazione interna e, in caso di un elevato rischio, tramite l'esecuzione di ulteriori verifiche;
- autorizzano, per mano del Direttore Generale o altro dipendente delegato, l'apertura di ciascun rapporto di corrispondenza o di passaggio (tale soggetto non

dovrebbe coincidere con il dirigente che ha promosso l'apertura del rapporto d'affari con il rispondente);

- attivano un controllo costante del rapporto, graduandone la frequenza e l'intensità sulla base del servizio di corrispondenza svolto.

#### **4.1.4.3 Rapporti ed operazioni che coinvolgono Paesi Terzi ad alto rischio**

Nei casi di rapporti continuativi, prestazioni professionali e operazioni che coinvolgono paesi terzi ad alto rischio, la Banca applica misure rafforzate di adeguata verifica che si sostanziano in:

- a) acquisizione di informazioni aggiuntive in merito allo scopo e alla natura del rapporto continuativo;
- b) acquisizione di informazioni sull'origine dei fondi e sulla situazione economico-patrimoniale del cliente e del titolare effettivo;
- c) acquisizione di informazioni sulle motivazioni delle operazioni previste o eseguite;
- d) acquisizione di un'autorizzazione del Direttore Generale o suo delegato, prima di avviare o proseguire o intrattenere un rapporto continuativo o effettuare un'operazione che coinvolga paesi terzi ad alto rischio;
- e) assicurare un controllo costante e rafforzato del rapporto continuativo, aumentando la frequenza e l'intensità dei controlli effettuati e individuando schemi operativi da sottoporre ad approfondimento.

La Banca applica misure rafforzate di adeguata verifica ai rapporti e alle operazioni che coinvolgono Paesi Terzi ad alto rischio ed in particolare

- con riferimento ai rapporti continuativi:
  - o al cliente/ titolare effettivo/ titolare ditta individuale residenti/domiciliati ovvero aventi sede legale (in caso di cliente soggetto diverso da persona fisica) in Paesi terzi alto rischio;
  - o al cliente con operatività in Paesi terzi alto rischio.

E' inoltre prevista la raccolta di un questionario di adeguata verifica con riferimento alle operazioni, eseguite a sportello, che coinvolgono un Paese terzo ad alto rischio.

È comunque vietato instaurare o proseguire rapporti continuativi o eseguire operazioni di cui siano parte, direttamente o indirettamente, società fiduciarie, trust, società di diritto estero anonime o controllate attraverso azioni al portatore con sede in Paesi terzi ad alto rischio.

#### **4.1.4.4 Operazioni caratterizzate da importi insolitamente elevati o per le quali sussistono dubbi sulla finalità**

La Banca applica misure rafforzate di adeguata verifica della clientela nei confronti dei clienti che compiono operazioni caratterizzate da importi insolitamente elevati ovvero rispetto alle quali sussistono dubbi circa la finalità cui le medesime sono, in concreto, preordinate.

In particolare, anche ai fini della rilevazione e la valutazione di operazioni e schemi operativi

potenzialmente anomali, rientrano nell'ambito delle operazioni caratterizzate da importi insolitamente elevati o per le quali sussistono dubbi circa le relative, le seguenti fattispecie:

- le operazioni di importo più elevato rispetto a quello atteso sulla base della conoscenza del cliente da parte della singola Banca e della natura e dello scopo del rapporto continuativo;
- gli schemi operativi anomali rispetto all'ordinaria attività del cliente o all'operatività tipica di clienti, prodotti o servizi analoghi;
- le operazioni particolarmente complesse rispetto ad analoghe operazioni associate a tipologie similari di clientela, prodotti o servizi.

