Banca Popolare di Lajatico

POLICY ANTIRICICLAGGIO

Politiche per la gestione del rischio di riciclaggio e di finanziamento del terrorismo, adottate dall'Organo con funzione di supervisione strategica ai sensi:

- ✓ delle ***Disposizioni***, emanate da Banca d'Italia con Provvedimento del 26/03/2019, ***in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari ai fini di riciclaggio e di finanziamento del terrorismo***;

- ✓ delle ***Disposizioni***, emanate da Banca d'Italia con Provvedimento del 30/07/2019, ***in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo***.

Delibera del Consiglio di Amministrazione del 24/09/2019

ELENCO VERSIONI

NUMERO VERSIONE	DATA DI APPROVAZIONE C.d.A.	NOTE
1	28/07/2011	
2	22/05/2014	
3	20/07/2017	
4	01/08/2019	
5	24/09/2019	

INDICE

1. PREMESSA

1.1 FINALITA' DELLA *POLICY* ANTIRICICLAGGIO

Il presente documento, rubricato *Politiche per la gestione del rischio di riciclaggio e di finanziamento del terrorismo* di seguito brevemente *Policy Antiriciclaggio,* adottato dalla Banca Popolare di Lajatico, di seguito brevemente *Banca*, esprime gli orientamenti strategici e le politiche aziendali per il governo dei rischi connessi con il riciclaggio ed il finanziamento del terrorismo formulati dal Consiglio di Amministrazione su parere favorevole del Collegio Sindacale. Sostituisce il precedente documento deliberato in data 01/08/2019 e sarà oggetto di aggiornamento nel continuo.

La *Policy* definisce:

- gli orientamenti strategici per la gestione dei rischi di riciclaggio e di finanziamento del terrorismo nella Banca, tenuto conto delle disposizioni normative e regolamentari vigenti (e di prossima emanazione) e delle *best practice* di settore;
- i principi generali e le linee guida per la prevenzione, la mitigazione e la gestione del rischio di riciclaggio e di finanziamento al terrorismo;
- i ruoli e le responsabilità degli Organi e delle altre unità organizzative aziendali;
- i processi di gestione e presidio del rischio di riciclaggio e di finanziamento del terrorismo.

La *Policy* prevede, infine, il sistema di *reporting* e di gestione dei flussi informativi tra la Funzione Antiriciclaggio e le Autorità di Vigilanza, gli Organi e le altre unità organizzative aziendali.

1.2 DEFINIZIONI

- **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;
- **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;
- **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**: la Circolare di Banca d'Italia n. 285 del 17 dicembre 2013, recante le Disposizioni di Vigilanza per le banche;
- **Cliente**: il soggetto che instaura rapporti continuativi, compie operazioni ovvero richiede od ottiene una prestazione professionale a seguito del conferimento di un incarico;
- **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;

- **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 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;
- **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**: l'accordo, in qualsiasi forma, tra una banca 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;
- **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 agiscono 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 Antiriciclaggio**: la Funzione Antiriciclaggio della Banca;
- **Funzione aziendale**: 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**: la Funzione di conformità alle norme (*Compliance*), la Funzione di controllo dei rischi (*Risk Management*), la Funzione Antiriciclaggio e la Funzione di revisione interna (*Internal Audit*). Per la Banca è stata istituita anche un'ulteriore Funzione di controllo di II livello – CROR (Controllo Rischi Operativi e Reputazionali) – che svolge, tra gli altri, attività di verifica a distanza e in loco in ambito antiriciclaggio. La Funzione di *Internal Audit* è esternalizzata alla società Unione Fiduciaria S.p.A.;
- **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;
- **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;
- **Persone Politicamente Esposte (PEPs)**: le persone fisiche indicate all'articolo 1, comma 2, lettera dd) del Decreto;
- **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;
- **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.

  La Banca considera rapporti continuativi:
  - conti correnti;
  - depositi a risparmio (nominativi o al portatore);
  - finanziamenti (sotto qualsiasi forma: mutui ipotecari/ chirografari, accolli, prestiti a rientro rateale, apertura di credito in conto corrente, etc.);
  - cassette di sicurezza (questi rapporti non hanno movimentazione di mezzi di pagamento e, quindi, operazioni; per gli stessi vigono gli obblighi di adeguata verifica in relazione all'instaurazione del rapporto e sue variazioni e/o estinzioni);
  - rilascio di garanzie e di impegni di firma (solo quelle rilasciate dalla Banca: crediti di firma);
  - dossier titoli;
  - carte di credito (adeguata verifica svolta dalla Banca nella qualità di intermediario collocatore);
  - carte di debito (escluso il Bancomat che non è un rapporto continuativo);
  - polizze private ramo vita;
  - garanzie acquisite dalla clientela (attive per la Banca);
  - deleghe a operare su rapporti continuativi su c/c e depositi a risparmio di qualsiasi tipo;
  - rapporti di estero commerciale e finanziario e posizioni di portafoglio (inteso come rapporto di portafoglio).

