



**Flowe S.p.A. – Società Benefit**

# **Policy di prevenzione e sul contrasto al riciclaggio e al finanziamento del terrorismo**

*Consiglio di amministrazione di Flowe S.p.A. – SB del 16 maggio 2024*

## Sommario

PREMESSA .....	4
1.1 CONTESTO DI RIFERIMENTO .....	5
1.2 AMBITO DEL DOCUMENTO .....	5
2 APPLICABILITÀ.....	6
2.1 DESTINATARI DEL DOCUMENTO.....	6
2.2 RESPONSABILITÀ DEL DOCUMENTO.....	7
3 DEFINIZIONI.....	7
3.1 RICICLAGGIO E FINANZIAMENTO DEL TERRORISMO.....	7
4 GOVERNANCE DEL MODELLO ANTIRICICLAGGIO .....	8
4.1 CONSIGLIO DI AMMINISTRAZIONE.....	10
4.2 AMMINISTRATORE DELEGATO.....	11
4.3 ESPONENTE RESPONSABILE PER L'AML.....	12
4.4 ORGANISMO DI VIGILANZA.....	13
4.5 COLLEGIO SINDACALE .....	14
4.6 FUNZIONE INTERNAL AUDIT .....	14
4.7 FUNZIONE COMPLIANCE.....	15
4.8 FUNZIONE ANTIRICICLAGGIO.....	15
4.8.1 RESPONSABILE DELLA FUNZIONE ANTIRICICLAGGIO .....	17
4.8.2 RESPONSABILE DELLA SEGNALAZIONE DI OPERAZIONI SOSPETTE .....	19
4.9 STRUTTURE DELLA BANCA CAPOGRUPPO.....	20
4.9.1 DIREZIONE AFFARI SOCIETARI, LEGALE E CONTENZIOSO .....	20
4.9.2 DIREZIONE RISORSE UMANE.....	20
4.9.3 DIREZIONE SERVICE, OPERATIONS & ICT .....	20
4.10 UNITA' BANKING SERVICES & CONTROLS.....	20
4.10.1 RESPONSABILE UNITA' BANKING SERVICES & CONTROLS .....	21
4.10 ALTRE STRUTTURE OPERATIVE.....	22
5 I PRINCIPI IN TEMA DI CONTRASTO DEL RICICLAGGIO E DEL FINANZIAMENTO DEL TERRORISMO .....	22
5.1 PROFILATURA DELLA CLIENTELA .....	22
5.2 ADEGUATA VERIFICA ORDINARIA DELLA CLIENTELA.....	25
5.2.1 PROCESSO DI <i>DIGITAL ONBOARDING</i> .....	26
5.2.2 PROCESSO EMISSIONE E GESTIONE STRUMENTI DI PAGAMENTO A SPENDIBILITA' LIMITATA.....	31
5.2.3 MOTORE DI ADEGUATA VERIFICA.....	33
5.3 ADEGUATA VERIFICA RAFFORZATA DELLA CLIENTELA .....	35

5.4	ADEGUATA VERIFICA SEMPLIFICATA DELLA CLIENTELA.....	36
5.5	ADEGUATA VERIFICA DELLA CLIENTELA ESEGUITA DA TERZI SOGGETTI .....	36
5.6	OBBLIGHI DI ASTENSIONE.....	36
5.7	CONTROLLI PER IL CONTRASTO AL FINANZIAMENTO DEL TERRORISMO.....	37
5.8	SEGNALAZIONE DI OPERAZIONE SOSPETTA.....	37
5.9	OBBLIGO DI CONSERVAZIONE DEI DOCUMENTI, DATI E INFORMAZIONI.....	38
5.9.1	ESENZIONI IN MATERIA DI CONSERVAZIONE DATI E INFORMAZIONI.....	39
5.10	FORMAZIONE DEI DIPENDENTI E COLLABORATORI .....	40
5.11	SISTEMI INTERNI DI SEGNALAZIONE DELLE VIOLAZIONI .....	40
5.12	ESERCIZIO DI AUTOVALUTAZIONE DEI RISCHI DI RICICLAGGIO.....	41
5.13	RISCHI SANZIONATORI E REPUTAZIONALI .....	41
5.14	COORDINAMENTO TRA FUNZIONE ANTIRICICLAGGIO ED ALTRE FUNZIONI DI CONTROLLO .....	42
6	NORMATIVA DI RIFERIMENTO .....	42
6.1	NORMATIVA ESTERNA .....	42
6.2	NORMATIVA INTERNA .....	45

## PREMESSA

Il riciclaggio e il finanziamento del terrorismo rappresentano fenomeni criminali che, anche in virtù della loro possibile dimensione transnazionale, costituiscono una grave minaccia per l'economia legale e possono determinare effetti destabilizzanti, soprattutto per il sistema bancario e finanziario.