Le misure rafforzate di adeguata verifica della clientela applicate dalla Banca al verificarsi di tali casistiche devono essere in grado di consentire alla singola Banca di valutare la natura sospetta delle operazioni e sono finalizzate a:

- comprendere il contesto e le finalità delle suddette operazioni;
- determinare la coerenza dell'operatività posta in essere dal cliente con il suo profilo
- economico - ad esempio attraverso l'acquisizione di ulteriori informazioni sull'origine e sulla destinazione dei fondi e sull'attività del cliente;
- eseguire un più frequente controllo costante del rapporto continuativo e delle ulteriori operazioni eseguite.

#### **4.1.5. Esecuzione da parte di terzi degli obblighi di adeguata verifica**

La Banca può commercializzare prodotti e servizi per il tramite di terzi e demandare a questi, in tutto o in parte, l'assolvimento degli adempimenti di adeguata verifica della clientela - ad eccezione del controllo costante - purché essi rientrino tra gli intermediari elencati all'art. 26, comma 2 del Decreto e ferma la piena responsabilità della Banca popolare del Cassinate per l'osservanza di detti obblighi.

L'attestazione deve essere chiaramente riconducibile al terzo attestante attraverso accorgimenti idonei (es. sottoscrizione da parte del personale a ciò autorizzato o invio con sistemi informatici), e deve essere trasmessa dal terzo e non dal cliente.

Tale attestazione, a seconda dello specifico obbligo di verifica a cui è diretta, deve recare almeno:

- i dati identificativi del cliente e, ove presenti, dell'esecutore e del titolare effettivo;
- le tipologie di fonti utilizzate per l'accertamento e la verifica dell'identità;
- le informazioni sulla natura e sullo scopo del rapporto o dell'operazione occasionale.

Ove gli obblighi non siano assolti in maniera adeguata, la Banca:

- informa il terzo attestante delle eventuali irregolarità o incongruenze;
- apporta le necessarie rettifiche o integrazioni;
- adempie in via diretta agli obblighi di adeguata verifica;
- si astiene dall'instaurare il rapporto continuativo o dall'eseguire l'operazione, valutando se effettuare una segnalazione alla UIF.

La Banca provvede, nell'ambito delle modalità di raccolta e di scambio delle informazioni, a:

- definire con il terzo le fasi dell'adeguata verifica demandate ai terzi, individuando i dati e le informazioni che è necessario siano trasmesse dai terzi e le modalità e la tempistica della trasmissione;
- definire le modalità e gli strumenti per lo scambio tempestivo dei flussi informativi;
- verificare, nei limiti della diligenza professionale, la veridicità dei documenti ricevuti e la correttezza e attendibilità delle informazioni desunte dagli stessi;
- acquisire, ove necessario, informazioni supplementari dai terzi, dal cliente ovvero da altre fonti.

È fatto comunque divieto di avvalersi, per l'esecuzione delle attività di adeguata verifica della clientela, di terzi aventi sede in Paesi terzi ad alto rischio.

Alla Banca può essere demandato l'assolvimento degli adempimenti di adeguata verifica della clientela - ad eccezione del controllo costante - quando faccia da tramite per la commercializzazione di prodotti e servizi di intermediari terzi soggetti alla disciplina antiriciclaggio, sui quali ricade la piena responsabilità per l'osservanza degli obblighi di adeguata verifica della clientela.

La Banca commercializza, secondo le succitate disposizioni normative, i seguenti prodotti / servizi di terzi:

- carte prepagate;
- gestioni patrimoniali mobiliari.

La commercializzazione dei prodotti / servizi è regolata da apposite convenzioni specifiche per prodotto.

#### **4.1.6. Obbligo di astensione**

Qualora ci si trovi nell'impossibilità di assolvere gli obblighi di adeguata verifica della clientela occorre astenersi dall'eseguire l'operazione e dall'instaurare ovvero proseguire il rapporto, valutando l'opportunità di effettuare una segnalazione di operazione sospetta alla UIF.

