



## **Regolamento del processo di Segnalazione Operazioni Sospette (SOS)**

<b>1</b>	<b>PREMESSA .....</b>	<b>3</b>
1.1	AMBITO DI APPLICAZIONE.....	3
1.2	RESPONSABILITA' DEL DOCUMENTO .....	4
1.3	OBIETTIVI DEL DOCUMENTO .....	4
1.4	STRUTTURA DEL DOCUMENTO.....	5
<b>2</b>	<b>LE POLICY DI RIFERIMENTO E AMBITO DI APPLICAZIONE .....</b>	<b>6</b>
<b>3</b>	<b>GLI ATTORI COINVOLTI.....</b>	<b>6</b>
3.1	RESPONSABILE ANTIRICICLAGGIO E DELEGATO ALLA SEGNALAZIONE DI OPERAZIONI SOSPETTE.....	7
3.2	PRIMO LIVELLO SEGNALETICO.....	9
3.3	STRUTTURE AZIENDALI DI BANCAMEDIO LANUM S.P.A. ....	11
3.3	ATTORI ESTERNI .....	11
<b>4</b>	<b>GLOSSARIO .....</b>	<b>15</b>
4.1	BANCHE DATI .....	16
<b>5</b>	<b>IL PROCESSO DELLE SEGNALAZIONI DELLE OPERAZIONI SOSPETTE .....</b>	<b>17</b>
5.1	AVVIO DEL PROCESSO SEGNALETICO .....	17
5.2	ASSEGNAZIONE DELLA PRATICA .....	25
5.3	ISTRUZIONE DELLA PRATICA .....	25
5.4	TRASMISSIONE DELLA PRATICA IN VALUTAZIONE .....	26
5.5	VALUTAZIONE DELLE OPERAZIONI SOSPETTE.....	27
5.6	SEGNALAZIONE DELL'OPERAZIONE .....	29
5.7	ANALISI UIF .....	30
5.8	ARCHIVIAZIONE DELLA PRATICA E MONITORAGGIO .....	31
5.9	RISERVATEZZA E CONSERVAZIONE DELLE SEGNALAZIONI .....	32
<b>6</b>	<b>INTERRELAZIONE CON ALTRE UNITA' ORGANIZZATIVE .....</b>	<b>32</b>
7.1	FLUSSI VERSO LA FUNZIONE ANTIRICICLAGGIO .....	33

7.2 FLUSSI INFORMATIVI IN USCITA.....	35
<b>8 LA NORMATIVA ESTERNA DI RIFERIMENTO .....</b>	<b>36</b>
<b>9 LE POLICY E LA NORMATIVA INTERNA DI RIFERIMENTO .....</b>	<b>38</b>

## 1 PREMESSA

Il presente Regolamento, illustra i principi guida, l'architettura organizzativa e le interdipendenze alla base del processo di "Segnalazione delle operazioni sospette".

La segnalazione delle operazioni sospette all'Unità di Informazione Finanziaria della Banca d'Italia costituisce uno dei pilastri fondamentali della normativa in materia di antiriciclaggio e contrasto al finanziamento del terrorismo, rappresentando una delle più importanti declinazioni del principio di "collaborazione attiva" cui sono chiamati i destinatari delle disposizioni del D. Lgs. Del 21 novembre 2007, n. 231 e s.m.i..

In particolare, gli obblighi di segnalazione delle operazioni sospette sono regolamentati dal Capo III – Obblighi di segnalazione - dell'art. 35 del D. Lgs. 231/2007. Ai sensi del predetto articolo, i soggetti destinatari della disciplina *"prima di compiere l'operazione, inviano senza ritardo alla UIF, una segnalazione di operazione sospetta quando sanno, sospettano o hanno 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 da attività criminosa."*

Il sospetto è desunto dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento o frazionamento o da qualsivoglia altra circostanza conosciuta, in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi a disposizione dei segnalanti, acquisiti nell'ambito dell'attività svolta ovvero a seguito del conferimento di un incarico. È un elemento di sospetto, ad esempio, il ricorso frequente o ingiustificato ad operazioni in contante, anche se non eccedenti la soglia di cui all'articolo 49 e, in particolare, il prelievo o il versamento in contante di importi non coerenti con il profilo di rischio del cliente.

La segnalazione di una operazione sospetta è il risultato, pertanto, di un complesso processo di valutazione, basato su elementi:

- oggettivi, quali le caratteristiche, l'entità e la natura dell'operazione;
- soggettivi, quali le caratteristiche personali, la capacità reddituale e l'attività economica esercitata.

I dipendenti cui compete, nel concreto, l'amministrazione e la gestione dei rapporti con la clientela hanno l'obbligo di comunicare, senza ritardo, le operazioni sospette al Delegato Antiriciclaggio, secondo le istruzioni contenute nel presente Regolamento.

### 1.1 AMBITO DI APPLICAZIONE

Il presente documento è approvato dal Consiglio di Amministrazione della Società, ed è rivolto a tutti i dipendenti e collaboratori della stessa.

Il presente Regolamento garantisce altresì il recepimento delle linee guida e dei principi contenuti nella Policy al fine di favorire un adeguato coordinamento tra i presidi antiriciclaggio locali e la Funzione Antiriciclaggio e ad assicurare una efficace circolazione delle informazioni a livello di Gruppo, al fine di contrastare il rischio di riciclaggio e finanziamento del terrorismo.

## **1.2 RESPONSABILITA' DEL DOCUMENTO**

---

Il Regolamento è approvato dal Consiglio di Amministrazione della Società, che approverà altresì eventuali modifiche e/o aggiornamenti della stessa.

La Funzione Antiriciclaggio concorre all'aggiornamento e alla revisione periodica del presente Regolamento, secondo quanto disposto dalla vigente policy sulla redazione della normativa interna. Il Responsabile Antiriciclaggio della Società sottopone al Consiglio di Amministrazione le proposte di aggiornamento e/o revisione del presente Regolamento per le valutazioni di competenza.

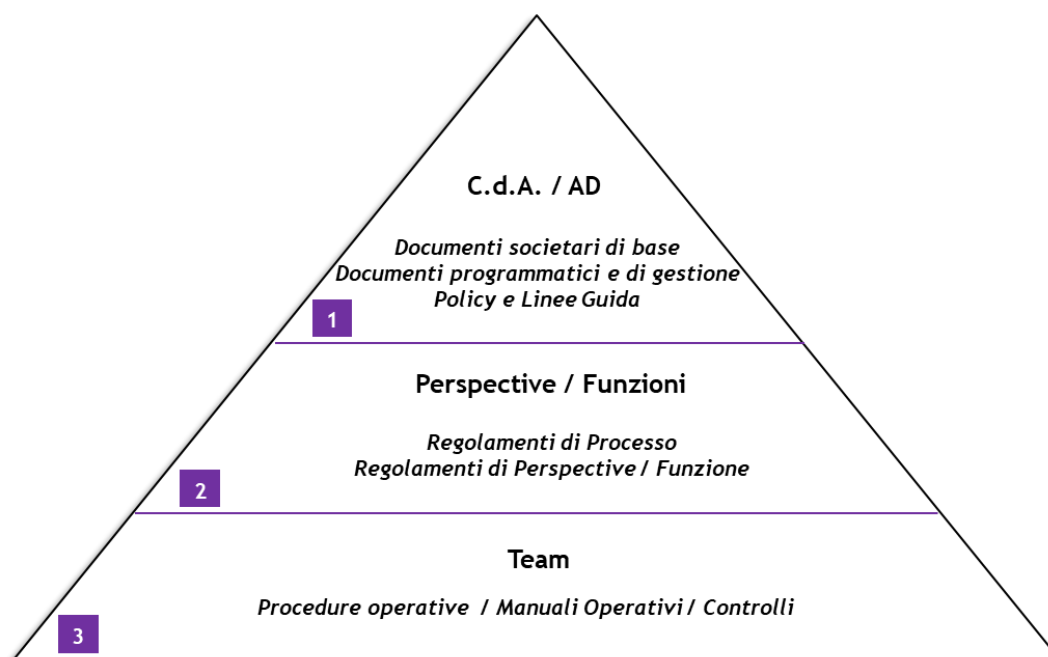
## **1.3 OBIETTIVI DEL DOCUMENTO**

---

Il presente documento, in applicazione della *policy* sul contrasto al riciclaggio e al finanziamento al terrorismo adottata dalla Società, ha l'obiettivo di:

- descrivere le fasi dei processi interni propedeutici alla segnalazione di operazioni sospette da parte del primo livello segnaletico cui compete la gestione concreta dei rapporti con la clientela, della Funzione Antiriciclaggio e del Delegato alla segnalazione di operazioni sospette;
- richiamare ruoli e responsabilità degli attori coinvolti nel processo, in relazione all'assetto organizzativo disciplinato dall'Ordinamento dei Servizi della Società;
- descrivere i principali output dal processo, la tempistica di produzione e i destinatari;
- descrivere le interrelazioni tra le diverse Unità Organizzative coinvolte nel processo, gli strumenti e i Flussi informativi.

Con riferimento alla *"Policy sulle modalità di redazione, approvazione, diffusione ed aggiornamento della normativa interna"*, il presente documento si colloca quindi al secondo livello della piramide documentale richiamata nello schema seguente.



## 1.4 STRUTTURA DEL DOCUMENTO

Il Regolamento si compone complessivamente di sette capitoli oltre al presente. Di seguito, sono descritte sinteticamente le principali tematiche trattate in ogni capitolo:

### **Capitolo 2: La policy di riferimento**

Obiettivo del Capitolo è richiamare i principi della Policy di riferimento.

### **Capitolo 3: Gli attori coinvolti**

Obiettivo del Capitolo è descrivere e richiamare in modo chiaro ruolo e responsabilità degli attori coinvolti nel processo oggetto del presente documento, definendo modalità di integrazione e coordinamento previste nei casi di processo di carattere interfunzionale.

### **Capitolo 4: Il glossario**

Obiettivo del Capitolo è richiamare le principali definizioni di riferimento.

### **Capitolo 5: Il processo**

Obiettivo del Capitolo è descrivere gli aspetti di carattere organizzativo il processo e modalità di interazione con altre entità organizzative o di società terze, interne o esterne al Gruppo Mediolanum, in relazione al processo oggetto di regolamentazione, gli strumenti utilizzati e gli output attesi dalle fasi in cui il processo è articolato.

### **Capitolo 6: Interrelazioni con le unità organizzative**

Descrive le unità organizzative che interagiscono nel processo riportando i flussi informativi in entrata e in uscita.

## Capitolo 7: La normativa esterna di riferimento

Si richiama il contesto normativo nel quale opera il presente Regolamento di processo.

## Capitolo 8: Le policy e la normativa interna di riferimento

Si riepilogano le fonti informative interne alla Banca che presentano relazioni con il processo in esame.

### 2 LE POLICY DI RIFERIMENTO E AMBITO DI APPLICAZIONE

Flowe SB S.p.A. ha adottato un'apposita *policy* per il contrasto al riciclaggio e al finanziamento del terrorismo, in applicazione di quanto disposto dal Decreto Antiriciclaggio e in linea con le Disposizioni su Organizzazione, Procedure e Controlli in materia antiriciclaggio emanate dalla Banca d'Italia.

La policy antiriciclaggio trova la sua principale declinazione nel presente Regolamento, nel Regolamento del processo di "Adeguata Verifica" e nel Regolamento dei Controlli, che insieme contengono le regole e le procedure che devono essere adottate dai dipendenti e dai collaboratori della Società per l'assolvimento degli obblighi in materia di antiriciclaggio e contrasto al finanziamento del terrorismo.

### 3 GLI ATTORI COINVOLTI

In coerenza con quanto previsto dalle Disposizioni su Organizzazione, Procedure e Controlli in materia antiriciclaggio emanate dalla Banca d'Italia, i compiti e le responsabilità in materia di mitigazione del rischio di coinvolgimento della Società in fatti di riciclaggio o di finanziamento al terrorismo sono rimessi in *primis* agli Organi aziendali.

In particolare, spetta al Consiglio di Amministrazione individuare politiche di governo di detti rischi adeguate all'entità e alla tipologia dei profili di rischio cui è concretamente esposta l'attività della Società. L'Amministratore Delegato appronta le procedure necessarie per dare attuazione a tali politiche; la Funzione Antiriciclaggio ne verifica, nel continuo, l'idoneità al fine di assicurare un adeguato presidio dei citati rischi, coordinandosi con le altre Funzioni Aziendali di Controllo.