  La Banca, invece, non considera rapporti continuativi:
  - prestazione di servizi di investimento in presenza di dossier titoli in essere presso la Banca;
  - sottoscrizione quote di OICR (fondi comuni e SICAV) e di fondi pensione;
  - acquisto/vendita strumenti finanziari derivati;
  - pronti contro termine;
  - sottoscrizione di prestiti obbligazionari;
  - *time deposit*;

- carte bancomat e carte di credito accessorie al conto di cui il titolare della carta risulta intestatario o delegato;
- conti transitori bancari;
- rapporti di sofferenza;
- pagamenti effettuati presso società che svolgono servizio riscossione tributi;
- contratti di *internet banking* e *home banking*;
- domiciliazione utenze;
- certificati di deposito. Se la sottoscrizione avviene per cassa senza regolamento su rapporto continuativo, la stessa assume configurazione operativa di "operazione occasionale"; pertanto l'adeguata verifica va effettuata con riferimento alla sottoscrizione o rimborso nel caso in cui si presentino i requisiti per configurare una "operazione occasionale" (importo pari o superiore a 5.000 euro, regolamento in contanti);
- versamento conferimento in danaro per costituenda società, che viene considerato un "rapporto tecnico" e rileva esclusivamente in qualità di "operazioni occasionali": pertanto l'adeguata verifica va effettuata con riferimento al versamento nel caso in cui si presentino i requisiti per configurare una "operazione occasionale" (importo pari o superiore a 5.000 euro, regolamento in contanti);
- smobilizzo crediti;
- deposito di titoli al portatore – non in gestione accentrata presso Monte Titoli - effettuato presso la Banca per consentire la partecipazione alle assemblee sociali.

- **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 agevolarne l'esecuzione;
- **Rischio di riciclaggio**: 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;
- **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;
- **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;
- **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:

- bonifico, quale definito all'articolo 2, punto 1), del regolamento (UE) n. 260/2012;
- addebito diretto, quale definito all'articolo 2, punto 2), del regolamento (UE) n. 260/2012;
- rimessa di denaro, quale definita all'articolo 4, punto 13), della direttiva 2007/64/CE, nazionale o transfrontaliera;
- 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 postpagato con caratteristiche simili.

1.3 CONTESTO NORMATIVO DI RIFERIMENTO

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

- Direttiva (UE) 2015/849 (cosiddetta IV Direttiva *AML/CFT*) 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 – così come modificata dalla Direttiva (UE) 2018/843 (cosiddetta V Direttiva *AML/CFT*) del Parlamento europeo e del Consiglio, del 30 maggio 2018 – 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 (in vigore dal 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 (in vigore dal 16 gennaio 2018).

I principali riferimenti normativi nazionali sono:

- Schema di decreto legislativo recante attuazione della Direttiva 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 che modifica la Direttiva 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio e di finanziamento del terrorismo e che modifica le Direttive 2009/138 (CE) e 2013/36 (UE) nonché modifiche ed integrazioni al D.Lgs. n. 231/2007 e ai Decreti legislativi 25 maggio 2017, n. 90 e n. 92, recanti attuazione della Direttiva 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015;
- Decreto Legislativo 21 novembre 2007 n. 231, di seguito brevemente *Decreto* – così come modificato dal D.Lgs. 25 maggio 2017 n. 90 – 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 modiche e integrazioni;
- Decreto Legislativo 22 giugno 2007 n. 109 – così come modificato dal D.Lgs. 25 maggio 2017 n. 90 – 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 del 26 marzo 2019, recante disposizioni su organizzazione, procedure e controlli in materia antiriciclaggio;
- Provvedimento della Banca d'Italia del 30 luglio 2019, recante disposizioni attuative in materia di adeguata verifica della clientela;
- Provvedimento della Banca d'Italia recanti 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);
- Istruzioni UIF del 28 marzo 2019 in materia di comunicazioni oggettive ai sensi dell'art. 47, comma 3, del Decreto;
- Provvedimento Banca d'Italia 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.