Nei casi in cui non sia possibile esercitare l'astensione a causa della sussistenza di un obbligo di legge di ricevere l'atto ovvero dell'impossibilità di rinviare l'operazione tenuto conto della normale operatività ovvero quando il differimento dell'operazione possa ostacolare eventuali indagini delle Autorità competenti, la Banca, dopo aver ricevuto l'atto o eseguito l'operazione, inoltra immediatamente alla UIF una segnalazione di operazione sospetta.

#### **4.1.7. Misure di contrasto al finanziamento del terrorismo**

La Banca è fortemente impegnata nella lotta al finanziamento del terrorismo nazionale e internazionale e si dota di appropriati procedure e sistemi interni per prevenire ed evitare l'instaurazione (ovvero la prosecuzione, ove questi siano già in essere) di rapporti e l'esecuzione di operazioni con soggetti inseriti nelle liste di contrasto alle attività terroristiche applicabili secondo le previsioni dell'ordinamento italiano..

A tal fine la Banca:

- esegue, per mezzo di procedure automatizzate, controlli anagrafici mirati a verificare l'eventuale presenza, tra la clientela, di nominativi inclusi nelle liste (c.d. *black lists*) dei soggetti designati dal Consiglio di Sicurezza dell'ONU, dall'Unione Europea, dai decreti del Ministero dell'Economia e delle Finanze, nonché di quella dell'*Office of Foreign Asset Control* (OFAC) degli Stati Uniti; gli esiti di tali controlli sono sempre verificati dal personale incaricato al fine di assicurare il corretto funzionamento delle procedure ed escludere eventuali casi di omonimia (c.d. falsi positivi);
- rifiuta di compiere operazioni che coinvolgano a qualunque titolo soggetti inseriti nelle *black lists* dei soggetti designati dal Consiglio di Sicurezza dell'ONU, dall'Unione Europea, dai decreti del Ministero dell'Economia e delle Finanze (es. ordinanti, beneficiari) e confermati come tali;
- applica, qualora previste dalle disposizioni applicabili, le misure di congelamento dei fondi e delle disponibilità economiche nei confronti dei soggetti per i quali sia stata accertata l'identità di soggetto designato;
- comunica alla UIF le misure applicate ai sensi del Decreto Legislativo 22 giugno 2007 n. 109 e successive modifiche e integrazioni, indicando i soggetti coinvolti, l'ammontare e la natura dei fondi o delle risorse economiche, entro trenta giorni dalla data di entrata in vigore dei regolamenti comunitari, delle decisioni degli organismi internazionali e dell'Unione europea e dei decreti del Ministro dell'Economia e delle Finanze, ovvero, se successiva, dalla data di detenzione dei

fondi e delle risorse economiche.

#### **4.2. Principi generali in materia di conservazione dei dati e delle informazioni**

Tutti i documenti, i dati e le informazioni acquisiti nell'ambito dello svolgimento delle attività di adeguata verifica della clientela sono conservati per un periodo di dieci anni dalla data di cessazione del rapporto continuativo o di esecuzione dell'operazione occasionale.

Ai fini dell'assolvimento degli obblighi di conservazione dei dati e delle informazioni concernenti l'operatività, soggetta ad obblighi antiriciclaggio, della propria clientela, la Banca si avvale dell'Archivio Unico Informatico (AUI) quale archivio standardizzato e strumento idoneo a:

- garantire il rispetto delle norme dettate in materia di protezione dei dati personali;
- prevenire qualsiasi perdita dei dati e delle informazioni e garantire la ricostruzione dell'operatività o attività del cliente;
- garantire l'accesso, in maniera completa e tempestiva, ai fatti e alle informazioni alle autorità;
- acquisire tempestivamente<sup>14</sup> i dati e le informazioni, con indicazione della relativa data;
- assicurare l'integrità dei dati e delle informazioni e la non alterabilità dei medesimi successivamente alla loro acquisizione;
- garantire la trasparenza, la completezza e la chiarezza dei dati e delle informazioni nonché il mantenimento della storicità degli stessi.