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

Un'efficace attività di prevenzione dei rischi non può, in ogni caso, essere demandata alle sole funzioni di controllo, ma deve svolgersi, in primo luogo, dove il rischio viene generato, in particolare nell'ambito delle linee operative, le quali sono le prime responsabili del processo di gestione dei rischi, nonché, nel caso in cui alle stesse sia affidata, nel concreto,

la gestione e amministrazione dei rapporti con la clientela costituiscono il primo livello segnalato.

I processi descritti nel presente Regolamento prevedono il coinvolgimento degli Organi e delle strutture aziendali della Società., rinviando all'Ordinamento dei Servizi della stessa ed ai Regolamenti di Funzione delle singole strutture interessate per una compiuta descrizione delle attività svolte, secondo l'articolazione di ruoli e responsabilità riportati nella *"Policy sul contrasto al riciclaggio e al finanziamento del terrorismo"* vigente.

### **3.1 RESPONSABILE ANTIRICICLAGGIO E DELEGATO ALLA SEGNALEZIONE DI OPERAZIONI SOSPETTE**

Il Responsabile della Funzione Antiriciclaggio (di seguito anche Responsabile Antiriciclaggio) è nominato dal Consiglio di Amministrazione, sentito il Collegio Sindacale. Il Responsabile della Funzione:

- 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;
- è indipendente nell'esecuzione delle sue funzioni;
- è collocato in posizione gerarchico-funzionale adeguata;
- accede direttamente agli Organi aziendali e comunica con essi senza restrizioni o intermediazioni;
- non deve avere responsabilità dirette di aree operative né deve essere gerarchicamente dipendente da soggetti responsabili di dette aree; in generale, non deve essere gerarchicamente subordinato ai responsabili delle funzioni sottoposte a controllo;
- ha accesso a tutti i necessari documenti aziendali per potere adempiere ai propri compiti previsti dalla regolamentazione di Vigilanza;
- verifica l'adeguatezza dei processi e delle procedure interne in materia di rilevazione, valutazione e segnalazione delle operazioni sospette, nell'ambito delle sue responsabilità di monitoraggio dell'efficacia di tutto il sistema di gestione e dei controlli interni a presidio del rischio di riciclaggio e di finanziamento del terrorismo.

Il Responsabile della Funzione Antiriciclaggio, con delibera del Consiglio di Amministrazione, è stato nominato anche Delegato all'invio delle segnalazioni, ai sensi dell'art. 35 del D. Lgs. 231/2007. Il Delegato alla Segnalazione delle Operazioni Sospette:

- ha libero accesso ai flussi informativi diretti agli Organi Aziendali e alle strutture coinvolte nel contrasto del riciclaggio e del finanziamento del terrorismo;
- può acquisire ogni informazione utile dalla struttura che svolge il primo livello di analisi;
- può consentire, con le indispensabili cautele di riservatezza e senza far menzione del nominativo del segnalante, che i Responsabili delle strutture aziendali abbiano conoscenza dei nominativi dei clienti segnalati, anche attraverso l'utilizzo di idonee basi informative, stante la particolare pregnanza che tale informazione può rivestire per



l'accettazione di nuovi clienti ovvero per la valutazione dell'operatività di clienti preesistenti;

- gestisce, per quanto di competenza, i rapporti con l'UIF e corrisponde tempestivamente alle eventuali richieste di approfondimento provenienti dalla medesima;
- presta consulenza alle strutture operative in merito alle procedure da adottare per la segnalazione di eventuali operazioni sospette ed all'eventuale astensione dal compimento delle operazioni;
- valuta, alla luce di tutti gli elementi disponibili, le operazioni sospette comunicate dal responsabile dell'unità organizzativa o della struttura competente alla gestione concreta dei rapporti con la clientela (cd. primo livello segnaletico), ovvero di cui sia altrimenti venuto a conoscenza nell'ambito della propria attività;
- effettua verifiche, anche a campione, sulla congruità delle valutazioni effettuate dal primo livello sull'operatività della clientela;
- assicura la trasmissione all'UIF delle segnalazioni ritenute fondate, omettendo l'indicazione dei nominativi dei soggetti coinvolti nella procedura di segnalazione dell'operazione;
- archivia, con propria motivazione scritta, le segnalazioni ritenute non fondate;
- comunica l'archiviazione delle segnalazioni che ha ritenuto non fondate al soggetto segnalante;
- valuta discrezionalmente se, a fronte delle segnalazioni di operazioni sospette pervenutegli, innalzare o diminuire il profilo di rischio dei soggetti correlati all'operatività analizzata, indipendentemente dall'esito conclusivo delle stesse, tenendo traccia delle motivazioni sottostanti;
- contribuisce all'individuazione delle misure necessarie a garantire la riservatezza e la conservazione dei dati, delle informazioni e della documentazione relativa alle segnalazioni.

Il Delegato abilita gli addetti della Funzione Antiriciclaggio ad operare, sotto la propria responsabilità, (1) nel sistema di segnalazione delle operazioni sospette (Infostat-UIF), secondo le disposizioni impartite dall'UIF, (2) nel sistema di profilatura del rischio al fine di dare seguito operativamente all'aumento/diminuzione del profilo dei soggetti analizzati deciso dallo stesso, (3)<sup>1</sup> nel sistema GE.SA.FIN. di richieste preventive di autorizzazione per operazioni/pagamenti sui documenti rappresentativi di merci in caso di paesi soggetti ad embargo / sanzionati / aventi restrizioni e/o nel sistema S.I.G.M.A. per operazioni/pagamenti avente per oggetto materiali d'armamento, nonché abilita gli addetti della Funzione Antiriciclaggio ad operare, sempre sotto la propria responsabilità, nel sistema di gestione delle segnalazioni aggregate (S.AR.A.).

---

<sup>1</sup> GEstione SANzioni FINanziarie e Sistema Informatico Gestione Materiali Armamenti tramite accesso al sito del MEF: <https://portaletesoro.mef.gov.it/>

## 3.2 PRIMO LIVELLO SEGNALETICO

---

### 3.2.1 STRUTTURE OPERATIVE

Le Strutture Operative sono le prime responsabili del processo di gestione dei rischi. Nel corso dell'operatività giornaliera tali strutture sono chiamate, infatti, ad identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale, in conformità con il processo di gestione dei rischi. Inoltre, tali strutture devono rispettare i limiti operativi loro assegnati, coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi.

Tutti i dipendenti ed i collaboratori delle Strutture Operative, nell'ambito delle mansioni a cui sono assegnati, sono tenuti a conoscere e uniformarsi alle leggi, ai regolamenti ed alle norme emanate dalla Società. I documenti aziendali che disciplinano aspetti organizzativi e comportamentali afferenti il rispetto delle norme vigenti, sia di legge sia definite internamente dalla Banca, sono portati a conoscenza di tutti i dipendenti e dei collaboratori attraverso la loro pubblicazione e diffusione secondo le modalità previste dalla normativa interna. In tale ambito, rivestono particolare importanza i piani di formazione e di aggiornamento professionale predisposti dalla Direzione Risorse Umane di Banca Mediolanum in collaborazione con la Funzione Antiriciclaggio, al fine di assicurare la piena consapevolezza delle finalità della normativa, dei suoi principi, degli obblighi e delle responsabilità aziendali.

Allorché dipendenti e collaboratori, nell'espletamento delle proprie attività, rilevino che i processi operativi non siano aderenti alle norme di riferimento o i presidi adottati non siano efficaci al fine di prevenire il coinvolgimento, anche inconsapevole, della Società o delle società del Gruppo in operazioni di riciclaggio o finanziamento del terrorismo devono darne tempestiva comunicazione al proprio responsabile.

Nel caso in cui alle Strutture Operative sia assegnata l'amministrazione e la gestione concreta dei rapporti con la clientela, alle medesime compete il processo di identificazione e di adeguata verifica della clientela loro assegnata quale primo livello di controllo, sviluppando la conoscenza della medesima ed assicurando un monitoraggio continuo nel corso del rapporto, in funzione del rischio sotteso. Ad esse compete, inoltre, lo svolgimento del processo di adeguata verifica rafforzata nei casi previsti dalla normativa e laddove richiesto dalla Funzione Antiriciclaggio, nonché l'onere di segnalare tempestivamente, ove possibile prima di compiere l'operazione, eventuali operazioni sospette, secondo le procedure e le modalità definite internamente, allorché sappiano sospettino o abbiano ragionevoli motivi di sospettare che sia stata compiuta, sia in corso o sia tentata un'operazione di riciclaggio o finanziamento del terrorismo.

Ogni Responsabile di Struttura è tenuto a curare al meglio la gestione del personale e degli strumenti operativi allo stesso affidati per assicurare il costante perseguimento degli obiettivi aziendali e deve, per quanto di competenza, osservare e far rispettare scrupolosamente tutte le norme vigenti, sia di legge sia interne. A ciascun Responsabile, è attribuita, inoltre, la responsabilità complessiva della conformità e dell'efficace funzionamento dei presidi di primo livello all'interno della propria struttura.

Allorché i Responsabili, nell'espletamento delle proprie funzioni, rilevino che i processi operativi non siano aderenti alle norme di riferimento o i presidi adottati non siano efficaci al fine di prevenire il coinvolgimento, anche inconsapevole, della Società o delle società del Gruppo in operazioni di riciclaggio o finanziamento del terrorismo devono, previ i necessari approfondimenti, interessare senza ritardi la Funzione Antiriciclaggio per le valutazioni di competenza.

A tal riguardo, la Società fornisce, ai propri dipendenti e collaboratori, strumenti operativi e procedure, anche informatiche, in grado di assisterli nei relativi adempimenti ai fini antiriciclaggio e appronta specifici programmi di formazione e aggiornamento professionale permanenti a favore di quest'ultimi, affinché abbiano adeguata conoscenza della normativa di riferimento e delle connesse responsabilità e siano in grado di utilizzare consapevolmente strumenti e procedure di ausilio nell'esecuzione degli adempimenti.

Nell'ambito delle Strutture Operative della Società, assume particolare rilevanza, l'Unità Banking Services & Controls.

#### 3.2.1.1 *Unità Banking Services & Controls*

L'Unità Banking Services & Controls costituisce il primo livello del processo di gestione dei rischi. Nel corso dell'operatività giornaliera tale struttura è chiamata, infatti, ad identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi. Inoltre, la struttura deve rispettare i limiti operativi assegnati coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi.

Tutti i dipendenti ed i collaboratori – anche *outsourcers* - dell'Unità, nell'ambito delle mansioni a cui sono assegnati, sono tenuti a conoscere e uniformarsi alle leggi, ai regolamenti ed alle norme emanate dalla Società. I documenti aziendali che disciplinano aspetti organizzativi e comportamentali afferenti il rispetto delle norme vigenti, sia di legge sia definite internamente dalla Società, sono portati a conoscenza di tutti i dipendenti e dei collaboratori attraverso la loro pubblicazione e diffusione secondo le modalità previste da dalla Società stessa.

Allorché dipendenti e collaboratori, nell'espletamento delle proprie attività, rilevino che i processi operativi non siano aderenti alle norme di riferimento o i presidi adottati non siano efficaci al fine di prevenire il coinvolgimento, anche inconsapevole, della Società operazioni

di riciclaggio o finanziamento del terrorismo devono darne tempestiva comunicazione al proprio responsabile.

Fornisce supporto ai soggetti titolari di poteri di amministrazione o direzione ovvero i loro delegati, al fine della valutazione e conseguente decisione sull'autorizzazione all'instaurazione, al mantenimento e/o all'interruzione del/i rapporto/i con i clienti / prospect qualificati come PEP e/o residenti in paesi definiti ad alto rischio, e/o per le operazioni eseguite dalla clientela su detti paesi ad alto rischio.

In particolare il Team AML ed il Team Account Monitoring, dell'Unità Banking Services & Controls procedono, per competenza, ad analizzare e monitorare giornalmente il transato dei clienti attraverso diversi INPUT (alert su sistemi automatici di rilevazione potenziali operazioni anomale/sospette, richieste dell'A.G., segnalazione interna, evidenza ecc.). Procedo ad analizzare il conto del cliente attenzionato attendendosi ad alcuni parametri, ad es:

1. Conformità del reddito dichiarato con la movimentazione;
2. Provenienza dei fondi;
3. Coerenza con lo storico del cliente;

Se in seguito alle analisi si ritiene necessario chiedere informazioni al cliente si procede con l'invio di Adeguata Verifica Rafforzata.