1.4 ADOZIONE ED AGGIORNAMENTO DEL DOCUMENTO

Il presente documento e i successivi aggiornamenti allo stesso sono approvati e adottati con delibera del Consiglio di Amministrazione della Banca, sentito il Collegio Sindacale.

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

2. PRESIDI ORGANIZZATIVI, PRINCIPI GENERALI E LIMITI OPERATIVI

2.1 PRESIDI ORGANIZZATIVI

La Banca assicura un'azione di prevenzione e di contrasto al riciclaggio e al finanziamento del terrorismo coerente con l'articolazione aziendale, 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 a livello di Banca;
- 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 dei dipendenti, delle procedure interne adottate e degli obblighi di legge e regolamentari in materia di antiriciclaggio.

2.2 PRINCIPI GENERALI E LIMITI OPERATIVI

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 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 è 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 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* diramate dalle autorità nazionali ed internazionali competenti in materia di contrasto al finanziamento del terrorismo;
- aprire conti di passaggio intrattenuti con un ente creditizio o istituto finanziario corrispondente di un Paese terzo ad alto rischio 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.

La Banca ha inoltre deciso di non operare con *money transfer*[1].

L'apertura di rapporti con:

- trust, società anonime o controllate attraverso azioni al portatore insediati in Paesi terzi;
- intermediari bancari, finanziari e assicurativi insediati in Paesi terzi ad alto rischio;

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

[1] Soggetti convenzionati e agenti diversi dagli agenti in attività finanziaria che svolgono servizi di pagamento di rimessa di denaro (art. 1, comma 2, lett. nn del Decreto e art. 1, comma 2, lett. h-septies.1, n. 6 del TUB).

La Banca presta inoltre particolare attenzione ai prodotti a duplice uso[2], 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 RESPONSABILITA'

3.1 RUOLI E RESPONSABILITA' 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.

3.1.1 ORGANO CON FUNZIONE DI SUPERVISIONE STRATEGICA

L'organo con funzione di supervisione strategica (Consiglio di Amministrazione):

- 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;
- approva la nomina e la revoca, sentito il Collegio Sindacale, del Responsabile delle segnalazioni di operazioni sospette, delegato dal legale rappresentante;
- definisce e 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;
- definisce 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;

[2] 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.

- 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

L'organo con funzione di gestione (Direzione Generale):

- 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;
- è responsabile dell'adozione di tutte le misure necessarie ad assicurare l'efficacia del sistema dei controlli antiriciclaggio;
- definisce la *Policy* per il governo dei rischi di riciclaggio e di finanziamento del terrorismo;
- 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;
- definisce la procedura per la segnalazione delle operazioni sospette assicurando l'omogeneità dei comportamenti, 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 le iniziative e le procedure per assicurare il tempestivo assolvimento degli obblighi di comunicazione alle autorità competenti;
- 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;
- approva 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;
- adotta strumenti idonei a verificare l'assolvimento delle attività a carico del personale.

3.1.3 ORGANO CON FUNZIONE DI CONTROLLO

L'organo con funzione di controllo (Collegio Sindacale), 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 e del conferimento della delega per la segnalazione delle operazioni sospette;
- 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;

- stimola l'approfondimento di eventuali 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, ripetute, sistematiche o plurime delle disposizioni di legge e delle relative disposizioni attuative.

3.2 RUOLI E RESPONSABILITA' 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 basato sul rischio, alla gestione dei rischi di riciclaggio e di finanziamento del terrorismo, attraverso la valutazione dell'adeguatezza dei processi e delle procedure adottate internamente.

La Funzione Antiriciclaggio è indipendente, ha accesso a qualsiasi informazione rilevante per i propri compiti e riferisce direttamente agli Organi aziendali. In coerenza con il principio di proporzionalità, è dotata di risorse qualitativamente e quantitativamente adeguate e comprende il Responsabile della Funzione Antiriciclaggio e il Responsabile delle segnalazioni di operazioni sospette.

Il Responsabile della Funzione Antiriciclaggio è la Dott.ssa Federica Turchi nonché Responsabile delle segnalazioni di operazioni sospette (come da nomina del C.d.A. del 28 luglio 2011); in osservanza della normativa, il suddetto nominativo è stato oggetto di apposita comunicazione ad UIF e Banca d'Italia.