Con particolare riferimento all'assolvimento degli obblighi di conservazione dei dati raccolti dalla clientela sottoposti ad adeguata verifica semplificata, i dati in questione sono conservati con le modalità previste dal Decreto e con le esimenti previste dalle Disposizioni delle Autorità di Vigilanza in materia di conservazione ed utilizzo dei dati.

Per la conservazione dei documenti e per la gestione dell'AUI, ferma restando la responsabilità per il corretto assolvimento degli obblighi di conservazione, la Banca si avvale di un centro di servizi autonomo che permette un accesso diretto e immediato ai sistemi di conservazione e registrazione.

I dati registrati nell'AUI sono aggregati mediante procedure informatiche e trasmessi alla UIF, secondo le modalità previste dalla medesima autorità, con cadenza mensile.

La Banca ai sensi delle disposizioni antiriciclaggio applicano gli obblighi di conservazione dei dati e delle informazioni conformemente alle citate disposizioni delle Autorità di Vigilanza in materia di conservazione dei dati.

Per il dettaglio sulle modalità di conservazione si rimanda al documento di *"Linee guida*

---

<sup>14</sup> È considerata tempestiva l'acquisizione conclusa entro trenta giorni dall'instaurazione del rapporto continuativo o dall'esecuzione dell'operazione, dalla variazione e dalla chiusura del rapporto continuativo (cfr. art. 32, comma 2, lett. b) del decreto antiriciclaggio).

sugli obblighi di conservazione e utilizzo dei dati e delle informazioni rilevanti ai fini antiriciclaggio”.

#### 4.3. Principi generali in materia di controlli interni

Il Sistema dei Controlli Interni Antiriciclaggio della Banca ha come obiettivo il monitoraggio nel continuo dei presidi AML inerenti:

- la gestione degli obblighi di adeguata verifica della clientela;
- l’affidabilità del sistema informativo di alimentazione dell’Archivio Standardizzato e dei
- flussi S.AR.A.;
- la tempestiva ed efficace rilevazione delle operazioni potenzialmente sospette.

La valutazione di adeguatezza dei presidi AML è condotta secondo un approccio di proporzionalità al rischio sia nelle fasi preliminari (risk assessment) che in quelle operative (risk based approach). In conformità a quanto previsto dal decreto antiriciclaggio, ciò si traduce nella predisposizione da parte dei soggetti obbligati di presidi, procedure e controlli per mitigare il rischio di riciclaggio e finanziamento al terrorismo adeguati alla loro natura e dimensione.

L’obiettivo del Sistema dei Controlli Interni in ambito antiriciclaggio è quindi di valutare l’efficacia e l’efficienza dei presidi AML determinando l’entità del rischio residuo cui i soggetti obbligati sono esposti.

Il Sistema dei Controlli Interni AML è così costituito dall’insieme delle regole, delle strutture organizzative, dei processi, delle procedure e delle risorse che hanno come obiettivo la prevenzione e la mitigazione del rischio di riciclaggio.

Il Sistema dei Controlli Interni AML è organizzato nelle seguenti macro-categorie di controlli:

- controlli base;
- evidenze automatiche;
- indicatori di rischio (KRI) e indicatori di performance (KPI).

Per il dettaglio sulle specificità riguardanti ciascuna macro-categoria di controllo e sulla metodologia di valutazione dei controlli si rimanda alle *“Linee guida sistema dei controlli interni Antiriciclaggio”*.

#### 4.4. Principi generali in materia di segnalazione delle operazioni sospette

Quando vi sia il sospetto o vi siano motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano dal compimento di un’attività criminosa, la Banca popolare del Cassinate invia

tempestivamente alla UIF una segnalazione di operazione sospetta in conformità a quanto previsto dal Decreto.

Il personale desume il sospetto dalle caratteristiche, dall'entità e dalla natura delle operazioni, dal loro collegamento o frazionamento o da qualsivoglia altra circostanza conosciuta, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui la segnalazione è riferita.