La natura mutevole delle minacce del riciclaggio e del finanziamento del terrorismo, facilitata anche dalla continua evoluzione della tecnologia e dei mezzi a disposizione dei criminali, richiede un costante adattamento dei presidi di prevenzione e contrasto.

Le raccomandazioni del Gruppo d'Azione Finanziaria Internazionale (GAFI) – principale organismo internazionale di coordinamento in materia – prevedono che le autorità pubbliche e il settore privato identifichino e valutino i rischi di riciclaggio e finanziamento del terrorismo cui sono esposti, al fine di adottare adeguate misure di mitigazione.

L'azione di prevenzione e contrasto del riciclaggio si esplica attraverso l'introduzione di presidi volti a garantire la piena conoscenza del Clientela, la tracciabilità delle transazioni finanziarie e l'individuazione delle operazioni sospette.

Fermo restando l'obbligo di calibrare gli assetti organizzativi antiriciclaggio secondo il principio di proporzionalità e di approccio in base al rischio (c.d. *Risk Based Approach*), le Disposizioni della Banca d'Italia in materia di Organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo, prevedono che i destinatari adottino almeno i seguenti presidi organizzativi minimi:

- a) attribuiscono a una funzione di controllo aziendale la responsabilità di assicurare l'adeguatezza, la funzionalità e l'affidabilità dei presidi antiriciclaggio;
- b) formalizzano l'attribuzione della responsabilità per la segnalazione delle operazioni sospette;
- c) attribuiscono a una funzione di controllo aziendale il compito di verificare in modo continuativo il grado di adeguatezza dell'assetto organizzativo antiriciclaggio e la sua conformità rispetto alla disciplina (funzione di internal auditing);
- d) nominano un Esponente aziendale quale Responsabile per l'Antiriciclaggio (di seguito anche Esponente Responsabile per l'AML).

Flowe S.p.A. – Società Benefit (di seguito la Società) è fortemente impegnata nell'evitare che i prodotti e i servizi offerti siano utilizzati per finalità criminali di riciclaggio e di finanziamento del terrorismo, promuovendo al loro interno una cultura improntata al pieno rispetto delle disposizioni vigenti e all'efficace assolvimento degli obblighi di collaborazione passiva, finalizzata a garantire la conoscenza approfondita della Clientela e la conservazione dei documenti relativi alle transazioni effettuate, e di collaborazione attiva volta all'individuazione e segnalazione delle operazioni sospette di riciclaggio.

In particolare, nell'ambito delle attività Benefit, la Società ambisce all'educazione e alla diffusione nei confronti dei giovani e delle diverse componenti sociali dei principi della sostenibilità e dell'innovazione, nonché a promuovere la cultura del benessere sociale ed economico, educando le nuove generazioni alla consapevolezza dei propri comportamenti di spesa e pertanto all'efficace gestione delle proprie risorse economiche, tramite materiali informativi, l'utilizzo delle tecnologie digitali e/o attraverso l'organizzazione di iniziative quali convegni e seminari.

Inoltre la Società promuove attivamente una mission di educational nei confronti della propria Clientela per quanto attiene il potenziale rischio a cui sono assoggettati stante le nuove frontiere delle frodi e truffe legate al mondo delle nuove tecnologie tramite soluzioni tecnologiche innovative che garantiscono affidabilità, tracciabilità di tutte le operazioni e replica geografica dati in *real time*, grazie all'utilizzo del *Cloud* e *Artificial Intelligence*.

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 e potenzialmente i propri Clienti.

L'Amministratore Delegato appronta le procedure necessarie per dare attuazione a tali politiche.

L'Esponente Responsabile per l'AML assicura che il Consiglio di Amministrazione disponga delle informazioni necessarie per comprendere pienamente la rilevanza dei rischi di riciclaggio cui la Società è esposta e sia tempestivamente informato delle decisioni che possono incidere sull'esposizione a tale rischio.

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. La Funzione 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.

L'Esponente Responsabile per l'AML funge da raccordo tra il Responsabile Antiriciclaggio e il Consiglio di Amministrazione.

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, stante anche l'assetto della Società, nell'ambito del processo di *onboarding* della Clientela (sia esso derivante da linee di *business* B2B o B2B2C) e nella verifica costante delle transazioni da questa realizzata. Le strutture impegnate in tali processi sono, quindi, le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi.

Nell'ottica di assicurare un'efficace prevenzione dei rischi di non conformità alla normativa, è inoltre fondamentale che le diverse strutture aziendali assicurino, in caso di offerta di prodotti e servizi nuovi, il tempestivo coinvolgimento della Funzione Antiriciclaggio della Società affinché quest'ultima possa effettuare in via preventiva le proprie valutazioni in termini di copertura dei possibili rischi connessi in materia di prevenzione al riciclaggio e finanziamento del terrorismo.