Almeno una volta l'anno, la Funzione presenta agli organi con funzione di supervisione strategica, gestione e controllo una relazione sulle iniziative adottate, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale. Nella relazione confluiscono anche i risultati dell'esercizio di autovalutazione condotto ai sensi della Parte Settima del Provvedimento della Banca d'Italia recante disposizioni attuative su organizzazione, procedure e controlli in materia antiriciclaggio.

3.2.1.1 RESPONSABILE ANTIRICICLAGGIO

La responsabilità della Funzione Antiriciclaggio è attribuita al Responsabile della Funzione Antiriciclaggio, il quale è nominato e revocato - per motivate ragioni - dal Consiglio di Amministrazione, sentito il Collegio Sindacale.

La nomina e la revoca del Responsabile della Funzione Antiriciclaggio sono comunicate formalmente alla Banca d'Italia entro 20 giorni dalla delibera del Consiglio di Amministrazione.

Il Responsabile della Funzione Antiriciclaggio riferisce direttamente agli Organi aziendali, ha accesso diretto all'organo con funzione di supervisione strategica e all'organo con funzione di controllo e comunica con essi senza restrizioni o intermediazioni.

Il Responsabile della Funzione Antiriciclaggio:

- deve essere in possesso di adeguati requisiti di indipendenza, autorevolezza e professionalità e non deve avere responsabilità dirette di aree operative né deve essere gerarchicamente dipendente da soggetti responsabili di dette aree;
- assicura il controllo di conformità sull'applicazione della normativa primaria e secondaria di riferimento;

- collabora e si coordina con le altre Funzioni aziendali coinvolte nel processo di gestione dei rischi di riciclaggio e di finanziamento del terrorismo.

3.2.1.2 RESPONSABILE DELLE SEGNALAZIONI DI OPERAZIONI SOSPETTE ("DELEGATO S.O.S.")

All'interno della Funzione Antiriciclaggio della Banca è individuato il Responsabile delle segnalazioni di operazioni sospette al quale è conferita la delega - di cui all'art. 36, comma 6, del D. Lgs. n. 231/2007 e successive modifiche e integrazioni - dal legale rappresentante, deliberata dall'Organo con funzione di supervisione strategica, sentito il Collegio Sindacale.

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;
- informa dell'esito della propria valutazione il 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:

- 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;
- 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 controlli anche a campione, anche avvalendosi del supporto di altre funzioni aziendali, sulla congruità delle valutazioni effettuate dai soggetti di primo livello sull'operatività della clientela;
- svolge un ruolo di interlocuzione unitaria con le Autorità[3] e risponde tempestivamente alle eventuali richieste di approfondimento provenienti dalla UIF.

Il Responsabile delle segnalazioni di operazioni sospette non deve avere responsabilità dirette di aree operative né deve essere gerarchicamente dipendente da soggetti di queste aree. Il ruolo del Responsabile delle segnalazioni è adeguatamente formalizzato e reso pubblico all'interno della struttura e la nomina e la revoca del medesimo responsabile sono comunicate tempestivamente alla UIF con le modalità indicate dalla stessa Autorità.

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 stante la particolare pregnanza che tale informazione può rivestire in sede di apertura di nuovi rapporti contrattuali ovvero di valutazione dell'operatività della clientela già in essere.

[3] 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.

3.2.2 FUNZIONE DI REVISIONE INTERNA (*"INTERNAL AUDIT"*)

La Funzione di *Internal Audit*, mediante controlli a distanza o ispettivi, verifica in modo continuativo il grado di adeguatezza dell'assetto organizzativo aziendale e la sua conformità rispetto alla disciplina di riferimento e in particolare:

- il rispetto degli obblighi di adeguata verifica, sia nella fase di instaurazione del rapporto continuativo, sia nel corso del rapporto stesso;
- il rispetto dell'obbligo di conservazione dei dati e delle informazioni acquisite nell'ambito delle attività di adeguata verifica della clientela, accertando l'effettiva acquisizione e l'ordinata conservazione dei dati e dei documenti secondo quanto prescritto dalla normativa primaria e secondaria di riferimento;
- l'effettivo grado di coinvolgimento del personale e dei responsabili delle strutture centrali e periferiche nell'attuazione dell'obbligo di collaborazione attiva.

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 di *Internal Audit* svolge interventi di *follow-up* per verificare l'adozione degli interventi correttivi prescritti a seguito della rilevazione di carenze ed irregolarità e può effettuare, su richiesta e in raccordo con la Funzione Antiriciclaggio, controlli in loco su base campionaria per verificare l'efficacia e la funzionalità delle procedure e dei processi antiriciclaggio e individuare eventuali criticità.