Al fine di agevolare l'individuazione delle operazioni sospette, le strutture fanno riferimento agli schemi comportamentali e agli indicatori di anomalia emanati e periodicamente aggiornati dalla UIF.

A titolo esemplificativo, ma non esaustivo, possono costituire motivo di sospetto:

- l'assunzione, da parte del cliente (o dell'esecutore), di comportamenti anomali al momento dell'esecuzione dell'operazione ovvero dell'instaurazione del rapporto continuativo, come ad esempio la riluttanza del cliente nel fornire le informazioni richieste (specialmente in merito all'origine del patrimonio e dei fondi, quando qualificabile come PEP);
- la disposizione di operazioni non coerenti con il profilo economico e finanziario del cliente (specialmente in caso di ricorso frequente e ingiustificato ad operazioni in contanti);
- l'intervento, nel rapporto o nell'operazione, di terzi privi di un evidente collegamento con il cliente;
- qualsiasi evento che obblighi la Banca alla segnalazione in ragione di una specifica previsione di legge;
- qualsiasi altro evento che non possa essere ricondotto alla normale operatività del cliente e che non possa essere ragionevolmente giustificato sulla base delle informazioni disponibili.

La Banca monitora nel continuo, anche per il tramite di procedure automatiche, l'andamento del rapporto e l'operatività poste in essere dal cliente e, qualora si rilevi un sospetto di riciclaggio del denaro o di finanziamento del terrorismo, è prevista l'attivazione della procedura interna di segnalazione.

È fatto divieto a tutto il personale, ove in possesso dell'informazione, di dare comunicazione al cliente interessato o a terzi della segnalazione o di notizie ad essa relative.

Tale divieto non si applica:

- alle comunicazioni effettuate all'Autorità di Vigilanza nell'esercizio delle funzioni previste dal Decreto;
- alle comunicazioni aventi ad oggetto, in un'ottica di collaborazione attiva, la condivisione delle informazioni con altri intermediari bancari e finanziari, idonee a garantire la corretta osservanza delle prescrizioni dettate in materia di prevenzione del riciclaggio e del finanziamento del terrorismo nei casi relativi allo stesso cliente o

alla stessa operazione, per finalità esclusivamente di prevenzione del riciclaggio o del finanziamento del terrorismo;

- alle comunicazioni con altri intermediari bancari e finanziari appartenenti ad uno stato membro o situati in Paesi terzi, a condizione che questi applichino misure equivalenti a quelle previste dal Decreto, nei casi relativi allo stesso cliente o alla stessa operazione, per finalità esclusivamente di prevenzione del riciclaggio o del finanziamento del terrorismo.

La Banca popolare del Cassinate adotta tutte le misure idonee a tutelare la riservatezza dell'identità delle persone coinvolte nel processo di segnalazione di una operazione sospetta. Il nominativo del segnalante può essere rivelato solo quando l'Autorità giudiziaria, con decreto motivato, lo ritenga indispensabile ai fini dell'accertamento di reati per i quali è stato avviato il procedimento.

Per la declinazione del modello organizzativo utilizzato dalla Banca per la gestione delle SOS si rimanda al documento di "*Linee guida per la segnalazione delle operazioni sospette*".

#### **4.5. Comunicazioni oggettive**

Nell'ambito degli obblighi definiti dall'art.47 del D. Lgs.231/2007 e delle correlate *Istruzioni in materia di comunicazioni oggettive* emanate da Banca d'Italia, la Banca trasmette alla UIF, con cadenza mensile, una comunicazione contenente i dati relativi a ogni movimentazione di denaro contante di importo pari o superiore a 10.000 euro, eseguita nel corso del mese solare a valere su rapporti ovvero mediante operazioni occasionali, anche se realizzata attraverso più operazioni singolarmente pari o superiori a 1.000 euro.