## 1.1 CONTESTO DI RIFERIMENTO

Le "Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo" emanate dalla Banca d'Italia con provvedimento del 26 marzo 2019, e successivamente modificate con provvedimento del 1° agosto 2023, (in seguito anche "**Disposizioni**") prevedono l'obbligo, per gli organi aziendali di ciascun destinatario, di definire e approvare una policy motivata che indichi le scelte del destinatario medesimo in concreto adottate in materia di assetti organizzativi, procedure e controlli interni, adeguata verifica e conservazione dei dati.

Al fine di adempiere compiutamente alle Disposizioni – emanate dall'Autorità di vigilanza ai sensi dell'art. 7 del Decreto Legislativo 21 novembre 2007, n. 231, (in seguito anche "**Decreto Antiriciclaggio**") – la Società ha adottato la presente policy (in seguito anche "**Policy**").

In particolare, la strategia della Società è attualmente orientata all'offerta di prodotti e servizi mediante identificazione tramite riconoscimento biometrico da parte di Clienti, residenti in Italia con canale distributivo esclusivamente tramite mobile App.

La presente Policy si inserisce nel più ampio sistema dei controlli interni della Società volti a garantire il rispetto della normativa vigente e costituisce il documento base dell'intero sistema dei presidi antiriciclaggio e antiterrorismo della Società stessa.

Nel predisporre la presente Policy, la Società ha tenuto in considerazione anche gli esiti dell'esercizio annuale di autovalutazione del Rischio di riciclaggio; i futuri aggiornamenti della Policy dovranno, parimenti, tenere conto degli esiti dell'autovalutazione annuale, tempo per tempo svolta.

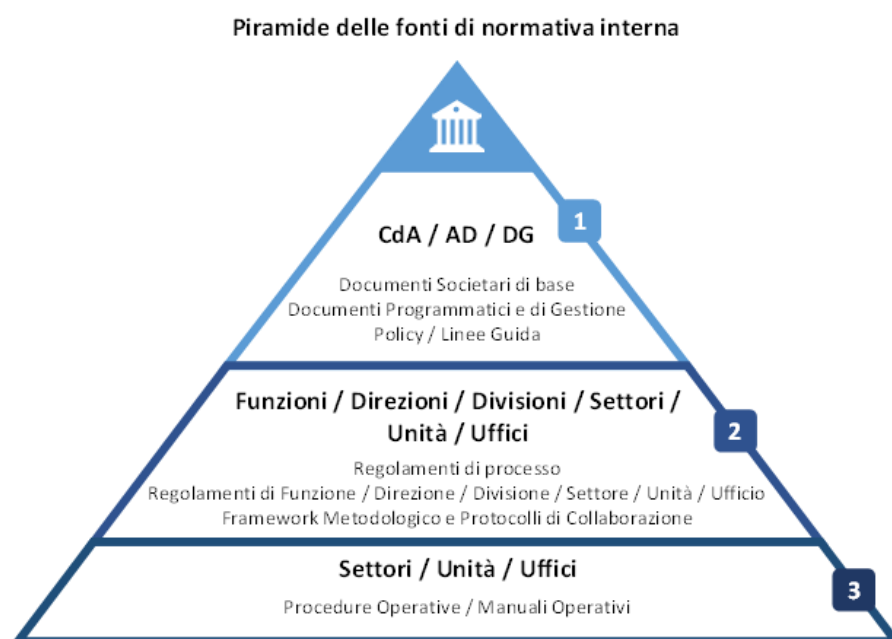
## 1.2 AMBITO DEL DOCUMENTO

I principi richiamati nella presente Policy trovano attuazione nei regolamenti di processo e/o nelle procedure operative, all'interno delle quali saranno meglio declinati i compiti, le attività operative e di controllo, alla base del rispetto degli adempimenti relativi alle normative.

Tali regolamenti e procedure descriveranno più nel dettaglio i presidi per il contrasto al riciclaggio e al finanziamento del terrorismo e gli attori coinvolti, i loro ruoli e le responsabilità all'interno di Flowe.

I principi richiamati nella presente 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, nel rispetto dei principi e delle normative in tema di presidio del rischio di riciclaggio e antiterrorismo. Si fa riferimento, in particolare, ai Regolamenti di processo – predisposti e aggiornati a cura della Funzione Antiriciclaggio – in materia di Adeguata Verifica, Segnalazione Operazioni Sospette e Conservazione e Controlli svolti dalla Funzione Antiriciclaggio, che, nel loro complesso, definiscono dettagliatamente responsabilità, compiti e modalità operative nella gestione del rischio di riciclaggio, costituendo il cosiddetto “Manuale Antiriciclaggio”.

Con riferimento alla “Policy di Gruppo sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna”, il presente documento si colloca al livello di vertice della piramide documentale richiamata nello schema seguente.



## 2. APPLICABILITÀ

### 2.1 DESTINATARI DEL DOCUMENTO

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

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

## 2.2 RESPONSABILITÀ DEL DOCUMENTO

La Policy è approvata dal Consiglio di Amministrazione della Società, che approverà altresì eventuali modifiche e/o aggiornamenti della stessa.