Successivamente in caso di mancato riscontro o riscontro ritenuto insufficiente o poco chiaro si procede con la richiesta di invio SOS.

### **3.3 STRUTTURE AZIENDALI DI BANCAMEDIOLANUM S.P.A.**

---

In relazione alle attività disciplinate all'interno del contratto di appalto per la fornitura di servizi di gestione aziendale (accordo di servizio) – con riferimento alle attività inerenti il processo in questione, la società Flowe si avvale della struttura dell'Unità Conformità ed Analisi AML della Funzione Antiriciclaggio di Banca Mediolanum S.p.A., per quanto attiene la lavorazione e gestione delle segnalazioni di operazioni sospette, ivi compreso l'archiviazione delle pratiche e l'invio delle segnalazioni tramite abilitazione al portale Infostat-UIF.

### **3.3 ATTORI ESTERNI**

---

Di seguito, sono descritti i ruoli e le responsabilità degli attori esterni che partecipano al processo.

#### **3.3.1 CSF**

Il Comitato di Sicurezza Finanziaria (CSF) è l'Autorità competente responsabile di monitorare, in Italia, il funzionamento del sistema di prevenzione e di sanzioni del finanziamento del terrorismo e del riciclaggio; esso è presieduto dal Direttore generale del Tesoro e composto da rappresentanti del Ministero dell'Economia e delle Finanze, del Ministero degli Affari Esteri, del Ministero dell'Interno, del Ministero della Giustizia, della Banca d'Italia, della Commissione Nazionale per le Società e la Borsa, dell'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo, dell'Unità di Informazione Finanziaria, della Guardia di Finanza, della Direzione Investigativa Antimafia, dell'Arma dei Carabinieri e della Direzione nazionale antimafia.

Ai fini dello svolgimento dei compiti riguardanti il congelamento delle risorse economiche, il CSF è integrato dall'Agenzia del demanio.

Ai fini della lotta alla proliferazione delle armi di distruzione di massa, il CSF è integrato dal Ministero dello Sviluppo Economico e dall'Agenzia delle Dogane.

Nell'ambito dei processi descritti nel presente Regolamento, nel caso di richiesta autorizzazione preventiva formale di una disposizione avente ad oggetto soggetti e/o merci in ambito restrizioni/embarghi, fornisce conferma (o diniego) a procedere con la stessa.

### 3.3.2 MEF

Il Ministero dell'Economia e delle Finanze (MEF) è responsabile delle politiche di prevenzione dell'utilizzo del sistema finanziario e di quello economico per fini di riciclaggio dei proventi di attività criminose e o finanziamento del terrorismo. In tali materie, promuove la collaborazione tra l'UIF, le Autorità di Vigilanza di Settore, gli ordini professionali, la DIA e la Guardia di Finanza.

Il Ministero dell'Economia e delle Finanze provvede altresì all'irrogazione delle sanzioni per violazione degli obblighi di cui al decreto 231/2007 e s.m.i. nei confronti dei soggetti obbligati come indicato nell'art.65 del citato decreto.

Nell'ambito dei processi descritti nel presente Regolamento, riceve le comunicazioni sulle infrazioni ai limiti alla circolazione del contante e dei titoli al portatore, ai sensi dell'art. 51 del D. Lgs. 231/2007.

Sentito il Comitato di Sicurezza Finanziaria, individua, con proprio decreto, una lista di paesi in ragione di rischio di riciclaggio e di finanziamento di terrorismo ovvero della mancanza di un adeguato scambio di informazioni anche in materia fiscale.

### 3.3.3 NSPV e DIA

Il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza (NSPV) è costituito all'interno del Corpo della Guardia di Finanza ed opera in prima linea sul fronte della lotta al riciclaggio sia come organismo investigativo di polizia, sia come organo amministrativo di controllo del settore dell'intermediazione finanziaria, unitamente alla Banca d'Italia e alla DIA. Nell'espletamento della propria attività, si avvale dei poteri e delle facoltà che la legge riconosce ai suoi appartenenti con riferimento alla specifica disciplina valutaria, oltre che di quelli propri della materia fiscale. La DIA e il Nucleo Speciale di Polizia Valutaria della

Guardia di finanza svolgono approfondimenti investigativi delle segnalazioni trasmesse dalla UIF. Il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza effettua, inoltre, i controlli diretti a verificare l'osservanza degli obblighi previsti dal d. lgs. 231/2007 e dalle relative disposizioni attuative.

La Direzione Investigativa Antimafia (DIA) accerta e contesta, con le modalità e nei termini di cui alla legge 24 novembre 1981, n. 689, ovvero trasmette alle Autorità di vigilanza di settore le violazioni degli obblighi di cui al decreto antiriciclaggio riscontrate nell'esercizio delle sue attribuzioni ed effettua approfondimenti investigativi, attinenti alla criminalità organizzata, delle segnalazioni di operazioni sospette trasmesse dalla UIF.

### 3.3.4 UIF

La UIF riceve e acquisisce informazioni riguardanti ipotesi di riciclaggio e di finanziamento del terrorismo, ne effettua l'analisi finanziaria e, su tali basi, ne valuta la rilevanza ai fini della trasmissione agli organi investigativi (Nucleo speciale di polizia valutaria della Guardia di Finanza -NSPV e Direzione investigativa antimafia-DIA) e della collaborazione con l'Autorità Giudiziaria.

L'Unità di Informazione Finanziaria per l'Italia (UIF), presso la Banca d'Italia, esercita le proprie funzioni in piena autonomia e indipendenza. In attuazione di tali principi, la Banca d'Italia disciplina con un regolamento l'organizzazione e il funzionamento della UIF, ivi compresa la riservatezza delle informazioni acquisite. La Banca d'Italia attribuisce alla UIF mezzi finanziari e risorse idonei ad assicurare l'efficace perseguimento dei suoi fini istituzionali. In particolare, la UIF esercita le seguenti funzioni:

- a) riceve le segnalazioni di operazioni sospette e ne effettua l'analisi finanziaria;
- b) analizza i flussi finanziari, al fine di individuare e prevenire fenomeni di riciclaggio di denaro e di finanziamento del terrorismo;
- c) può sospendere, per un massimo di cinque giorni lavorativi, operazioni sospette, anche su richiesta del Nucleo speciale di polizia valutaria della Guardia di finanza, della Direzione investigativa antimafia e dell'Autorità giudiziaria ovvero su richiesta di un'altra FIU, ove non ne derivi pregiudizio per il corso delle indagini. La UIF provvede a dare immediata notizia della sospensione all'autorità che ne ha fatto richiesta;
- d) avuto riguardo alle caratteristiche dei soggetti obbligati, emana istruzioni, pubblicate nella Gazzetta Ufficiale della Repubblica italiana, sui dati e le informazioni che devono essere contenuti nelle segnalazioni di operazioni sospette e nelle comunicazioni oggettive, sulla relativa tempistica nonché sulle modalità di tutela della riservatezza dell'identità del segnalante;
- e) al fine di agevolare l'individuazione delle operazioni sospette, emana e aggiorna periodicamente, previa presentazione al Comitato di sicurezza finanziaria, indicatori di anomalia, pubblicati nella Gazzetta Ufficiale della Repubblica italiana e in apposita sezione del proprio sito istituzionale;

- f) effettua, anche attraverso ispezioni, verifiche al fine di accertare il rispetto delle disposizioni in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo, con riguardo alle segnalazioni di operazioni sospette e ai casi di omessa segnalazione di operazioni sospette, nonché con riguardo alle comunicazioni alla UIF previste dal presente decreto e ai casi di omissione delle medesime, anche avvalendosi della collaborazione del Nucleo speciale di polizia valutaria della Guardia di Finanza;
- g) in relazione ai propri compiti, accerta e contesta ovvero trasmette alle Autorità di vigilanza di settore le violazioni degli obblighi di cui al presente decreto di cui viene a conoscenza nell'esercizio delle proprie funzioni istituzionali;
- h) assicura la tempestiva trasmissione alla Direzione nazionale antimafia e antiterrorismo dei dati, delle informazioni e delle analisi, secondo quanto stabilito dall'articolo 8, comma 1, lettera a). Assicura, altresì, l'effettuazione delle analisi richieste dalla Direzione nazionale antimafia e antiterrorismo ai sensi dell'articolo 8, comma 1, lettera d).
- i) decide e divulga i parametri (criteri oggettivi) che definiscono le c.d. "Comunicazioni oggettive" che i soggetti obbligati saranno tenuti a trasmettere alla stessa Unità con cadenza periodica.

La UIF, avvalendosi delle informazioni raccolte nello svolgimento delle proprie attività:

- a) svolge analisi e studi su singole anomalie, riferibili a ipotesi di riciclaggio e di finanziamento del terrorismo su specifici settori dell'economia ritenuti a rischio, su categorie di strumenti di pagamento e su specifiche realtà economiche territoriali, anche sulla base dell'analisi nazionale dei rischi elaborata dal Comitato di sicurezza finanziaria;
- b) elabora e diffonde modelli e schemi rappresentativi di comportamenti anomali sul piano economico e finanziario riferibili a possibili attività di riciclaggio e di finanziamento del terrorismo.

### 3.3.5 AUTORITÀ DI VIGILANZA DI SETTORE

Le Autorità di vigilanza di settore verificano il rispetto, da parte dei soggetti rispettivamente vigilati, degli obblighi previsti dal presente decreto e dalle relative disposizioni di attuazione. A tal fine:

- a) adottano, nei confronti dei soggetti rispettivamente vigilati, disposizioni di attuazione del presente decreto in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela;
- b) verificano l'adeguatezza degli assetti organizzativi e procedurali dei soggetti obbligati rispettivamente vigilati;
- c) definiscono procedure e metodologie per la valutazione del rischio di riciclaggio e finanziamento, del terrorismo cui gli intermediari rispettivamente vigilati sono esposti nell'esercizio della propria attività;



- d) esercitano i poteri attribuiti dal d. lgs. 231/07, anche al fine di assicurare il rispetto delle norme tecniche di regolamentazione adottate ai sensi della Direttiva antiriciclaggio.

### 3.3.6 ALTRI INTERMEDIARI

Come già ribadito la segnalazione delle operazioni sospette all'Unità di Informazione Finanziaria della Banca d'Italia costituisce uno dei pilastri fondamentali della normativa in materia di antiriciclaggio e contrasto al finanziamento del terrorismo, rappresentando una delle più importanti declinazioni del principio di "collaborazione attiva" cui sono chiamati i destinatari delle disposizioni del D. Lgs. Del 21 novembre 2007, n. 231 e s.m.i..

In tal senso la Società ha convenuto specifici accordi sul tema in questione con altri intermediari destinatari delle disposizioni che operano come primo livello segnaletico in funzione di apposite convenzioni per servizi o accordi di distribuzione di prodotti con la Società stessa.

Flowe riceve, e comunica lei stessa, i nominativi dei clienti comuni segnalati da parte degli intermediari con cui la stessa opera (a titolo esemplificativo Mooney S.p.A.<sup>2</sup>), in ottemperanza ai limiti ed ai vincoli di riservatezza posti dalla normativa tempo per tempo vigente.

La Funzione Antiriciclaggio analizza pertanto le segnalazioni di possibili operazioni anomale ricevute da intermediari terzi con cui sono in essere accordi di distribuzione o collocamento di prodotti o servizi nell'ambito dei flussi di "collaborazione attiva" disciplinati attraverso i menzionati accordi, fornendo riscontro, ove richiesto, all'intermediario terzo segnalante.

## 4 GLOSSARIO

-“Indicatori di anomalia”: fattispecie rappresentative di operatività ovvero di comportamenti anomali posti in essere dalla clientela, finalizzate ad agevolare la valutazione, da parte dei soggetti obbligati, degli eventuali profili di sospetto di riciclaggio o di finanziamento del terrorismo.