La Banca ha deciso di esternalizzare la Funzione di *Internal Audit* alla società Unione Fiduciaria S.p.A., come da accordo di esternalizzazione del 25 giugno 2014 cui si rimanda.

A far data dal 23 aprile 2018, le attività di verifica in loco presso le Filiali in ambito antiriciclaggio sono demandate alla Funzione CROR, come da circolare interna n. 70/2018.

3.2.3 COMITATO DI CONTROLLO NUOVI PRODOTTI

L'Ufficio *Marketing* coinvolge la Funzione Antiriciclaggio e le altre Funzioni interessate (come le ulteriori Funzioni di controllo e l'Ufficio Organizzazione e Processi) in sede di ideazione ovvero di ingresso in nuovi mercati e segmenti e sviluppo di nuovi prodotti, servizi e canali, 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 DIPENDENTE

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 sanno, sospettano, hanno 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

4.1 APPROCCIO BASATO SUL RISCHIO E PROFILATURA DELLA CLIENTELA

In base al principio dell'approccio basato sul rischio[4], 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[5]:

a) 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/o la sua natura giuridica) 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[6], il profilo economico

[4] 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. Tra questi rientrano gli obblighi di congelamento previsti nei confronti di soggetti inseriti nelle liste dell'Unione Europea, emanate anche in attuazione delle Risoluzioni dell'Organizzazione delle Nazioni Unite, per il contrasto al finanziamento del terrorismo e all'attività dei Paesi che minacciano la pace e la sicurezza internazionale. Ne consegue che non è possibile instaurare o mantenere un rapporto d'affari con soggetti inclusi in tali liste se non nei limiti e alle condizioni tassativamente previste dalle norme di legge.

[5] Cfr. art. 17, comma 3 del Decreto.

[6] 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.

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;

b) criteri generali di valutazione concernenti il rapporto continuativo 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 e finanziario 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.

Si dispone che la Banca non esegua alcuna operazione senza la presenza fisica del cliente, fatta eccezione per i seguenti casi:

- operazioni effettuate con sistemi di cassa continua, sportelli automatici o per corrispondenza;
- operazioni effettuate attraverso soggetti che svolgono attività di trasporto valori;
- operazioni effettuate mediante carte di pagamento;
- disposizioni impartite mediante canale *internet* (*trading on line*, *internet banking*);
- disposizioni impartite mediante canale *corporate banking* interbancario (*home banking*).

Si definisce che sia classificabile "ingente" il patrimonio superiore ad euro 300.000.

Si definisce altresì di "cospicuo ammontare" la singola operazione superiore ad euro 100.000.

Alla luce di tali criteri, 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 (irrilevante; basso; medio; alto).

A ciascuna fascia di rischio i destinatari associano un coerente livello di profondità, estensione e frequenza delle misure di adeguata verifica.

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;
- di specifici eventi quali acquisizione della qualifica PEP, accertamenti penali/indagini finanziarie, variazioni di compagine societaria (es. partecipazioni di società fiduciarie e/o trust), cambiamento di attività (in settori a rischio), notizie di stampa rilevanti ai fini antiriciclaggio, invio di segnalazioni di operazioni sospette, cambio residenza verso Paesi terzi ad alto rischio.

4.2 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[7], 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 della Banca, la soglia di importo per l'effettuazione dell'adeguata verifica è definita in 5.000 euro, ed è coincidente con il limite fissato nelle disposizioni delle Autorità di vigilanza in materia di conservazione dei dati;
- il cliente dispone l'esecuzione di un'operazione occasionale che consista in un trasferimento di fondi[8] 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[9];
- 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[10], 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;
- l'esercizio di un controllo costante nel corso del rapporto continuativo attraverso:
    - 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;

[7] 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.

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

[9] 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.

[10] 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'aggiornamento periodico dei dati identificativi e delle informazioni inerenti alla clientela secondo la frequenza determinata dal profilo di rischio, nonché in occasione dell'acquisizione di particolari qualifiche (es. cariche rilevanti a fini PEP).

  A tale proposito, si specifica che, a livello operativo:

  - ✓ per il profilo di rischio ***alto*** l'aggiornamento avviene almeno ogni **12** mesi;
  - ✓ per il profilo di rischio ***medio*** l'aggiornamento avviene almeno ogni **24** mesi;
  - ✓ per il profilo di rischio ***basso*** l'aggiornamento avviene almeno ogni **48** mesi;
  - ✓ per il profilo di rischio ***irrilevante*** l'aggiornamento avviene almeno ogni **60** mesi.