L'Amministratore Delegato definisce la Policy sottoposta all'approvazione del Consiglio di Amministrazione e ne cura l'attuazione.

L'Esponente Responsabile per l'Antiriciclaggio monitora che la medesima sia adeguata e proporzionata, tenendo conto delle caratteristiche della Società e dei rischi cui essa è esposta.

La Funzione Antiriciclaggio concorre all'aggiornamento e alla revisione periodica della presente Policy.

## 3 DEFINIZIONI

Per quanto attiene le "definizioni" e la terminologia contenute nel presente documento si fa specifico richiamo alle definizioni – aggiornate tempo per tempo – contenute nel Decreto Antiriciclaggio, nelle disposizioni attuative emesse dalle Autorità preposte, nonché dagli Orientamenti EBA pubblicati.

### 3.1 RICICLAGGIO E FINANZIAMENTO DEL TERRORISMO

La definizione di riciclaggio adottata – a fini di prevenzione – dal disposto normativo in vigore recepisce quella contenuta nella direttiva comunitaria ed è più ampia rispetto alla fattispecie delineata dal codice penale negli articoli 648bis e 648ter. Per il sistema penale, infatti, il reato di riciclaggio non si applica a chi ha commesso il reato presupposto: l'uso e l'occultamento dei proventi criminosi da parte delle persone che hanno commesso il reato che ha generato tali proventi (cd. "autoriciclaggio") sono considerati, infatti, come *post factum* non punibile.

La definizione di «riciclaggio», ai sensi dell'articolo 2, comma 4, del decreto antiriciclaggio:

- a) la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni;
- b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
- c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
- d) la partecipazione a uno degli atti previsti dalle lettere precedenti, l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolare l'esecuzione;
- e) Il riciclaggio è considerato tale anche se le attività che hanno generato i beni da riciclare si sono svolte fuori dai confini nazionali.

Il riciclaggio è considerato tale anche se le attività che hanno generato i beni da riciclare si sono svolte fuori dai confini nazionali.

Il riciclaggio è solitamente rappresentato come un processo in tre stadi:

introduzione ( <i>placement</i> ):	i proventi da reato, anche non colposo, mediante una serie di operazioni, vengono raccolti e collocati presso istituzioni finanziarie e/o non finanziarie;
stratificazione ( <i>layering</i> ):	è attuato mediante il compimento di una serie di operazioni finanziarie complesse, anche apparentemente non collegate tra di loro, dirette ad ostacolare la ricostruzione dei flussi finanziari;
impiego ( <i>integration</i> ):	si riutilizzano i proventi delle attività criminali nell'economia legale, in modo tale da apparire formalmente di origine legale.



I tre stadi non sono statici e possono sovrapporsi: l'utilizzo delle istituzioni finanziarie per finalità criminali può avvenire in uno qualunque degli stadi sopra descritti.

Per «finanziamento del terrorismo» si intende, in conformità con l'art. 1, comma 1, lettera d), del decreto legislativo 22 giugno 2007, n. 109: *“qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi e risorse economiche, in qualunque modo realizzata, destinati ad essere, direttamente o indirettamente, in tutto o in parte, utilizzati per il compimento di una o più condotte con finalità di terrorismo, secondo quanto previsto dalle leggi penali, ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette”*.

Il Ministro dell'Economia e delle Finanze su proposta del Comitato di sicurezza finanziaria dispone, con proprio decreto, il congelamento dei fondi e delle risorse economiche detenuti, anche per interposta persona fisica o giuridica, da persone fisiche, giuridiche, gruppi o entità, designati, secondo i criteri e le procedure stabiliti dalle medesime risoluzioni, dal consiglio di Sicurezza delle Nazioni Unite o da un suo Comitato.

Nelle more dell'adozione dei provvedimenti di designazione disposti dalle Nazioni Unite e nel rispetto degli obblighi sanciti dal Consiglio di sicurezza delle Nazioni Unite e delle specifiche misure restrittive disposte dall'Unione europea nonché dalle iniziative assunte dall'autorità giudiziaria in sede penale, il Ministro dell'economia e delle Finanze, su proposta del Comitato di sicurezza finanziaria, dispone con proprio decreto, per un periodo di sei mesi, rinnovabili nelle stesse forme sino a quando ne permangano le condizioni, il congelamento dei fondi e delle risorse economiche detenuti (c.d. misure di congelamento nazionali), anche per interposta persona fisica o giuridica, da persone fisiche, giuridiche, gruppi o entità, che pongono in essere o tentano di porre in essere una o più condotte con finalità di terrorismo, secondo quanto previsto dalle leggi penali, o volte al finanziamento dei programmi di proliferazione delle armi di distruzione di massa o che minacciano la pace e la sicurezza nazionale.

I Fondi e le Risorse economiche sottoposte a congelamento non possono costituire oggetto di alcun atto di trasferimento, disposizione o utilizzo.