-“Operazione sospetta”: Il Decreto Antiriciclaggio prevede che i soggetti obbligati, prima di compiere l'operazione, inviano senza ritardo alla UIF, una segnalazione di operazione sospetta quando sanno, sospettano o hanno 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 da attività criminosa. Il sospetto è desunto dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento o frazionamento o da qualsivoglia altra circostanza

<sup>2</sup> Servizio di versamento contante presso sportelli esercente Mooney S.p.A. (ex Sisal)



conosciuta, in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi acquisiti ai sensi del presente decreto. Il ricorso frequente o ingiustificato ad operazioni in contante, anche se non eccedenti la soglia di cui all'articolo 49 del d. lgs. 231/07 e, in particolare, il prelievo o il versamento in contante di importi non coerenti con il profilo di rischio del cliente, costituisce elemento di sospetto. In presenza degli elementi di sospetto, i soggetti obbligati non compiono l'operazione fino al momento in cui non hanno provveduto ad effettuare la segnalazione di operazione sospetta. Sono fatti salvi i casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto ovvero nei casi in cui l'esecuzione dell'operazione non possa essere rinviata tenuto conto della normale operatività ovvero nei casi in cui il differimento dell'operazione possa ostacolare le indagini. In dette ipotesi, i soggetti obbligati, dopo aver ricevuto l'atto o eseguito l'operazione, ne informano immediatamente la UIF.

- “Evidenze o Inattesi”: operazione o comportamento ritenuto anomalo rilevato dal sistema dei presidi adottato dalla Società al fine di contrastare il rischio di essere coinvolta, anche inconsapevolmente, in fenomeni di riciclaggio o finanziamento del terrorismo (sistemi automatici di rilevazione, sistemi di rilevazione specifici della Funzione Antiriciclaggio, segnalazioni esogene ed endogene).

- FCM Temenos: diagnostico per l'individuazione, con frequenza giornaliera, settimanale e mensile, di possibili operazioni sospette (inattesi), sulla base di specifiche di regole, messe a punto e costantemente aggiornate da un gruppo di lavoro interbancario di esperti, in conformità con il Provvedimento recante gli indicatori di anomalia per gli intermediari della Banca d'Italia e con gli schemi di rappresentativi di comportamenti anomali pubblicati dalla UIF.

- WORKFLOW AML: Database aziendale, in uso alla Funzione Antiriciclaggio, per la gestione dei processi di istruzione, valutazione ed archiviazione delle evidenze analizzate.

- GE.SA.FIN. (GEstione SANzioni FINANziarie): applicazione, a supporto dell'ufficio V della Direzione V del Dipartimento del Tesoro del MEF, per gestire il processo di richiesta di autorizzazione e controllo delle transazioni finanziarie da e verso soggetti appartenenti a paesi sanzionati.

- S.I.G.M.A.: Sistema Informatico Gestione Materiali Armamenti, a supporto delle attività istituzionali dell'Ufficio VI della Direzione V del Dipartimento del Tesoro del MEF che, sulla base di quanto previsto dalla legge 9 luglio 1990, n. 185 come modificata da D.Lgs. 105/2012, ha il compito di vigilare, insieme ad uno specifico nucleo della Guardia di Finanza, sull'attività degli istituti di credito in merito al finanziamento delle operazioni disciplinate dalla legge n. 185/90, per finalità di contrasto al terrorismo.

## 4.1 BANCHE DATI

---

Le principali Banche dati utilizzate dalla Funzione Antiriciclaggio e da Flowe sono:

- CERVED: banca dati utilizzata per valutare la solvibilità di imprese e persone, con una gamma di servizi che spazia dalle informazioni camerali a informazioni commerciali integrate.
- COMPLIANCE DAILY CONTROL: banca dati internazionale contenente i nominativi di persone fisiche e giuridiche coinvolte in reati di natura penale a monte del riciclaggio o rientranti in determinate categorie (es. Persone Esposte Politicamente).
- In aggiunta, la funzione analizza dati e notizie reperibili sulle cosiddette “fonti aperte” (internet, riviste specializzate, quotidiani etc..).

## 5 IL PROCESSO DELLE SEGNALAZIONI DELLE OPERAZIONI SOSPETTE

Il presente Regolamento illustra le diverse fasi del processo di segnalazione delle operazioni sospette; facendo riferimento alla tassonomia dei processi aziendali.

Di seguito è rappresentato il processo nella sua articolazione complessiva:



### 5.1 AVVIO DEL PROCESSO SEGNALETICO

La Funzione Antiriciclaggio analizza le segnalazioni di possibili operazioni sospette, le cui fonti ed origini possono essere ricondotte a:

- Segnalazioni esogene ed endogene che pervengono alla Funzione dalle strutture di primo livello (sede) e dalle Autorità di Vigilanza o dagli Organi investigativi;
- Sistemi automatici di rilevazione;
- Sistemi di rilevazione specifici, costituiti dalle analisi massive e dai controlli a distanza (cd. presidi) attivati direttamente dalla Funzione Antiriciclaggio.

#### 5.1.1 SEGNALAZIONI ESOGENE ED ENDOGENE

##### 5.1.1.1 Segnalazioni Esogene

L'avvio del processo segnaletico può scaturire dalle richieste ricevute da qualsiasi Intermediario, Autorità o Organo investigativo esterno tra cui, ad esempio, il Nucleo

Speciale di Polizia Valutaria della Guardia di Finanza, la DIA, l'Autorità Giudiziaria, o altri intermediari (c.d. collaborazione attiva).

In questo caso, l'Ufficio Atti Giudiziari della Direzione Affari Societari, Legale e Contenzioso di Banca Mediolanum notifica all'Unità Banking Services & Controls, Team AML che provvede a censire le richieste ricevute, anche con riferimento all'apposito dato aggiuntivo da inserire in FCM Temenos per la profilatura di rischio del cliente, e ad aprire – nelle fattispecie espressamente previste dal presente Regolamento<sup>3</sup> - apposita segnalazione nel Sistema gestionale affinché la Funzione Antiriciclaggio possa effettuare gli approfondimenti di competenza e sottoporre al Delegato le segnalazioni da valutare ai fini dell'eventuale inoltro all'UIF.

Anche le richieste di approfondimento provenienti dall'UIF o dalle Autorità di Vigilanza competenti tramite istanze attivano approfondimenti interni, condotti dalla Funzione Antiriciclaggio, da cui possono scaturire segnalazioni di operazioni sospette.

Nel caso di richieste provenienti dall'UIF, la Funzione Antiriciclaggio provvede a censire la richiesta ricevuta, avviando apposita istruttoria sulla posizione del/i cliente/i interessato/i, tramite l'apertura di apposita segnalazione nel Sistema gestionale.

Nel caso di istanze ricevute dalle Autorità di Vigilanza, la Funzione Compliance trasmette per e-mail copia dell'istanza ricevuta alla Funzione Antiriciclaggio, la quale provvede a censire la richiesta ricevuta, avviando apposita istruttoria sulla posizione del/i cliente/i interessato/i, tramite l'apertura di apposita segnalazione nel Sistema gestionale.

L'Unità Banking Services & Controls, Team AML analizza, infine, le segnalazioni di possibili operazioni anomale ricevute da intermediari terzi con cui sono in essere accordi di distribuzione o collocamento di prodotti o servizi nell'ambito dei flussi di "collaborazione attiva" disciplinati attraverso i menzionati accordi.

A tal riguardo, detta unità provvede a censire la richiesta ricevuta, avviando apposita istruttoria sulla posizione del/i cliente/i interessato/i, tramite l'apertura di apposita segnalazione nel Sistema gestionale, fornendo riscontro, ove richiesto, all'intermediario terzo segnalante.

#### 5.1.1.2 Segnalazioni Endogene

I dipendenti dell'Unità Banking Services & Controls, cui compete l'amministrazione e/o la gestione concreta dei rapporti con la clientela, comunicano senza ritardo alla Funzione Antiriciclaggio, secondo le modalità di seguito illustrate, le operazioni di cui all'art. 35 del Decreto Antiriciclaggio.

---

<sup>3</sup> Cfr. par. 7.1.1

Le strutture operative della Società (Team AML, Team Account Monitoring, Caring etc..) inviano, **senza ritardo**, segnalazione di operazione sospetta, **sicuramente nei seguenti casi**:

- ✓ cliente reticente a fornire delucidazioni e/o documentazione sulla operatività rilevata (mancanza AVR) in caso di presenza di operatività almeno pari a 10.000 euro e/o in presenza di ulteriori elementi/indici di anomalia,
- ✓ ricezione atto giudiziario (fatto salvo pignoramenti), denuncia, richiamo interbancario e/o reclamo su disconoscimento operazioni (phishing attivo e passivo),
- ✓ cliente che, a fronte delle verifiche, risultasse avere documentazione falsa,
- ✓ cliente che, a fronte delle verifiche, risultasse avere pregiudizievoli e/o protesti

La comunicazione deve essere inviata, possibilmente, prima di compiere l'operazione, fatti salvi i casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto ovvero nei casi in cui l'esecuzione dell'operazione non possa essere rinviata tenuto conto della normale operatività, ovvero nei casi in cui il differimento dell'operazione possa ostacolare le indagini.

Qualora i dipendenti delle strutture operative che gestiscono o amministrano nel concreto i rapporti con la clientela qualifichino un'operazione come sospetta, segnalano tempestivamente l'operazione attraverso caricamento di apposita segnalazione di operazione sospetta all'interno del sistema gestionale Workflow AML, allegando in formato elettronico tutta la documentazione che ritengono possa essere di supporto alla valutazione della medesima.

Il dipendente, nell'ambito dell'attività lavorativa, quando sa, sospetta o ha motivi ragionevoli di sospettare, si rivolge tempestivamente al suo responsabile al fine di valutare, unitamente a quest'ultimo, la trasmissione della segnalazione alla Funzione Antiriciclaggio di Banca Mediolanum.

Il sospetto deve fondarsi su una valutazione compiuta di tutti gli elementi delle operazioni – oggettivi e soggettivi.

In ragione della tutela della riservatezza del segnalante, ciascun dipendente/collaboratore riceverà le rispettive notifiche a mezzo email delle sole evidenze da lui trasmesse, di avvenuta presa in carico e di avvenuta archiviazione della stessa.

#### - **Funzione Antiriciclaggio**

Il Delegato alla segnalazione delle operazioni sospette effettua, con il supporto della Funzione Antiriciclaggio di Banca Mediolanum, delle verifiche, anche a campione, sulla congruità delle valutazioni dell'operatività della clientela, da parte delle strutture che effettuano il primo livello di analisi.

### 5.1.1.3 *Indici di anomalia*

La normativa in materia antiriciclaggio individua un preciso processo valutativo delle operazioni finanziarie che l'intermediario è tenuto ad effettuare per rilevare eventuali indici di anomalia e di sospetto ai fini dell'antiriciclaggio dell'antiterrorismo.

A monte delle valutazioni complessive svolte, si colloca l'indispensabile collaborazione attiva di tutti i soggetti coinvolti, sia con riferimento al personale di Flowe, che alla rete distributiva con particolare attenzione all'acquisizione di una approfondita conoscenza della clientela.

Al fine di agevolare la valutazione da parte degli intermediari sugli eventuali profili di sospetto di riciclaggio o di finanziamento del terrorismo Banca d'Italia ha emanato il Provvedimento del 12 maggio 2023 "Indicatori di anomalia dell'Unità di informazione finanziaria per l'Italia (UIF)" pubblicato in GU n.121 del 25 maggio 2023 , che richiede tra l'altro agli intermediari di adottare procedure interne di valutazione idonee a garantire la tempestività della segnalazione, la riservatezza dei soggetti coinvolti nell'effettuazione della segnalazione stessa e l'omogeneità dei comportamenti.

Tali indicatori (n. 34 indicatori di anomalia), ciascuno dei quali articolato in sub-indici, che costituiscono esemplificazioni dell'indicatore di riferimento. Si mette in questo modo a disposizione dei destinatari uno strumento operativo per la selezione di situazioni che possono venire alla loro attenzione nell'ambito della concreta attività svolta, da valutare per decidere se ricorrono i presupposti per una segnalazione di operazioni sospette.

L'elencazione degli indicatori e dei relativi sub-indici non è esaustiva; i destinatari valutano pertanto con la massima attenzione ulteriori comportamenti che, sebbene non descritti, siano tali da generare in concreto profili di sospetto.

Gli indicatori da 1 a 8 (sezione A) evidenziano profili che attengono al comportamento o alle caratteristiche qualificanti del soggetto cui è riferita l'operatività; gli indicatori da 9 a 32 (sezione B) riguardano le caratteristiche e la configurazione dell'operatività, anche in relazione a specifici settori di attività; gli indicatori 33 e 34 (sezione C) attengono a operatività che potrebbero essere connesse al finanziamento del terrorismo e a programmi di proliferazione di armi di distruzione di massa.