4.2.1 MISURE SEMPLIFICATE DI ADEGUATA VERIFICA

In presenza di un basso rischio di riciclaggio e di finanziamento del terrorismo, determinato sulla base di specifici fattori, la Banca applica misure semplificate di adeguata verifica connotate da una minore profondità, estensione e frequenza rispetto alle misure ordinarie, 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 o del titolare effettivo;
- verificare l'identità del 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;
- effettuare la revisione del profilo di rischio del cliente al ricorrere di specifiche circostanze (quali, ad esempio, l'apertura di una nuova tipologia di rapporto) e comunque almeno ogni 5 anni;
- ridurre la frequenza e la profondità dei controlli effettuati 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 ed in funzione dello scopo e della natura del rapporto e della 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;
- 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.

L'identificazione dei clienti considerati a basso rischio, e dei relativi esecutori e titolari effettivi, viene effettuata attraverso l'acquisizione - mediante apposito questionario antiriciclaggio - dei dati identificativi e delle ulteriori informazioni previste, nonché con la raccolta di copia del documento identificativo dell'esecutore.

4.2.2 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:
    - 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;
    - 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; la verifica del reddito e del patrimonio è raccomandata in presenza di clientela con un profilo di rischio alto;
    - 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;
- nell'acquisizione dell'autorizzazione del Direttore Generale per l'avvio o la prosecuzione del rapporto continuativo nei casi previsti dal Decreto e dalle disposizioni delle Autorità di vigilanza in materia di adeguata verifica;
- nella maggiore frequenza degli aggiornamenti delle informazioni acquisite, tramite:
    - ✓ controlli più frequenti sul rapporto continuativo, volti a rilevare tempestivamente eventuali variazioni del profilo di rischio del cliente;
    - ✓ controlli più frequenti o approfonditi sulle operazioni, per rilevare tempestivamente eventuali elementi di sospetto di riciclaggio. In questo ambito, occorre verificare la destinazione dei fondi e le ragioni alla base di una determinata operatività.

In presenza di operazioni caratterizzate da importi "insolitamente elevati" ovvero rispetto alle quali sussistono dubbi circa la finalità cui le medesime sono, in concreto, preordinate, risulta opportuno adottare appropriate misure rafforzate di adeguata verifica della clientela per verificare l'eventuale natura sospetta delle operazioni in questione attraverso:

- la comprensione del contesto e delle finalità delle operazioni, nonché della coerenza con il profilo economico e finanziario del cliente;
- un più frequente controllo costante del rapporto continuativo e delle ulteriori operazioni eseguite.

Rientrano in questo ambito:

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

In conformità alle disposizioni normative vigenti, si applica in ogni caso il regime rafforzato di adeguata verifica al ricorrere dei seguenti casi:

- clienti, titolari effettivi ed esecutori che rivestono la qualifica di Persone Politicamente Esposte (PEPs);
- clienti legati ad una persona politicamente esposta (PEP) per via della titolarità effettiva congiunta di enti giuridici, essendo essi qualificabili come soggetti con i quali la persona politicamente esposta intrattiene notoriamente stretti legami;
- clienti che intrattengono con la PEP legami o relazioni d'affari senza tuttavia averne lo status (es. co-titolari di conto);
- cliente e/o esecutore e/o titolare effettivo residenti o aventi sede in Paesi terzi ad alto rischio;
- rapporti ed operazioni occasionali che coinvolgono Paesi terzi ad alto rischio nei casi indicati dall'art. 24, c. 5, lett. a), del Decreto;
- clienti che svolgono un'attività economica in uno dei seguenti settori a rischio[11]:
    - compro oro;
    - società fiduciarie;
    - gioco e scommesse.
- clienti beneficiari dell'erogazione di fondi pubblici (anche di origine comunitaria);
- trust[12] e strutture qualificabili come veicoli di interposizione patrimoniale;
- clienti partecipati da società fiduciarie e da trust;
- intermediari bancari o finanziari corrispondenti con sede in un Paese terzo;
- quando vi sia sospetto di riciclaggio o finanziamento del terrorismo, valutando contestualmente l'opportunità di attivare l'iter per la segnalazione delle operazioni sospette;
- quando con riferimento al cliente - e ai soggetti ad esso collegati - o all'eventuale titolare effettivo sia stata inoltrata una segnalazione di operazione sospetta;
- in relazione al ricorso a prodotti, operazioni, tecnologie che possano aumentare il rischio di riciclaggio o di finanziamento del terrorismo;
- in relazione a indici reputazionali negativi rilevanti ai fini antiriciclaggio. Rileva, tra l'altro, la sussistenza di procedimenti penali, quando questa informazione è notoria o comunque nota e non coperta da obblighi di segretezza che ne impediscono l'utilizzo ai sensi del codice di procedura penale;
- in relazione ad operazioni di versamento di contante o valori provenienti dall'estero di importo complessivo pari o superiore a 10.000 euro;
- in relazione all'utilizzo nei versamenti/prelevamenti di tagli di banconote da 200 e/o 500 euro per importi unitari pari o superiori a 2.500 euro (seppur tale soglia non sia più espressamente prevista dalla normativa in vigore).