Il congelamento dei “fondi” e/o delle “risorse economiche” (c.d. embargo/sanzione finanziario/a) avviene nei confronti dei presunti terroristi (“soggetti designati”, ovvero “le persone fisiche, le persone giuridiche, i gruppi e le entità designati come destinatari del congelamento sulla base dei regolamenti comunitari e della normativa nazionale”), imponendo agli Intermediari Finanziari di inibire qualsiasi atto di movimentazione e/o trasferimento, nonché ogni atto di disposizione, la vendita, la locazione, l'affitto, la costituzione di diritti reali di garanzia o anche l'accesso in modo da modificarne il volume, l'importo la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consenta l'uso dei fondi, compresa la gestione di portafoglio.

Il congelamento o “embargo finanziario” si differenzia dal cosiddetto “embargo commerciale” legato al divieto di commercio e di scambio con Paesi sanzionati, al fine di isolare e mettere i loro governi in una difficile situazione politica ed economica interna.

## 4 ATTORI COINVOLTI

Il modello di contrasto ai rischi di riciclaggio e finanziamento del terrorismo è gestito, a livello di Gruppo, mediante uno specifico processo finalizzato ad implementare e mantenere regole, procedure e strutture organizzative funzionali ad assicurare la prevenzione e la gestione dei rischi in questione, da parte di tutte le società del Gruppo.

Il modello prevede che la responsabilità primaria in materia di presidio dei rischi di riciclaggio e finanziamento del terrorismo sia rimessa agli Organi Aziendali di ogni società del Gruppo, ciascuno secondo le rispettive competenze ed in conformità agli indirizzi della Capogruppo. L'articolazione dei



compiti e delle responsabilità in materia di antiriciclaggio da parte degli organi e delle funzioni aziendali deve essere chiaramente definita in ogni società.

Coerentemente con i principi di governo societario ammessi, il modello riconosce, per ogni società del Gruppo, la centralità del Consiglio di Amministrazione per quanto attiene alle politiche di governo dei rischi in questione: ad esso spetta l'approvazione della *policy* antiriciclaggio prevista dalle Disposizioni (in linea con i principi della presente Policy) e la responsabilità dell'adozione di un sistema adeguato alle caratteristiche dell'impresa; a tal proposito, si organizza in modo tale da poter affrontare la tematica dei rischi di riciclaggio e finanziamento del terrorismo con la dovuta attenzione ed il necessario livello di approfondimento.

L'Organo con funzione di gestione cura l'attuazione degli indirizzi strategici e delle politiche di governo del rischio di riciclaggio approvati dall'organo con funzione di supervisione strategica ed è responsabile per l'adozione di tutti gli interventi necessari ad assicurare l'efficacia dell'organizzazione e del sistema dei controlli antiriciclaggio.

L'Organo con funzione di controllo, nel quadro della responsabilità di vigilare sulla osservanza della normativa e sulla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni in materia antiriciclaggio, mantiene un costante raccordo anche con la Funzione Antiriciclaggio.

In conformità al principio di proporzionalità e ove previsto dalle specifiche normative di riferimento, ciascuna società del Gruppo istituisce un'apposita Funzione Antiriciclaggio, deputata a prevenire e contrastare la realizzazione di operazioni di riciclaggio.

Al fine di realizzare opportune sinergie ed economie di scala, sfruttando centri di competenza altamente specializzati, le società del Gruppo Bancario e quelle del Gruppo Assicurativo possono delegare alla Capogruppo – sulla base di appositi accordi di *outsourcing*, redatti nel rispetto della regolamentazione di vigilanza nonché in conformità ai principi sanciti all'interno della "Politica aziendale in materia di esternalizzazione" – attività proprie della funzione antiriciclaggio ai sensi della vigente normativa e/o lo svolgimento di specifici obblighi previsti dalla medesima normativa.

Nei predetti accordi devono essere regolati almeno i seguenti aspetti:

- gli obiettivi della funzione e il contenuto delle attività esternalizzate;
- i livelli di servizio attesi;
- la frequenza minima dei flussi informativi;
- gli obblighi di riservatezza delle informazioni acquisite nell'esercizio della funzione o delle attività;
- la possibilità di rivedere le condizioni del servizio al verificarsi di modifiche nell'operatività e nell'organizzazione della Società.

Le società del Gruppo nominano un proprio responsabile della funzione antiriciclaggio ed un proprio delegato alla segnalazione delle operazioni sospette, in linea con i principi stabiliti nella presente Policy (come *infra* definito).

In un'ottica di Gruppo, riveste un'importanza cruciale una buona organizzazione dei lavori e la circolazione delle informazioni, in modo che le questioni intersocietarie connesse alle disposizioni in materia di antiriciclaggio e contrasto al finanziamento del terrorismo siano discusse con il supporto di un adeguato lavoro istruttorio, le cui risultanze sono anche sottoposte al Comitato Rischi della Capogruppo.