Tali elementi attengono a due diversi profili, il primo è relativo ai rapporti o alle operazioni poste in essere (oggettivo), il secondo invece è relativo al cliente (soggettivo).

Le operatività sono individuate come sospette solo in presenza di circostanze soggettive e oggettive. In proposito, andrà considerato che gli indicatori e taluni sub-indici contengono riferimenti a circostanze sia soggettive sia oggettive.

Flowe, richiedendo una attenta e costante verifica di tali indicatori di anomalia, segnala ulteriori elementi, che, soprattutto se presenti contemporaneamente, dovranno far

scaturire una più attenta verifica del rapporto o dell'operazione. A tal proposito ha selezionato preliminarmente gli indicatori rilevanti alla luce della concreta attività svolta e quindi quelli da considerare a essi applicabili (Allegato 1 "Indicatori di anomalia Prexta").

## **PROFILO OGGETTIVO DEI RAPPORTI E DELLE OPERAZIONI POSTE IN ESSERE (ENTITÀ, NATURA E CARATTERISTICHE)**

Si richiede una più attenta verifica nei seguenti casi:

1. tipologia del datore di lavoro,
2. tipologia dell'attività del soggetto richiedente (c.d. TAE),
3. estinzione anticipata di un finanziamento a termine (entro 6 mesi),
4. rapporto fra il numero dei dipendenti complessivo dell'ente datoriale e il numero dei dipendenti richiedenti il finanziamento, anche con riferimento agli anni di vita dell'ente datoriale stesso.

## **PROFILO SOGGETTIVO DI COLUI CHE COMPIE L'OPERAZIONE (CAPACITÀ ECONOMICA E TIPO DI ATTIVITÀ LAVORATIVA SVOLTA)**

Si richiede una conoscenza approfondita del cliente, con particolare riferimento alle sue caratteristiche economiche, e alle sue esigenze finanziarie. Tale conoscenza dovrebbe essere approfondita a tal punto da consentire di individuare, o quanto meno ipotizzare, la provenienza dei beni e proventi del patrimonio dei clienti. Si richiede altresì una verifica puntuale dei collegamenti con altri soggetti o con altre operazioni; Infatti, la lettura di una operazione di per sé anomala o atipica e tale da suscitare dubbi, se collocata all'interno di un contesto, potrebbe trovare una giustificazione coerente e plausibile. Per contro l'assenza di specifici profili di anomalia non è sufficiente di per sé ad escludere il sospetto che un'operazione possa essere connessa a fatti di riciclaggio.

Si richiede quindi una maggiore attenzione e verifica nei seguenti casi:

- i Clienti, i titolari effettivi e gli esecutori con riferimento ai quali sono stati rilevati degli indici reputazionali negativi, sulla base di:
  - ricorrenza dei nominativi nelle liste delle persone o degli enti associati ai fini degli obblighi di congelamento previsti dai Regolamenti comunitari o dai decreti emanati dal MEF, ai sensi del D. Lgs. N. 109/2007;
  - notizie negative fornite direttamente dal Cliente o dal consulente finanziario di riferimento, aventi ad oggetto procedimenti penali, procedimenti per danno erariale, procedimenti per responsabilità amministrativa degli enti (ex D. Lgs. 231/01), etc.;

- richieste/provvedimenti provenienti dall'Autorità Giudiziaria, ai sensi: del Codice Antimafia (accertamenti richiesti dall'Autorità Penale ai sensi del D. Lgs. 159/2011 - Antimafia - fase delle indagini preliminari) o della normativa antiriciclaggio (accertamenti richiesti dall'Autorità Penale ai sensi del Decreto Antiriciclaggio - Antiriciclaggio - fase delle indagini preliminari);
- decreti di sequestro, ovvero misure cautelari reali e di prevenzione adottate dall'Autorità Giudiziaria;
- i Clienti, i titolari effettivi e gli esecutori oggetto di segnalazione alla UIF;
- i Clienti e/o i titolari effettivi che rientrano nella definizione di "Persone Esposte Politicamente";
- in presenza di un rischio più elevato di riciclaggio o finanziamento del terrorismo.

### **(COMPORTAMENTO)**

In particolare, deve essere opportunamente considerato, dall'Agente in Attività Finanziaria o dal Dipendente/Collaboratore di quest'ultimo incaricato, il comportamento tenuto dal Cliente o dall'esecutore, quale, a titolo esemplificativo ma non esaustivo (per ulteriori indicatori di anomalia si rimanda al provvedimento contenente indicatori di anomalia pubblicato dalla UIF):

- la riluttanza o incapacità nel fornire informazioni anche rispetto all'operatività svolta e/o sulla origine dei fondi la ripetuta modifica delle informazioni fornite o il fatto che siano fornite informazioni incomplete o erronee;
- l'interposizione di soggetti terzi senza apparente giustificazione (es. viene costantemente accompagnato da altre persone che appaiono estremamente interessate all'operatività ovvero alle modalità di esecuzione della prestazione) e/o il rilascio di deleghe o procure del tutto incoerente con l'attività svolta o varia molto frequentemente i soggetti delegati;
- porre ripetuti quesiti in ordine alle modalità di applicazione della normativa antiriciclaggio e antiterrorismo e cerca di indurre l'Agente in Attività Finanziaria ad eludere tali presidi, anche tentando di stabilire relazioni eccessivamente confidenziali;
- l'indisponibilità o l'impossibilità di produrre documentazione in merito alla propria identità (fatto salvo il caso dei richiedenti asilo);
- la ripetuta modifica delle informazioni fornite o il fatto che siano fornite informazioni incomplete o erronee e/o significativamente difforni, contraddittorie o comunque non coerenti con quelli tratte da fonti affidabili e indipendenti (es. testate giornalistiche o altri siti di divulgazione notizie via web);



- la presenza di un documento identificativo utilizzato dallo stesso nella procedura di on-boarding che la Certification Authority ha valutato come “contraffatto”, con conseguente scarto/rigetto della pratica;
- la volontà di ricevere le comunicazioni a esso rivolte ad un recapito diverso da quello indicato (ad esempio, residenza, domicilio, indirizzo di posta elettronica, numero di cellulare, applicazione web o mobile o altro strumento di comunicazione a distanza) o non risulta rintracciabile ai recapiti indicati ovvero chiede l'invio diretto delle comunicazioni a soggetti a lui non collegati, indirizzi e-mail, etc.);
- l'indisponibilità di esibire la documentazione o le informazioni di prassi, con conseguente rinuncia immotivata all'operatività o richiesta di svolgerne una differente, soprattutto se quest'ultima comporta un aggravio di costi a proprio carico;
- l'esecuzione o l'intenzione di eseguire operazioni caratterizzate da importi insolitamente elevati o rispetto alle quali sussistano dubbi circa la finalità cui le medesime sono, in concreto, preordinate;
- la ricezione di pagamenti (in caso di estinzioni anticipate) da parte di soggetti terzi privi di un legame con il Cliente e senza apparente (e documentata) motivazione;
- la mancata ragionevolezza dell'operazione in funzione dell'abituale operatività/patrimonio/reddito, delle caratteristiche, delle competenze o delle conoscenze normalmente attese per il settore di attività dichiarate dal Cliente.

affinché possa configurarsi - almeno in via astratta - l'eventualità di un'operazione sospetta, occorre di volta in volta, nella pratica, integrare tali indici con l'attenta valutazione della situazione effettiva del cliente o degli altri soggetti/entità coinvolte.

### 5.1.2 SISTEMI AUTOMATICI DI RILEVAZIONE

L'Unità Banking Services & Controls, Team AML provvede ad analizzare gli “inattesi” (*alerts*) che emergono dal sistema FCM Temenos (Profile).

Tali sistemi rilevano *real-time*, giornalmente, settimanalmente e mensilmente possibili anomalie, individuate in funzione di specifiche regole messe a punto e costantemente aggiornate, in conformità agli indicatori di anomalia emanati dalla Banca d'Italia ed agli schemi rappresentativi di comportamenti anomali pubblicati, tempo per tempo, dalla UIF.

Rientrano tra i sistemi automatici di rilevazione anche le analisi dei rilievi generali, pervenuti tramite il portale Infostat-UIF, relativi al flusso S.A.R.A. In questo caso, è cura della Funzione Antiriciclaggio effettuare le verifiche preliminari ed avviare apposita istruttoria sulla posizione del/i cliente/i interessato/i, tramite l'apertura di apposita segnalazione nel Sistema gestionale.



### 5.1.3 SISTEMI DI RILEVAZIONE SPECIFICI DELLA FUNZIONE ANTIRICICLAGGIO

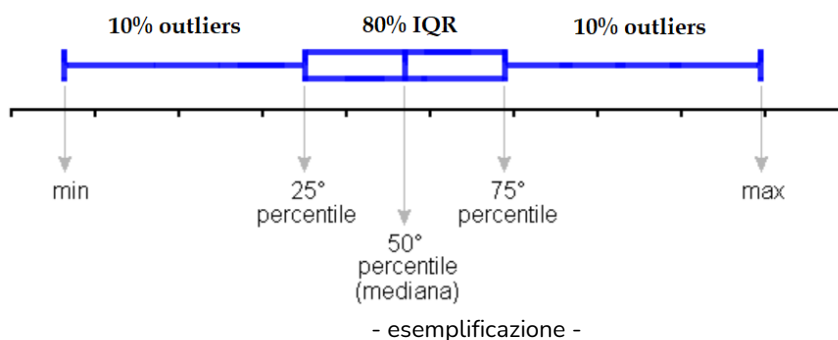
La Funzione Antiriciclaggio pone in essere, inoltre, dei controlli di secondo livello, costituiti dalle “verifiche massive” e dai “presidi”.

Le verifiche massive hanno lo scopo di individuare e approfondire annualmente, su base campionaria, possibili comportamenti anomali nell’operatività dei clienti. A tal riguardo, possono essere effettuate tre tipologie di analisi massiva: (1) geografica (2) mirata alle operazioni singole (3) combinata (o complessa).

Per la definizione del perimetro di clientela in ambito della verifica massiva, una volta definito la base dati del campione, si applicano le seguenti regole tramite utilizzo della tecnica di Tukey per l’eliminazione degli *outlier* attraverso le differenze interquartili:

- Viene selezionato il 20% del campione tra i clienti facenti parte degli “*outliers*” (valori compresi nel primo quartile ( $Q_1$ ) o nel terzo quartile ( $Q_3$ )), ovvero ricompresi nel 25% della clientela ai lati (dispersione) del campione,
- Viene selezionato il 80% del campione tra i clienti compresi compresa tra il terzo ( $Q_3$ ) ed il primo ( $Q_1$ ) quartile ( $Q = Q_3 - Q_1$ ), ovvero l’ampiezza della fascia di valori che contiene la metà “centrale” dei valori osservati.

La formula statistica volta a definire il dato IQR (Inter Quartile Range) della clientela compresa tra il terzo ( $Q_3$ ) ed il primo ( $Q_1$ ) quartile ( $Q = Q_3 - Q_1$ ).



$$\text{Posizione } Q_1 = \frac{Q_1(pos) = \frac{N+1}{4} \times 1}{N = \text{numero valori}}$$

$$\text{Posizione } Q_3 = \frac{Q_3(pos) = \frac{N+1}{4} \times 3}{}$$

I presidi hanno l’obiettivo di individuare, nel *continuum*, possibili comportamenti anomali dei clienti, legati alla soddisfazione di parametri predefiniti.

Rientrano, tra i presidi, anche le pratiche riaperte dalla Funzione Antiriciclaggio a seguito di monitoraggio richiesto dal Delegato. In questo caso, il sistema gestionale, avvalendosi dell'apposito scadenziere previsto all'interno del *database* riapre la verifica sul cliente.

Le verifiche massive ed i presidi sono oggetto di pianificazione annuale e vengono sottoposti, per la relativa valutazione ed approvazione, al Consiglio di Amministrazione della Società.

Il Responsabile della Funzione Antiriciclaggio riesamina, periodicamente, i presidi e le analisi massive, con particolare riferimento ai parametri utilizzati per la rilevazione delle operazioni potenzialmente sospette e alla incidenza delle operazioni sospette effettivamente inoltrate, rispetto agli inattesi esaminati.

## 5.2 ASSEGNAZIONE DELLA PRATICA

---

Il Coordinatore dei gestori che si occupano dell'analisi delle SOS della Funzione Antiriciclaggio della Banca e/o il responsabile dell'Unità stessa, a fronte di ciascuna segnalazione esogena o endogena ricevuta tramite l'apertura di apposita segnalazione nel Sistema gestionale, individua il gestore cui affidare l'analisi di dettaglio della medesima, per il conseguente inoltro in valutazione al Delegato.