[11] Sul punto, si specifica che il sistema di profilatura in uso assegna la fascia di rischio alta in presenza dei seguenti codici ATECO: 24.41, 26.52, 32.12, 46.48, 47.77, 95.25; 92.00, 93.29; 64.30, 66.19.

[12] In tal caso andrà acquisita copia dell'ultima versione dell'atto istitutivo, al fine di raccogliere e monitorare nel continuo le informazioni in merito alle finalità in concreto perseguite, all'identità del fondatore, del guardiano, dei beneficiari e del trustee, alle modalità di esecuzione del trust e a ogni altra caratteristica del medesimo.

4.2.2.1 PERSONE POLITICAMENTE ESPOSTE

L'utilizzo di fondi ottenuti illecitamente da soggetti che ricoprono - o hanno ricoperto in passato - cariche pubbliche 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, l'eventuale titolare effettivo ed il legale rappresentante / esecutore rientrino 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 l'eventuale presenza, tra la clientela, di nominativi inclusi nelle liste fornite da appositi *provider* esterni[13]. 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, del legale rappresentante / esecutore 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[14]; 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; il soggetto che autorizza decide altresì in merito all'eventuale perdita dello status di PEP e al conseguente abbassamento del profilo di rischio con applicazione di misure ordinarie di adeguata verifica[15].

Ai soggetti qualificati come Persone Politicamente Esposte viene attribuito il profilo di rischio più alto dal sistema di profilatura in uso.

4.2.2.2 RAPPORTI DI CORRISPONDENZA TRANSFRONTALIERI CON INTERMEDIARI BANCARI O FINANZIARI CORRISPONDENTI DI UN PAESE TERZO

Per rapporti di corrispondenza si intendono 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. Non sono incluse le operazioni una tantum o il semplice scambio di chiavi *Swift*. Per conti di passaggio si intendono i rapporti bancari di corrispondenza transfrontalieri, intrattenuti tra intermediari finanziari, utilizzati per effettuare operazioni in nome proprio e per conto della clientela.

In base all'approccio basato sul rischio, le misure di adeguata verifica rafforzata applicate nei confronti dell'intermediario corrispondente con sede in un Paese terzo con cui si instauri un conto corrente di

[13] Le liste ad oggi utilizzate sono le *World-Check* fornite da *Thomson Reuters*. La Funzione Antiriciclaggio si adopera affinché le procedure informatiche dedicate a tali controlli utilizzino liste costantemente aggiornate.

[14] La raccolta di informazioni deve consentire di acquisire un apprezzabile grado di certezza che i fondi impiegati non siano frutto di reati di natura corruttiva o di altre fattispecie criminose.

[15] 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.

corrispondenza transfrontaliero sono modulate, ponendo particolare attenzione, nella valutazione del rischio, al Paese terzo in cui l'ente è insediato.

Prima di avviare un rapporto continuativo con un Ente Corrispondente di un Paese Terzo, per tale intendendosi i Paesi extracomunitari, la banca dovrà:

- accertarsi che l'ente corrispondente (corrispondente diretto) non sia una Banca di comodo o un intermediario che consenta l'accesso ai conti correnti di corrispondenza con banche di comodo;
- formalizzare con il corrispondente un accordo scritto recante i termini, gli obblighi, le attività e le responsabilità antiriciclaggio che le parti si impegnano reciprocamente a rispettare;
- acquisire ulteriori informazioni sul corrispondente, 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;
- valutare 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;
- autorizzare, per mano del Direttore Generale, l'apertura di ogni conto di corrispondenza;
- attivare un controllo costante del rapporto, graduandone la frequenza e l'intensità sulla base del servizio di corrispondenza svolto.