Nell'ambito dell'attività di indirizzo e coordinamento di gruppo, gli Organi aziendali della Banca (in qualità di Capogruppo) adottano gli indirizzi strategici in materia di gestione del Rischio di riciclaggio e controlli antiriciclaggio. La Capogruppo assicura che gli Organi aziendali delle altre società appartenenti al Gruppo attuino, nella propria realtà aziendale, le strategie e le politiche di Gruppo.

Al fine di perseguire la piena e concreta attuazione del modello di Gruppo, le controllate in perimetro adottano una *policy* coerente con i principi e le linee guida contenute nella presente Policy, secondo un principio di proporzionalità e in base alle specificità della propria attività.

Ai sensi delle Disposizioni vigenti, al fine di accrescere l'omogeneità delle valutazioni effettuate sulla Clientela comune alle entità di un gruppo e di accrescere la capacità dello stesso di prevenire e gestire i rischi di riciclaggio, la Capogruppo è tenuta ad istituire – mediante la creazione di apposito registro centralizzato – una base informativa comune che consenta a tutte le società appartenenti al gruppo di valutare in modo omogeneo la Clientela.

In attuazione di quanto precede, sulla base del principio dell'approccio basato sul rischio, la Banca istituisce una base informativa comune per tutte le società dalla medesima controllate (direttamente o indirettamente) nel cui ambito sono condivise e mantenute opportunamente aggiornate informazioni concernenti la Clientela ad alto rischio di riciclaggio (a titolo esemplificativo, Clienti oggetto di precedente segnalazione alla UIF).

La Funzione Antiriciclaggio individua ulteriori tipologie di informazioni che potranno essere condivise laddove sussistano rapporti di collocamento/distribuzione (o altra relazione d'affari rilevante) tra la Capogruppo e le singole società controllate (ovvero tra queste ultime).

La Capogruppo adotta adeguate misure tecniche e organizzative per garantire che i dati contenuti nella base informativa comune siano trattati nel rispetto della vigente normativa nazionale in materia di protezione dei dati personali.

Le Funzioni Antiriciclaggio delle società controllate attivano appositi flussi informativi periodici verso la capogruppo, aventi ad oggetto le principali attività svolte, gli esiti dei controlli effettuati e le principali iniziative intraprese per rimuovere le disfunzioni accertate.

Il Responsabile Antiriciclaggio di Gruppo è in ogni caso informato tempestivamente degli esiti delle attività di controllo effettuate presso le società appartenenti al Conglomerato finanziario, nonché di ogni accadimento di rilievo.

Il modello di contrasto al riciclaggio e al finanziamento del terrorismo adottato dalla Società prevede, pertanto, il coinvolgimento delle strutture organizzative, secondo l'articolazione di ruoli e responsabilità di seguito riportata.

#### 4.1 CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione:

- approva e riesamina periodicamente gli indirizzi strategici e le politiche di governo dei rischi connessi con il riciclaggio e con il finanziamento del terrorismo;
- approva la presente Policy ed è responsabile del riesame periodico della stessa, al fine di assicurarne l'efficacia nel tempo;
- approva l'istituzione della Funzione Antiriciclaggio individuandone compiti e responsabilità nonché modalità di coordinamento e di collaborazione con le altre Funzioni Aziendali di Controllo;
- approva le linee di indirizzo di un sistema dei controlli interni organico e coordinato, funzionale alla pronta rilevazione ed alla gestione del rischio di riciclaggio e di finanziamento del terrorismo e provvede al suo riesame periodico al fine di assicurarne l'efficacia nel tempo;
- approva i principi per la gestione dei rapporti con la Clientela classificata ad "alto rischio";
- assicura nel continuo che i compiti e le responsabilità in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo siano allocati in modo chiaro e appropriato, garantendo che le funzioni operative e quelle di controllo siano distinte e che le funzioni medesime siano fornite di risorse qualitativamente e quantitativamente adeguate;
- assicura che sia approntato un sistema di flussi informativi adeguato, completo e tempestivo verso gli Organi aziendali e tra le funzioni di controllo;
- assicura che le carenze e le anomalie riscontrate in esito ai controlli di vario livello siano portate tempestivamente a sua conoscenza e promuove l'adozione di idonee misure correttive, delle quali valuta l'efficacia;

- nomina l'Esponente Responsabile per l'AML e assicura che il medesimo soddisfi le condizioni previste dalle Disposizioni;
- assicura che l'Esponente Responsabile per l'AML sia tempestivamente informato delle decisioni che possono incidere sull'esposizione al Rischio di riciclaggio della Società;
- assicura la tutela della riservatezza nell'ambito della procedura di segnalazione di operazioni sospette;
- esamina, con cadenza almeno annuale, la relazione del Responsabile della Funzione Antiriciclaggio sulle attività di verifica svolte, sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale e dei componenti la rete di vendita nonché sulle comunicazioni inoltrate dal Collegio Sindacale e/o dall'Organismo di Vigilanza; nel caso in cui dette comunicazioni si riferiscano a infrazioni considerate rilevanti, ne viene data informativa anche alla prima riunione utile da parte del Responsabile della Funzione Antiriciclaggio;
- esamina, con cadenza almeno annuale, il documento sui risultati dell'autovalutazione dei rischi di riciclaggio condotta dalla Funzione Antiriciclaggio;
- valuta i rischi conseguenti all'operatività con paesi terzi associati a più elevati rischi di riciclaggio e individua i presidi per attenuarli, di cui monitora l'efficacia;
- sentito il Collegio Sindacale, nomina e revoca il Responsabile della Funzione Antiriciclaggio e il Delegato alla Segnalazione di Operazioni Sospette;
- definisce e approva i criteri per il coordinamento e la direzione delle società del Gruppo, nonché la determinazione dei criteri per l'esecuzione delle istruzioni della Banca d'Italia.