Nel caso, invece, di evidenze provenienti da Sistemi automatici di rilevazione o da Sistemi di rilevazione specifici della Funzione, il Coordinatore dei gestori che si occupano dell'analisi delle SOS della Funzione Antiriciclaggio della Banca e/o il responsabile dell'Unità stessa provvede ad individuare il gestore cui affidare l'analisi di dettaglio della medesima e sottoporla successivamente, al ricorrere di determinate condizioni, alla valutazione del Delegato, ovvero procedere alla archiviazione della stessa (cfr. par. 5.4).

All'atto dell'assegnazione della pratica, il sistema trasmette al gestore una apposita notifica a mezzo *e-mail*.

## 5.3 ISTRUZIONE DELLA PRATICA

---

La fase di istruzione della pratica è propedeutica alla raccolta di tutte le informazioni utili a qualificare l'operazione o il comportamento anomalo rilevato ed a poterla portare in valutazione al Delegato completa di tutti gli elementi secondo le regole del successivo par. 5.4.

Il gestore della Funzione Antiriciclaggio della Banca istruisce la pratica, tramite il Sistema gestionale in uso, raccogliendo e analizzando le informazioni relative al profilo soggettivo del cliente e oggettivo dell'operazione.

In tale ambito, il gestore procede, in particolare, all'acquisizione ed all'approfondimento dei dati anagrafici del cliente e di quelli forniti dal medesimo in sede di adeguata verifica, controllando, allo stesso tempo, la presenza di analisi e/o segnalazioni pregresse sul medesimo, il relativo profilo di rischio di riciclaggio, gli investimenti effettuati in prodotti del Gruppo, la presenza di notizie o pregiudizievoli sulle banche dati in uso e su fonti aperte, nonché eventuali richieste di informazioni o provvedimenti censiti nel database Atti Giudiziari.

Il gestore provvede altresì ad analizzare la movimentazione effettuata sul rapporto di conto corrente e gli eventuali legami con altri soggetti (es. intestatario carta prepagata, etc.), nonché ad approfondire le caratteristiche, l'entità e la natura della/e operazione/i in esame, interfacciandosi anche con i Team AML e/o Account Monitoring dell'Unità Banking Services & Controls.

L'Unità Banking Services & Controls effettua, in ogni caso ed in autonomia, il controllo ed il monitoraggio nel continuo sull'operato dei clienti ai fini dei controlli di primo livello in ambito Antiriciclaggio.

Pertanto tale Unità, ove non sia stato attivato dalla Funzione Antiriciclaggio per gli approfondimenti sopra descritti, può a sua volta essere parte attiva, nell'ambito del processo segnaletico, inserendo apposite segnalazioni tramite email (cfr. par. 5.1.1.2), ove ad, esito dei controlli effettuati, emergano delle evidenze di possibili operazioni anomale.

## 5.4 TRASMISSIONE DELLA PRATICA IN VALUTAZIONE

---

Al termine della fase di istruttoria, il gestore redige una sintesi delle analisi effettuate, compilando l'apposito campo del Sistema gestionale. Al fine di individuare e qualificare gli eventuali elementi di sospetto, ciascun gestore assume a riferimento gli indicatori di anomalia della Banca d'Italia e gli schemi di comportamento anomalo dell'UIF.

I singoli gestori ed i Coordinatori/Responsabili (cd. soggetti abilitati) possono, a seguito degli approfondimenti effettuati, archiviare direttamente le pratiche aperte a seguito di evidenze generate da sistemi automatici di rilevazione o da sistemi di rilevazione specifici della Funzione Antiriciclaggio, ove non rilevino elementi di sospetto (cd. falsi positivi), mantenendo adeguata evidenza delle analisi effettuate e delle motivazioni sottostanti.

Devono essere trasmesse al Delegato alla segnalazione di operazioni sospette per le necessarie valutazioni tutte le pratiche relative alle segnalazioni esogene ed endogene, indipendentemente dal controvalore delle operazioni sottostanti e dalla presenza o meno di elementi di sospetto.

## 5.5 VALUTAZIONE DELLE OPERAZIONI SOSPETTE

---

Il Delegato alla segnalazione di operazioni sospette riceve direttamente le schede predisposte dal gestore, tramite il Sistema gestionale, e può procedere come segue:

- richiedere al gestore ulteriori informazioni, rimandando la scheda “in lavorazione”;
- richiedere all’UIF l’applicazione di un Provvedimento di sospensione, ai sensi dell’art. 6, comma 4, lettera c) del d. lgs. 231/07 (cfr. par. 5.5.1);
- richiedere, all’Unità Banking Services & Controls, l’estinzione del rapporto ex art. 42 d. lgs. 231/07, nei casi di impossibilità oggettiva di effettuare l’adeguata verifica, valutando se effettuare una segnalazione di operazione sospetta alla UIF ex art. 35 del d. lgs. 231/07 (cfr. par. 5.5.2);
- richiedere, all’Unità Banking Services & Controls di valutare l’estinzione del rapporto, ove, pur non ricorrendo le condizioni di cui all’art. 42, lo stesso presenti elementi di rischio elevato di riciclaggio o finanziamento del terrorismo o sia utilizzato in modo incoerente con lo scopo e la natura dello stesso;
- richiedere preventiva autorizzazione al CSF, per effettuare specifiche operazioni rientranti nelle fattispecie dallo stesso disciplinate (es. operazioni con paesi sotto embargo finanziario o aventi ad oggetto armamenti)<sup>4</sup>.
- ritenere sospetta la segnalazione e fornire indicazioni all’Unità Analisi AML di Banca Mediolanum per effettuare la segnalazione all’UIF ex art. 35 d. lgs. 231/07, tramite il portale Infostat-UIF;
- non ritenere sospetta la segnalazione e archivarla, mantenendo evidenza, tramite il Sistema gestionale, delle valutazioni effettuate, fornendo indicazioni al gestore della pratica perché sia data apposita informativa dell’archiviazione al dipendente o al collaboratore della Rete di Vendita che ha effettuato la segnalazione e ponendo evidenza della presenza di eventuali procedimenti/provvedimenti sul cliente, affinché l’Unità Banking Services & Controls registri l’informazione in apposito dato aggiuntivo anagrafico;
- non ritenere sospetta l’operazione e archivarla, mantenendo evidenza delle valutazioni effettuate, richiedendo, tuttavia, l’innalzamento del profilo di rischio del/i cliente/i interessato/i e/o il monitoraggio continuativo della posizione per un determinato lasso temporale alla Struttura Operativa segnalante e/o all’Unità Conformità e Analisi AML della Funzione Antiriciclaggio di Banca Mediolanum, ovvero pianificando uno specifico monitoraggio in via continuativa o alla scadenza di un termine prestabilito definito dal Delegato stesso (es. a tre mesi, a sei mesi, etc.).

### 5.5.1 RICHIESTA PROVVEDIMENTO DI SOSPENSIONE

---

<sup>4</sup> Tramite accesso al portale: <https://portalesoro.mef.gov.it/> e l’utilizzo di apposite credenziali sulle applicazioni: GE.SA.FIN. o S.I.G.M.A.

All'Unità di Informazione Finanziaria è riconosciuto, ex art. 6, comma 4, lettera c), del D. Lgs. n. 231/07, il potere di sospendere, anche su richiesta del Nucleo Speciale di Polizia Valutaria della Guardia di Finanza, della DIA e dell'Autorità Giudiziaria, per un massimo di cinque giorni lavorativi, operazioni sospette di riciclaggio o di finanziamento del terrorismo, dandone immediata notizia a tali organi. La procedura di sospensione, nella maggior parte dei casi, prende avvio con la comunicazione in via d'urgenza, da parte di un soggetto obbligato, di un'operazione sospetta di riciclaggio richiesta dal cliente ma non ancora eseguita, che viene sottoposta alla UIF affinché valuti l'opportunità di disporre la sospensione.

Nell'ambito della propria attività istruttoria la UIF, prende contatto con gli Organi investigativi allo scopo di verificare che – come previsto dalla legge – l'eventuale sospensione non pregiudichi il corso di indagini; la verifica è anche volta ad acquisire elementi in merito all'eventuale successiva adozione di misure cautelari giudiziarie e a fornire informazioni utili per la migliore efficacia delle stesse.

Qualora il Delegato intenda richiedere l'applicazione del provvedimento di sospensione all'UIF, si attiva tempestivamente per:

- predisporre il testo della richiesta di sospensiva (c.d. informativa di sospensione) da inviare a mezzo email all'indirizzo [uif.sos1@bancaditalia.it](mailto:uif.sos1@bancaditalia.it), previa anticipazione telefonica alla stessa;
- trasmettere la segnalazione di operazione sospetta all'UIF, valorizzando l'apposito campo strutturato "richiesta sospensione".

La richiesta del provvedimento di sospensione può altresì essere avanzata al Delegato, per le valutazioni di competenza, da parte di ciascun dipendente, mediante apposita e-mail all'indirizzo [antiriciclaggio@mediolanum.it](mailto:antiriciclaggio@mediolanum.it), nella quale sono dettagliati i motivi del sospetto e gli elementi a supporto del provvedimento di urgenza (alla richiesta deve seguire apposito caricamento di segnalazione operazione sospetta all'interno del sistema gestionale apposito).

## 5.5.2 OBBLIGHI DI ASTENSIONE

Qualora la Società si trovi nella impossibilità oggettiva di effettuare l'adeguata verifica della clientela, si astiene dall'instaurare, eseguire ovvero proseguire il rapporto, le operazioni (c.d. obbligo di astensione) procedendo, se del caso, all'estinzione del rapporto continuativo già in essere e valutando se effettuare una segnalazione di operazione sospetta alla UIF. Prima di effettuare la segnalazione di operazione sospetta alla UIF e al fine di consentire l'eventuale esercizio del potere di sospensione, la Società si asterrà dall'eseguire le operazioni per le quali sospetta vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo.

Nei casi in cui l'astensione non sia possibile in quanto sussiste un obbligo di legge di ricevere l'atto ovvero l'esecuzione dell'operazione per sua natura non possa essere rinviata o l'astensione possa ostacolare le indagini, permane l'obbligo di immediata segnalazione di operazione sospetta.

La Società si astiene dall'instaurare rapporti o eseguire operazioni e pone fine al rapporto continuativo già in essere con:

- clienti o potenziali clienti residenti in paesi esteri (clientela non in *target*);
- operazioni con paesi esteri c.d. "ad alto rischio", come individuati dalla Società ed in linea con le previsioni della Capogruppo.

La Società si astiene altresì dall'offrire prodotti/servizi o dar corso ad operazioni che potrebbero favorire l'anonimato.

E' fatta in ogni caso salva l'applicazione dell'articolo 35, comma 2 (ossia, dopo aver ricevuto l'atto o eseguito l'operazione, il Delegato alle SOS ne informerà immediatamente la UIF), nei casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto.

## 5.6 SEGNALAZIONE DELL'OPERAZIONE

La segnalazione di una operazione sospetta è il risultato di un complesso processo di valutazione, basato su elementi:

- oggettivi, quali le caratteristiche, l'entità e la natura dell'operazione;
- soggettivi, quali le caratteristiche personali, la capacità reddituale e l'attività economica esercitata.

Il Delegato alla segnalazione di operazioni sospette, esamina le segnalazioni pervenutegli e, qualora le ritenga fondate tenendo conto dell'insieme degli elementi a sua disposizione, fornisce indicazioni al gestore dell'Unità Conformità e Analisi AML di Banca Mediolanum per la predisposizione della segnalazione da inoltrare all'UIF, indicando il livello di rischio dell'operatività segnalata, secondo il suo prudente apprezzamento, ed il fenomeno a cui la stessa è riconducibile, in base alla tassonomia definita dall'UIF.

Il gestore cui è assegnata la pratica provvede quindi a predisporre la bozza di segnalazione, contenente, tra l'altro, la descrizione dell'operatività sospetta e dei motivi del sospetto e la sottopone nuovamente al Delegato, tramite il Sistema gestionale. Il Delegato, esaminata la bozza della segnalazione e apportate le modifiche e/o le integrazioni che ritiene opportune, autorizza la trasmissione della segnalazione alla UIF, che viene effettuata dal gestore, priva del nominativo del segnalante.