Le operazioni oggetto di comunicazione fanno parte del patrimonio informativo posto a base delle complessive valutazioni sul carattere sospetto dell'operatività dei clienti. La comunicazione oggettiva esclude l'obbligo di segnalazione dell'operazione come sospetta, ai sensi dell'art. 35 del D. Lgs. 231/2007, quando la stessa operazione non presenta collegamenti con altre operazioni di diversa tipologia che facciano desumere una complessiva operatività sospetta ovvero non sia effettuata da clienti ad elevato rischio di riciclaggio e finanziamento del terrorismo.

#### **4.6. Gestione degli embarghi**

Il contesto normativo in materia di embarghi prevede misure restrittive e sanzionatorie dirette contro Paesi terzi, nonché entità non statali e persone fisiche o giuridiche e in particolare:

- embarghi sulle armi;
- altre restrizioni commerciali specifiche o generali (divieto di esportazione e di importazione);

- restrizioni finanziarie (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti);
- restrizioni all'ammissione (divieto di visto o di viaggio);
- sanzioni penali per chi finanzia associazioni terroristiche od eversive e per chi effettua operazioni di esportazione di beni a duplice uso in violazione delle normative amministrative prescritte in tema di "dual use".

Affinché la Banca Popolare del Cassinate non incorra, nell'ambito delle proprie attività istituzionali, in violazioni della normativa in materia di embarghi, tramite le strutture preposte alla gestione dell'operatività con l'estero, promuove l'adozione di misure che assicurino:

- controlli anagrafici e sulle operazioni;
- la tracciabilità dei controlli effettuati per operazioni provenienti da ovvero dirette verso i Paesi, le persone e le entità nei cui confronti sono stabilite restrizioni.

La Banca applica, ove necessario, le restrizioni finanziarie stabilite dagli organismi nazionali ovvero internazionali di riferimento (es. congelamento di beni e risorse, divieti di determinate transazioni finanziarie, divieti di operazioni documentarie legate a esportazione di merce a duplice uso e/o pericolosa) previste dalla normativa tempo per tempo vigente.

#### **4.7. Presidi in materia di trasferimento di fondi**

La Banca, in qualità di prestatori di servizi di pagamento, si dota di procedure interne in grado di individuare le operazioni di pagamento (es. bonifici) prive delle informazioni sull'ordinante e sul beneficiario che devono essere necessariamente riportate in conformità alle disposizioni contenute nel Regolamento (UE) 2015/847 e determinano, in assenza di queste, quando rigettare o sospendere la transazione sulla base delle indicazioni fornite dagli Orientamenti congiunti delle Autorità di Vigilanza europee emanati ai sensi dell'art. 25 del Regolamento (UE) 2015/847 .

Qualora la Banca identifichi un prestatore di servizi di pagamento come ripetutamente inadempiente a seguito dell'omissione dei prescritti dati informativi relativi all'ordinante o al beneficiario, essa è chiamata ad adottare, sulla base di opportune valutazioni e in applicazione dell'approccio basato sul rischio, provvedimenti che possono inizialmente includere richiami e diffide, prima di rifiutare qualsiasi futuro trasferimento di fondi proveniente da quel prestatore di servizi di pagamento o di limitare o porre fine ai suoi rapporti con lo stesso.

Per il dettaglio dei presidi adottati dalla Banca si rimanda alla *"Policy per l'applicazione del Regolamento Europeo n. 847/2015 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il Regolamento CE n.1781/2006"*.

#### **4.8. Limitazioni all'uso del contante e dei titoli al portatore**

La Banca popolare del Cassinate assolve compiutamente agli obblighi in materia di limitazione del contante e dei titoli al portatore ai sensi dell'articolo 49 del Decreto Legislativo 21 novembre 2007, n. 231 successive modifiche e integrazioni.

Ove siano rilevate violazioni alle disposizioni di cui all'art.49, la Banca comunica tempestivamente al Ministero dell'Economia e delle Finanze le infrazioni di cui sia venuta a conoscenza.