## 4.2 AMMINISTRATORE DELEGATO

L'Amministratore Delegato:

- cura l'attuazione degli indirizzi strategici e delle politiche di governo del Rischio di riciclaggio approvati dal Consiglio di Amministrazione ed è responsabile per l'adozione di tutti gli interventi misure necessarie ad assicurare l'efficacia dell'organizzazione e del sistema dei controlli antiriciclaggio;
- ai fini di quanto sopra, esamina le proposte di interventi organizzativi e procedurali presentate dal Responsabile della Funzione Antiriciclaggio e formalizza, motivandola, l'eventuale decisione di non accoglierle;
- garantisce una comunicazione periodica al Consiglio di Amministrazione circa le attività svolte dal Responsabile della Funzione Antiriciclaggio nonché la trasmissione al medesimo Organo di informazioni e dati sufficientemente esaurienti e tempestivi sui rischi in materia di riciclaggio e finanziamento del terrorismo;
- informa il Consiglio di Amministrazione in merito a eventuali violazioni gravi o significative in materia di riciclaggio e finanziamento del terrorismo e raccomanda le relative azioni correttive;
- garantisce che il Responsabile della Funzione Antiriciclaggio (i) abbia accesso diretto a tutte le informazioni necessarie per l'adempimento dei propri compiti, (ii) disponga di risorse umane e tecniche e di strumenti sufficienti per poter assolvere adeguatamente i compiti che gli sono stati assegnati e (iii) sia informato sugli incidenti e sulle carenze individuati dai sistemi di controllo interno e dalle autorità di vigilanza;
- tiene conto, nella predisposizione delle procedure operative, delle indicazioni e delle linee guida emanate dalle autorità competenti e dagli organismi internazionali;
- definisce e cura l'attuazione di un sistema di controlli interni funzionale alla pronta rilevazione e alla gestione del Rischio di riciclaggio e ne assicura l'efficacia nel tempo, in coerenza con gli esiti dell'esercizio di autovalutazione dei rischi;
- assicura che le procedure operative e i sistemi informativi consentano il corretto adempimento degli obblighi di adeguata verifica della Clientela e di conservazione dei documenti e delle informazioni;
- in materia di segnalazione di operazioni sospette, definisce e cura l'attuazione di una procedura adeguata alle specificità dell'attività, alle dimensioni e alle complessità della Banca, secondo il principio di proporzionalità e l'approccio basato sul rischio; tale procedura è in grado di garantire certezza di riferimento, omogeneità nei comportamenti, applicazione generalizzata all'intera struttura, il pieno utilizzo delle informazioni rilevanti e la ricostruibilità dell'iter valutativo;
- con riferimento al medesimo tema, adotta misure volte ad assicurare il rispetto dei requisiti di riservatezza della procedura di segnalazione nonché strumenti, anche informatici, per la rilevazione delle operazioni anomale;

- definisce e cura l'attuazione delle iniziative e delle procedure necessarie per assicurare il tempestivo assolvimento degli obblighi di comunicazione alle Autorità previsti dalla normativa antiriciclaggio;
- definisce la presente Policy e ne cura l'attuazione;
- definisce e cura l'attuazione di procedure informative volte ad assicurare la conoscenza dei fattori di rischio a tutte le strutture aziendali coinvolte e agli organi incaricati di funzioni di controllo;
- definisce e cura l'attuazione delle procedure di gestione dei rapporti con la Clientela classificata ad "alto rischio", in coerenza con i principi fissati dal Consiglio di Amministrazione;
- stabilisce i programmi di addestramento e formazione del personale sugli obblighi previsti dalla disciplina antiriciclaggio; l'attività di formazione riveste carattere di continuità e sistematicità e tiene conto dell'evoluzione della normativa e delle procedure predisposte dalla Società;
- stabilisce gli strumenti idonei a consentire la verifica dell'attività svolta dal personale in modo da rilevare eventuali anomalie che emergano, segnatamente, nei comportamenti, nella qualità delle comunicazioni indirizzate ai referenti e alle strutture aziendali nonché nei rapporti del personale con la Clientela;
- assicura, nei casi di esternalizzazione dei compiti operativi della Funzione Antiriciclaggio, il rispetto della normativa applicabile e riceve periodiche informazioni sullo svolgimento delle attività esternalizzate.
- assicura, nei casi di operatività a distanza (es., effettuata attraverso canali digitali), l'adozione di specifiche procedure informatiche per il rispetto della normativa antiriciclaggio, con particolare riferimento all'individuazione automatica di operazioni anomale.