La segnalazione, ove possibile, prevede un richiamo degli indicatori di anomalia\schemi di comportamenti anomali individuati dalle Autorità competenti ed assunti a base della valutazione della stessa.

Le segnalazioni di operazioni sospette sono trasmesse tempestivamente, una volta ottenuta l'autorizzazione del Delegato tramite il Sistema gestionale, dalla Funzione Antiriciclaggio alla UIF, in via telematica, attraverso il portale Infostat-UIF della Banca d'Italia, seguendo le istruzioni contenute nel Manuale Operativo pubblicato dalla UIF e presente sul portale medesimo.

La segnalazione:

- è contraddistinta da un numero identificativo e da un numero di protocollo attribuito in modo univoco, su base annua, dal sistema informativo della UIF;
- indica se nell'operatività segnalata è stato ravvisato il sospetto di riciclaggio, di finanziamento del terrorismo, di proliferazione di armi di distruzione di massa, ovvero se la medesima è stata originata nell'ambito di una procedura di *voluntary disclosure* cui il cliente ha aderito;
- può indicare altresì il fenomeno al quale l'operazione sospetta è riferibile, qualora corrisponda a uno degli schemi rappresentativi di comportamenti anomali;
- riporta l'evento che ha dato origine all'inoltro della medesima, scegliendo fra quelli riportati dalla normativa: qualora concorrano più eventi deve essere indicato quello più significativo;
- contiene il riferimento (numero identificativo o numero di protocollo) ad eventuali segnalazioni ritenute collegate ed il motivo del collegamento.

A segnalazione avvenuta, viene aggiornato il profilo di rischio di riciclaggio del cliente segnalato a cura della Funzione Antiriciclaggio, innanzandolo a livello "alto".

## 5.7 ANALISI UIF

La UIF effettua l'analisi finanziaria delle segnalazioni ricevute; a tal riguardo, può acquisire ulteriori informazioni presso i soggetti obbligati, avvalersi degli archivi ai quali ha accesso, scambiare informazioni con omologhe autorità estere (FIU).

L'analisi finanziaria consiste in una serie di attività sotto il profilo tecnico-finanziario, volte a comprendere, sulla base dell'insieme degli elementi acquisiti, il contesto all'origine della segnalazione, individuare i collegamenti soggettivi e operativi, ricostruire il percorso dei flussi finanziari segnalati come sospetti e identificare le possibili finalità sottostanti.

Al termine dell'analisi finanziaria, la UIF trasmette le segnalazioni ritenute fondate, corredate di una relazione tecnica, al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza (NSPV) e alla Direzione Investigativa Antimafia (DIA) per gli eventuali approfondimenti investigativi; comunica all'Autorità Giudiziaria i fatti di possibile rilevanza penale; mantiene invece evidenza per dieci anni delle segnalazioni che non presentano un effettivo rischio di riciclaggio o di finanziamento del terrorismo, mediante procedure che consentano, sulla base di protocolli di intesa, la consultazione da parte degli Organi investigativi.



In tale ambito, la UIF può richiedere ulteriori informazioni o approfondimenti, telefonicamente o a mezzo e-mail, al Delegato in merito alle segnalazioni inoltrate.

Al fine di tracciare le richieste ricevute e le risposte fornite, l'Unità Conformità e Analisi AML di Banca Mediolanum provvede ad aprire apposita segnalazione di analisi nel Sistema gestionale e a fornire riscontro all'UIF a mezzo PEC, previa autorizzazione del Delegato.

Ai sensi dell'art. 41, comma 2, del D.Lgs. n. 231/2007, l'Unità di Informazione Finanziaria, con modalità idonee a garantire la tutela della riservatezza, comunica al segnalante, direttamente ovvero tramite gli organismi di autoregolamentazione, gli esiti delle segnalazioni, anche tenendo conto delle informazioni ricevute dalla Direzione investigativa antimafia e dal Nucleo speciale di polizia valutaria della Guardia di finanza.

A tal riguardo, il Coordinatore dei gestori che si occupano dell'analisi delle SOS della Funzione Antiriciclaggio provvede ad analizzare le segnalazioni archiviate ed a predisporre specifica reportistica per il Delegato alla segnalazione di operazioni sospette.

L'Unità di Informazione Finanziaria trasmette, infine, a un campione di segnalanti, una scheda informativa di **feedback**, contenente un riscontro sull'attività segnaletica dell'anno precedente. L'iniziativa mira a favorire, presso gli intermediari, processi di autovalutazione interna in merito alla propria collaborazione attiva in materia di prevenzione del riciclaggio e del finanziamento del terrorismo. A tal riguardo, la Funzione Antiriciclaggio riceve ed analizza periodicamente, di concerto con il Delegato alla segnalazione di operazioni sospette, le schede di *feedback* trasmesse dall'Unità di Informazione Finanziaria e predispone apposita informativa per il Consiglio di Amministrazione di Flowe SB S.p.A.

## 5.8 ARCHIVIAZIONE DELLA PRATICA E MONITORAGGIO

Una volta trasmessa la segnalazione all'UIF, il gestore della Funzione Antiriciclaggio procede all'archiviazione della pratica e di tutti gli allegati prodotti dalla procedura, attribuendo il numero di protocollo di segnalazione, tramite il portale Infostat-UIF di riferimento.

Gli atti e i documenti in cui sono indicate le generalità dei soggetti segnalanti e segnalati sono custoditi in formato elettronico sia sul Sistema gestionale sia nell'apposita *directory* di rete della Funzione Antiriciclaggio, il cui accesso è consentito esclusivamente agli addetti della Funzione, sotto la diretta responsabilità del Delegato alla segnalazione delle operazioni sospette.

Nel caso in cui il Delegato abbia deciso di archiviare la segnalazione senza dar corso alla trasmissione della medesima all'UIF, fornisce indicazioni all'Unità Conformità ed Analisi AML di Banca Mediolanum affinché il Responsabile del dipendente della Struttura Operativa che ha effettuato la segnalazione, riceva apposita e-mail, dalla Funzione Antiriciclaggio, con l'indicazione dell'esito dell'avvenuta archiviazione.



Resta ferma la possibilità, per il Delegato, di richiedere all'Unità Conformità e Analisi AML di Banca Mediolanum:

- il monitoraggio nel continuo del cliente;
- di riesaminare la posizione del cliente alla scadenza di un determinato intervallo temporale indicato dal Delegato medesimo;
- di analizzare la posizione del cliente nel caso trattasi di cliente comune di Gruppo

La Funzione Antiriciclaggio provvede, di conseguenza, a monitorare la posizione della pratica ove richiesto dal Delegato alle segnalazioni delle operazioni sospette, aprendo apposita segnalazione nel Sistema gestionale.

## 5.9 RISERVATEZZA E CONSERVAZIONE DELLE SEGNALAZIONI

Tutte le pratiche analizzate dalla Funzione Antiriciclaggio sono adeguatamente conservate tramite il Sistema gestionale. In particolare, tutte le informazioni e gli approfondimenti svolti in merito alla segnalazione di un'operazione sospetta sono storicizzati nell'archivio informativo della stessa Unità Analisi AML di Banca Mediolanum oltre che archiviate in apposita *share* di rete al cui accesso sono abilitati esclusivamente i gestori dell'Unità sopra citata. Sono inoltre applicate le *policy* operative di sicurezza previste dalla Società (es. *back up* giornaliero dell'archivio). Tutta la documentazione attestante l'iter di segnalazione viene conservata tutelando la riservatezza dei dati contenuti, del nominativo del segnalato e del segnalante.

Ferma restando la tutela della riservatezza dell'identità del soggetto di primo livello che ha effettuato la segnalazione, il Delegato alla segnalazione delle operazioni sospette può consentire che i nominativi dei clienti oggetto di segnalazione sospetta siano consultabili – anche attraverso l'utilizzo di idonee basi informative – dai responsabili delle diverse strutture operative aziendali, 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.

I responsabili abilitati all'accesso delle informazioni osservano gli obblighi di riservatezza sui nominativi dei clienti oggetto di segnalazione di operazione sospetta, in ottemperanza a quanto previsto dal D. Lgs. 196/2003 e nel rispetto della "lettera di incarico" sottoscritta in sede di assunzione.

## 6 INTERRELAZIONE CON ALTRE UNITÀ ORGANIZZATIVE

Fermo restando l'obbligo di segnalazione, alla Funzione Antiriciclaggio, di eventuali operazioni sospette secondo le modalità illustrate nel presente Regolamento, si riportano, di seguito, i principali flussi informativi attivati tra la Funzione Antiriciclaggio e le altre unità organizzative.

## 7.1 FLUSSI VERSO LA FUNZIONE ANTIRICICLAGGIO

---

La Funzione Antiriciclaggio, in aggiunta alla analisi delle segnalazioni di operazioni sospette da parte dei dipendenti, ha attivato, nell'ambito del complessivo apparato dei controlli di secondo livello svolti, appositi flussi informativi da parte di talune strutture amministrative e di *back office* della sede.

Tali flussi sono propedeutici all'avvio di apposita fase istruttoria, che prevede il coinvolgimento dei consulenti finanziari di riferimento dei clienti o delle strutture operative a cui gli stessi sono assegnati, ai fini degli approfondimenti del caso e della eventuale qualificazione delle operazioni sottostanti come sospette.

### 7.1.1 FUNZIONE COMPLIANCE

La Funzione Compliance segnala, alla Funzione Antiriciclaggio, i nominativi dei clienti/dipendenti oggetto di segnalazione alla CONSOB, in ottemperanza a quanto previsto in materia di *market abuse*, allegando le schede di dettaglio delle operazioni ritenute anomale con ogni informazione utile a ricostruire la cronologia degli eventi e le ragioni sottostanti dette operazioni.

### 7.1.2 DIREZIONE AFFARI SOCIETARI, LEGALE E CONTENZIOSO

L'Ufficio Atti Giudiziari della Direzione Affari Societari, Legale e Contenzioso provvede, alla ricezione di richieste o provvedimenti da parte degli Organi Investigativi e dell'Autorità Giudiziaria, alla notifica delle medesime a Flowe. L'Unità Banking Services & Controls, Team AML carica nel gestionale di riferimento FCM (Temenos), inserendo, lo specifico codice da attribuire alla posizione del/i cliente/i interessato/i, affinché tale informazione sia tenuta in debito conto per la profilatura di rischio della clientela.

L'Unità Banking Services & Controls, Team AML provvede, inoltre, a comunicare tempestivamente alla Funzione Antiriciclaggio della Banca, tramite inserimento di apposite schede nominative nel Sistema gestionale:

- le richieste provenienti dall'Autorità Giudiziaria, predisposte ai sensi del Codice Antimafia (accertamenti richiesti dall'Autorità Penale ai sensi della D. Lgs 159/2011 – Antimafia – fase delle indagini preliminari);
- le richieste provenienti dalle Autorità Giudiziarie, predisposte ai sensi della normativa antiriciclaggio (accertamenti richiesti dall'Autorità Penale ai sensi del D.Lgs 231/07 – Antiriciclaggio – fase delle indagini preliminari);
- i Decreti di sequestro: misure cautelari reali e misure di prevenzione a prescindere dalla tipologia dei medesimi ("per equivalente", "di rapporti", anche Conservativi);
- la presenza di pregiudizievoli e/o procedure concorsuali (es. fallimenti) in capo al cliente.

Non è prevista l'apertura della scheda di segnalazione da parte dell'Unità Banking Services & Controls, Team AML, nel Sistema gestionale, nel caso in cui:

- il soggetto su cui l'Autorità indaga ha rapporti estinti da oltre un anno;
- la richiesta di accertamento, proveniente dall'Autorità risulta collegata a segnalazioni di operazioni sospette effettuate dalla Funzione Antiriciclaggio, (riconducibili ad uno specifico protocollo UIF indicato nella richiesta o comunque indicato nel testo); in questo caso, l'Ufficio Atti Giudiziari trasmette a mezzo e-mail, alla Funzione Antiriciclaggio, una informativa circa il tipo di approfondimento richiesto.

Il personale della Funzione Antiriciclaggio ha accesso, in ogni caso, al Database in uso presso l'Ufficio Giudiziari, al fine di poter valutare, in sede di istruttoria delle pratiche, la presenza di eventuali richieste o provvedimenti pregressi sulla posizione del cliente esaminato.