Nel caso in cui i conti di corrispondenza siano accessibili indirettamente anche ad altri intermediari (corrispondenti indiretti), la Banca, in conformità con le disposizioni normative in materia, è chiamata a:

- verificare l'esistenza di tali rapporti e valutare il sistema dei controlli posti in essere dall'ente corrispondente diretto;
- acquisire informazioni sull'area geografica di operatività dei corrispondenti indiretti.

4.2.2.3 CLIENTELA RESIDENTE IN UN PAESE TERZO AD ALTO RISCHIO

La Banca applica misure rafforzate di adeguata verifica quando il cliente e/o il titolare effettivo e/o esecutore siano residenti o abbiano sede in Paesi terzi ad alto rischio.

E' 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.

4.2.3 ESECUZIONE DA PARTE DI TERZI DEGLI OBBLIGHI DI ADEGUATA VERIFICA

La Banca può demandare, in tutto o in parte, l'assolvimento degli obblighi di adeguata verifica della clientela a soggetti terzi – ad eccezione del controllo costante – purché essi rientrino tra gli intermediari elencati all'art. 26, comma 2, del Decreto e ferma la propria piena responsabilità per l'osservanza di detti obblighi (a tale scopo, la Banca ha predisposto uno specifico Modello di Attestazione). 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 reca:

- 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 – da parte di intermediari terzi soggetti alla disciplina antiriciclaggio, sui quali ricade la piena responsabilità per l'osservanza degli obblighi di adeguata verifica della clientela.

4.2.4 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.

4.3 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 sospettati o responsabili di attività terroristiche.

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 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* (es. esecutori, ordinanti, beneficiari) e confermati come tali;
- applica 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.

4.4 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 non incorra, nell'ambito delle proprie attività istituzionali, in violazioni della normativa in materia di embarghi, la stessa promuove l'adozione di misure che assicurino:

- controlli anagrafici e sulle operazioni;
- controlli da effettuarsi 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 finanziare 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.

4.5 PRESIDI IN MATERIA DI TRASFERIMENTO DI FONDI

La Banca, in qualità di prestatore 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 determina, 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.

4.6 LIMITAZIONI ALL'USO DEL CONTANTE E DEI TITOLI AL PORTATORE

La Banca 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.

4.7 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 continua ad avvalersi 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 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 del sistema informatico in uso che permette un accesso diretto e immediato.

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

Infine, la Banca obbligata ai sensi delle disposizioni antiriciclaggio applica gli obblighi di conservazione dei dati e delle informazioni conformemente alle citate disposizioni delle Autorità di Vigilanza in materia di conservazione dei dati (consultazione chiusa).

4.8 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 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, come da *Regolamento per la segnalazione delle operazioni sospette di riciclaggio e di finanziamento del terrorismo* cui si rimanda.

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 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.

4.9 METODOLOGIA DI VALUTAZIONE DEL RISCHIO

L'identificazione e la valutazione periodica del rischio inerente e delle correlate vulnerabilità costituisce il primo momento logico del modello di gestione del rischio e risulta funzionale 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*) e 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, destinataria delle disposizioni delle Autorità di vigilanza di settore, conduce un'autovalutazione del rischio di riciclaggio cui è esposta con cadenza annuale, secondo i criteri e la metodologia fornita dalle medesime Autorità di vigilanza di settore e descritte nelle rispettive relazioni annuali.

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 dipendenti e dei collaboratori.

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

La funzione antiriciclaggio della Banca 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.

4.11 SISTEMA INTERNO DI SEGNALAZIONE DELLE VIOLAZIONI

Al fine di garantire la conformità alle disposizioni normative vigenti, la Banca è dotata 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.

5. FLUSSI INFORMATIVI

Il sistema dei flussi è costituito sia da flussi informativi derivanti da attività con periodicità definita sia da informative prodotte all'occorrenza che possono essere predisposte anche in maniera non strutturata (rientrano in tale categoria anche gli incontri, le condivisioni e le comunicazioni interne di natura informativa).

Gli obiettivi perseguiti mediante un adeguato sistema di flussi sono almeno i seguenti:

- assicurare agli Organi aziendali e alle diverse Funzioni di disporre delle informazioni necessarie allo svolgimento effettivo e consapevole dei compiti loro affidati;
- garantire una valorizzazione piena dei diversi livelli di responsabilità all'interno dell'organizzazione, atta ad assicurare il corretto funzionamento della struttura e, più in generale, efficienza nella gestione ed efficacia nei controlli.

I flussi informativi identificati sono indicati nell'ambito del *Regolamento dei flussi informativi* cui si rimanda.