#### **4.9. Metodologia di valutazione del rischio**

L'identificazione e la valutazione periodica del rischio inerente e delle correlate vulnerabilità costituiscono il primo momento logico del modello di gestione del rischio e risultano funzionali alla definizione dei principi di appetito al rischio e dei conseguenti limiti da portare all'approvazione degli organi societari nell'ambito del Risk Appetite Framework (RAF) nonché all'individuazione e programmazione degli interventi di mitigazione del rischio in materia di riciclaggio e di finanziamento del terrorismo.

Le disposizioni applicabili prevedono che i soggetti obbligati valutino il livello di rischio cui sono esposti al fine di predisporre procedure, strumenti e controlli appropriati (cosiddetta "autovalutazione") da riportare nella Relazione annuale.

La Banca conduce un'autovalutazione del rischio di riciclaggio cui è esposta con cadenza annuale.

#### **4.10. Formazione del personale e consulenza**

Nella consapevolezza che un'efficace applicazione della normativa antiriciclaggio presuppone la piena conoscenza delle sue finalità, dei relativi principi, degli obblighi e delle responsabilità da essa derivanti, la Banca realizza specifici programmi di formazione del personale sugli obblighi previsti dalla normativa antiriciclaggio e di contrasto al finanziamento del terrorismo, al fine di diffondere tra i propri dipendenti una cultura del rischio di riciclaggio e di sensibilizzare tutto il personale sulle problematiche connesse a tale rischio.

La Banca assicura una specifica preparazione in materia di antiriciclaggio (specialmente in merito agli obblighi di adeguata verifica della clientela) ai dipendenti che sono a più diretto contatto con la clientela e al personale appartenente alla Funzione Antiriciclaggio, dedicando loro continui programmi di formazione affinché siano aggiornati sull'evoluzione del rischio di riciclaggio e sugli schemi tipici delle operazioni finanziarie criminali.

La funzione antiriciclaggio della Banca, in raccordo con le altre funzioni aziendali competenti in materia di formazione, cura la predisposizione di un piano di

addestramento sugli obblighi previsti dalla normativa antiriciclaggio, finalizzato a conseguire un aggiornamento su base continuativa dei suoi dipendenti e dei suoi collaboratori.

All'interno della Relazione sulla pianificazione annuale delle attività della funzione antiriciclaggio, il Responsabile della funzione antiriciclaggio informa il Consiglio di Amministrazione sullo stato di avanzamento dell'attività di formazione.

La funzione antiriciclaggio effettua inoltre attività di consulenza ed assistenza specialistica sulle modalità di assolvimento degli obblighi antiriciclaggio ed antiterrorismo sia nei confronti delle strutture operative coinvolte, sia nei confronti degli Organi Sociali della Banca.

#### **4.11. Sistema interno di segnalazione delle violazioni**

Al fine di garantire la conformità alle disposizioni normative vigenti, la Banca si dota di procedure interne per favorire la segnalazione, da parte del personale, di violazioni potenziali o effettive delle disposizioni normative in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo.

Le procedure adottate sono volte ad assicurare:

- la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'Autorità giudiziaria in relazione ai fatti oggetto delle segnalazioni. In tal caso, l'identità del segnalante intervenuto nel processo può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato;
- la tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie o sleali conseguenti la segnalazione;
- lo sviluppo di un adeguato canale di segnalazione, anonimo e indipendente.

Le segnalazioni delle violazioni inerenti l'antiriciclaggio devono essere inviate in busta chiusa al Responsabile Antiriciclaggio.

#### **5.ALLEGATI**

- Allegato 1: Linee Guida l'adeguata verifica della clientela
- Allegato 2: Linee Guida per la conservazione dei dati e delle informazioni
- Allegato 3: Linee Guida sul sistema dei controlli interni AML
- Allegato 4: Linee Guida per la segnalazione delle operazioni sospette
- Allegato 5: Metodologia per l'autovalutazione dei rischi di riciclaggio e di finanziamento del terrorismo