#### 7.1.2 UNITA' BANKING SERVICES & CONTROLS

Il Team AML dell'Unità Banking Services & Controls esegue i controlli di merito sui possibili match evidenziati tramite *alert* da sistema (*screen* su liste dell'*infoprovider* SGR Consulting e su liste pubbliche<sup>5</sup>), sia in fase di censimento di nuovi clienti sia quotidianamente sull'intera anagrafe dei clienti della Società.

L'esito del controllo sulle liste può fornire riscontro sulla possibilità che il *prospect* o il cliente sia presente in una delle seguenti liste:

- PEP;
- PIL;
- CRIME (*complete*);
- SANCTION (*complete*);
- CLIENTI INDESIDERATI,
- APPALTI

In caso di riscontro con le liste, la linea effettua un ulteriore controllo di merito tramite notizie web, al fine di comprendere se il *prospect* sia effettivamente il soggetto presente nella lista.

Qualora l'esito di tale controllo sia dubbio, ovvero non vi siano sufficienti informazioni per poter certificare l'attribuzione della corrispondenza del nominativo del cliente/*prospect* analizzato con quello presente nelle liste, l'Unità richiede ulteriori informazioni al cliente/*prospect*, prima di procedere al completamento del censimento anagrafico.

Al termine della fase di analisi, l'operatore della Unità provvede:

---

<sup>5</sup> SANCTION (EU, ONU, OFAC), APPALTI

- se il *prospect* o il cliente non risulta essere il soggetto presente nella lista di riferimento, ad effettuare il censimento o la variazione anagrafica e terminare le proprie attività;
- se il *prospect* o il cliente risulta essere il soggetto presente nella lista di riferimento, a caricare una scheda nel Sistema gestionale, affinché la struttura preposta alla istruttoria<sup>6</sup> esegua gli approfondimenti e le valutazioni del caso.

In ogni caso, l'operatore della Unità provvede a registrare i controlli e le verifiche effettuate, mantenendo evidenza della motivazione che ha portato ad escludere o ad includere il *prospect* o il cliente in una delle liste di cui sopra.

## 7.2 FLUSSI INFORMATIVI IN USCITA

---

Il Delegato alla segnalazione di operazioni sospette comunica, con le modalità organizzative ritenute più appropriate, l'esito della propria valutazione ai dipendenti che hanno dato origine alla segnalazione.

Ferma restando la tutela della riservatezza dell'identità del soggetto di primo livello che ha effettuato la segnalazione, il Delegato alla segnalazione di operazioni sospette può consentire che i nominativi dei clienti oggetto di segnalazione di operazione sospetta siano consultabili – tramite utilizzo di apposita base informativa – dai responsabili delle diverse Strutture Operative aziendali, 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.

L'elenco dei soggetti abilitati è conservato a cura del Delegato.

La Funzione Antiriciclaggio – Unità Conformità ed Analisi AML, fornisce altresì supporto e flussi informativi ai seguenti settori/uffici.

### 6.2.1 FUNZIONE COMPLIANCE

La Funzione Antiriciclaggio informa e coinvolge tempestivamente la Funzione Compliance in tutti i casi in cui, nell'ambito dei controlli effettuati, rileva punti di debolezza nei presidi organizzativi o anomalie nei comportamenti di dipendenti e collaboratori che possano costituire una violazione delle disposizioni in materia di antiriciclaggio e finanziamento del terrorismo, nonché di altre normative applicabili alla Banca.

Infine, la Funzione Antiriciclaggio collabora con la Funzione Compliance nella evasione di eventuali istanze di vigilanza o di reclami ricevuti dalla clientela con riferimento agli aspetti legati alla normativa antiriciclaggio e finanziamento al terrorismo.

---

<sup>6</sup> Per quanto concerne le Persone Esposte Politicamente, si rinvia all'apposito Regolamento di processo.

## 7.2.2 DIREZIONE AFFARI SOCIETARI, LEGALI E CONTENZIOSO

La Funzione Antiriciclaggio inoltra, all'Ufficio Atti Giudiziari della Direzione Affari Societari, Legali e Contenzioso, eventuali richieste ricevute da parte degli Organi ispettivi o dell'Autorità Giudiziaria, fornendo supporto nella evasione delle stesse.

### **8 La normativa esterna di riferimento**

Si riportano, di seguito i principali riferimenti normativi adottati a livello comunitario e nazionale.

In ambito comunitario, le principali normative di riferimento in materia di prevenzione e contrasto del riciclaggio di denaro e del finanziamento del terrorismo si rinvencono attualmente nella Direttiva (UE) 2018/1673 del 23 ottobre 2018 sulla lotta al riciclaggio mediante il diritto penale (c.d. VI° Direttiva Antiriciclaggio) e nella 2018/843 del Parlamento Europeo e del Consiglio del 30 maggio 2018 "che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE" (c.d. V° Direttiva Antiriciclaggio) e nella Direttiva 2015/849/CE del Parlamento europeo e del Consiglio del 20/05/2015 "relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione" (c.d. IV° Direttiva Antiriciclaggio).

Si evidenzia, inoltre, il Regolamento delegato (UE) 2020/855 della Commissione del 7 maggio 2020, recante la modifica del regolamento delegato (UE) 2016 /1675, che integra la direttiva (UE) 2015/849/CE del Parlamento Europeo e del Consiglio per quanto concerne l'elenco dei Paesi terzi ad alto rischio.

Si riportano, infine, gli Orientamenti EBA - GL/2021/02 - del 1° marzo 2021, ai sensi dell'articolo 17 e dell'articolo 18, paragrafo 4, della direttiva (UE) 2015/849 sulle misure 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 («Orientamenti relativi ai fattori di rischio di ML/TF»), che abrogano e sostituiscono gli orientamenti JC/2017/37.

A livello nazionale, attualmente, la principale normativa di riferimento è rappresentata da:

- D. Lgs. 22/6/2007, n. 109 e successive modifiche ed integrazioni, recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo internazionale;
- D.Lgs. 231/2007 e successive modifiche ed integrazioni, nonché disposizioni attuative emanate dalle Autorità di Vigilanza in materia di:

- organizzazione, procedure e controlli interni;
- adeguata verifica della Clientela;
- segnalazioni aggregate (c.d. S.Ar.A.);
- conservazione e utilizzo dei dati e delle informazioni a fini antiriciclaggio;
- comunicazioni oggettive;

Completano il quadro di riferimento a livello nazionale, i decreti del Ministro dell'Economia e delle Finanze (MEF) e gli schemi rappresentativi di comportamenti anomali emanati dalla UIF.

La normativa di riferimento in materia di embarghi può essere suddivisa nelle seguenti categorie:

- normativa europea;
- normativa primaria e secondaria nazionale.

### **Normativa europea**

La principale normativa europea è contenuta nei seguenti provvedimenti:

- Regolamento 2580/2001/CE del Consiglio del 27/12/2001 che stabilisce l'obbligo di congelamento di capitali e il divieto di prestazione di servizi finanziari nei confronti di determinate persone fisiche, persone giuridiche, gruppi o entità che commettono o tentano di compiere atti di terrorismo e di persone giuridiche, gruppi o entità dalle prime controllate;
- Regolamento 881/2002/CE del Consiglio del 27/5/2002 che impone specifiche misure restrittive nei confronti di determinate persone ed entità (elencate nell'allegato al Regolamento medesimo) associate a Osama bin Laden, alla rete Al-Qaeda e ai Talebani;
- Regolamento 428/2009/CE del Consiglio del 5 maggio 2009 che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito dei prodotti a duplice uso (modificato da ultimo dal Regolamento Delegato (UE) 2018/1922 del 10 novembre 2018);
- Regolamento (UE) n. 753/2011 del Consiglio dell'1 agosto 2011, concernente ulteriori misure restrittive nei confronti di determinate persone, gruppi, imprese e entità "in considerazione della situazione in Afghanistan" e delle decisioni assunte dal "Comitato per le sanzioni" e dal "Comitato 1267" istituiti presso il Consiglio di Sicurezza delle Nazioni Unite<sup>7</sup>.

### **Normativa nazionale**

La normativa primaria italiana è contenuta nei seguenti provvedimenti:

---

<sup>7</sup> Il "Comitato delle sanzioni" è stato istituito presso il Consiglio della Sicurezza delle Nazioni Unite (CSNU) a norma del punto 30 della risoluzione 1988 (2011) del CSNU, mentre il "Comitato 1267" è stato istituito sempre presso il CSNU a norma delle risoluzioni 1267 (1999) e 1333 (2000) del Consiglio di Sicurezza delle Nazioni Unite.

- Legge n. 185/1990, come modificata dal D. Lgs. n. 105/2012 emanato in attuazione della Direttiva 2009/43/CE recante “Nuove norme sul controllo dell’esportazione, importazione e transito dei materiali di armamento”. Tale legge costituisce tuttora la base della disciplina in materia di trasferimenti di beni classificati “materiali d’armamento”;
- D. Lgs. n. 221/2017 che ha riordinato e semplificato la disciplina delle procedure di autorizzazione all’esportazione di prodotti e tecnologie a duplice uso e delle sanzioni in materia di embarghi commerciali, nonché per ogni tipologia di operazione di esportazione di materiali proliferanti. In detto decreto è confluita la disciplina in precedenza contenuta nel D. Lgs. n. 11/2007, nel D. Lgs. n. 64/2009 e nel D. Lgs. n. 96/2003, che sono stati abrogati. Il decreto prevede (artt. da 18 a 21) l’applicazione di sanzioni penali e amministrative a carico di chi effettua operazioni di esportazione di beni “*dual use*” in violazione della normativa.

Per quanto concerne la normativa secondaria, si devono considerare i Provvedimenti della Banca d’Italia già ricordati, nonché, in particolare il Provvedimento della Banca d’Italia del 27 maggio 2009 reca indicazioni operative per l’esercizio di controlli rafforzati contro il finanziamento dei programmi di proliferazione di armi di distruzione di massa.

## 9 Le policy e la normativa interna di riferimento

Si riepilogano le fonti informative interne alla Banca che presentano relazioni con il processo in esame:

- La Policy sul contrasto al riciclaggio e al finanziamento del terrorismo ha quale principale obiettivo quello di definire:
  - le regole di governo, i ruoli e le responsabilità in materia di contrasto ai rischi di riciclaggio e finanziamento del terrorismo da adottare nell’ambito del Gruppo;
  - le linee guida di Gruppo per il contrasto ai rischi di riciclaggio e finanziamento del terrorismo.

I principi richiamati nella policy trovano attuazione nella documentazione interna di dettaglio (es. regolamenti di processo, procedure operative etc.), nella quale sono meglio declinati i compiti, le attività operative e di controllo, alla base del rispetto dei principi e delle normative in tema di presidio del rischio di riciclaggio e antiterrorismo.

- il Regolamento della Funzione Antiriciclaggio, che illustra i principî guida, l’architettura organizzativa, i processi e gli strumenti adottati dalla Funzione Antiriciclaggio per adempiere ai propri compiti;
- il Regolamento del processo di adeguata verifica, in cui sono descritte le fasi dei processi di adeguata verifica, ivi compresa l’adeguata verifica rafforzata e l’adeguata

verifica semplificata, le logiche sottostanti l'attribuzione del profilo di rischio, l'adeguata verifica nel continuo;

- il Regolamento del processo dei controlli di secondo livello svolti dalla Funzione Antiriciclaggio, in cui sono descritte le fasi dei processi inerenti la tracciatura dei controlli di secondo livello in materia di AML, ivi compresi quelli relativi alla conservazione e registrazione, identificando eventuali azioni a mitigazione della rischiosità rilevata;
- il Regolamento di gestione delle Persone Esposte Politicamente (c.d. PEP), in cui sono descritte le diverse fasi del processo per la corretta gestione della clientela che rientra nelle fattispecie di Persone Esposte Politicamente come previsto dalla normativa vigente, tenuto conto altresì delle "buone prassi" richiamate nella menzionata comunicazione della Banca d'Italia, nonché richiamare ruoli e responsabilità degli attori coinvolti nel processo, in relazione all'assetto organizzativo, ai compiti e alle responsabilità;
- i manuali operativi interni alla Funzione Antiriciclaggio, che descrivono approfonditamente i processi operativi di dettaglio e gli elementi alla base dei modelli di presidio del rischio di riciclaggio e finanziamento del terrorismo;
- le procedure operative delle unità di primo livello che gestiscono l'amministrazione e la gestione concreta dei rapporti con la clientela in materia di gestione dei rischi e di prevenzione e presidio del rischio di riciclaggio e finanziamento del terrorismo.