#### 4.3 ESPONENTE RESPONSABILE PER L'AML

La Società conferisce l'incarico di Esponente Responsabile per l'AML della stessa Società ad un soggetto individuato, dotato dei necessari requisiti.

Prima della nomina, il Consiglio di Amministrazione accerta l'esistenza in capo al candidato alla carica di Esponente Responsabile per l'AML di eventuali conflitti di interesse e l'idoneità delle misure adottate per prevenirli e/o gestirli. A tal fine, il Consiglio di Amministrazione considera – quantomeno – le seguenti ipotesi di conflitto e le relative misure rimediale:

- deleghe su aree operative oggetto di verifica da parte del Responsabile della Funzione Antiriciclaggio;
- diretto coinvolgimento in operazioni che formino oggetto di scrutinio da parte della Funzione Antiriciclaggio;
- eventuali rapporti di parentela o affinità con il Responsabile Antiriciclaggio o con il personale della Funzione Antiriciclaggio della Banca capogruppo;
- deleghe in merito alla gestione delle risorse umane e tecniche della Funzione Antiriciclaggio;
- deleghe in merito alla predisposizione ed approvazione delle politiche, procedure e misure di controllo interno in materia AML.

La Società adotta apposite misure organizzative, da valutarsi caso per caso, al fine di mitigare eventuali conflitti di interessi connessi al conferimento dell'incarico di Esponente Responsabile per l'AML; al riguardo, la Società può adottare una o più delle seguenti misure:

- rimodulazione delle deleghe/competenze dell'Esponente Responsabile per l'AML;
- obbligo per l'Esponente Responsabile per l'AML di riferire in Consiglio su eventuali situazioni di conflitto;
- possibilità per il Responsabile Antiriciclaggio di riferire direttamente al Consiglio di Amministrazione;
- predisposizione di report periodici del Responsabile Antiriciclaggio direttamente a beneficio del Consiglio di Amministrazione.

Per ciò che attiene ai profili di competenza, l'Esponente Responsabile per l'AML deve essere in possesso di approfondite conoscenze teoriche o pratiche nei seguenti ambiti:

- rischi di riciclaggio, politiche, controlli e procedure AML nonché modello di business della Banca e del settore in cui la medesima opera;
- gestione dei rischi (individuazione, valutazione, monitoraggio, controllo e mitigazione delle principali tipologie di rischio della Società);
- sistemi di controllo interno.

L'Esponente Responsabile per l'AML deve inoltre prendere parte ad attività di *induction* in materia AML su base periodica.

In considerazione del fatto che l'incarico di Esponente Responsabile per l'AML ha natura esecutiva, per gli amministratori che non svolgano già incarichi di natura esecutiva, il Consiglio di Amministrazione verifica il possesso in capo a tale esponente dei requisiti e dei criteri di idoneità previsti per gli amministratori con incarichi esecutivi.

L'Esponente Responsabile per l'AML costituisce il principale punto di contatto tra il Responsabile Antiriciclaggio e il Consiglio di Amministrazione e assicura che quest'ultimo disponga delle informazioni necessarie per comprendere pienamente la rilevanza dei rischi di riciclaggio cui la Società e il Gruppo sono esposti.

L'Esponente Responsabile per l'AML:

- monitora che le politiche, le procedure e le misure di controllo interno in materia di antiriciclaggio siano adeguate e proporzionate, tenendo conto delle caratteristiche della Società e dei rischi cui essa è esposta;
- coadiuva il Consiglio di Amministrazione nelle valutazioni concernenti l'articolazione organizzativa e la dotazione di risorse della Funzione Antiriciclaggio;
- assicura che gli Organi aziendali siano periodicamente informati in merito alle attività svolte dal Responsabile Antiriciclaggio nonché in merito alle interlocuzioni intercorse con le Autorità;
- informa gli Organi aziendali delle violazioni e criticità concernenti l'antiriciclaggio di cui sia venuto a conoscenza e raccomanda le opportune azioni;
- verifica che il Responsabile Antiriciclaggio abbia accesso diretto a tutte le informazioni necessarie per l'adempimento dei propri compiti, disponga di risorse umane e tecniche e di strumenti sufficienti e sia informato su eventuali carenze relative all'antiriciclaggio individuate dalle altre funzioni di controllo interno e dalle Autorità di vigilanza;
- assicura che le problematiche e le proposte di intervento rappresentate dal Responsabile Antiriciclaggio siano valutate dagli Organi aziendali.

L'Esponente Responsabile per l'AML verifica altresì l'adeguatezza e la completezza delle informazioni e dei dati comunicati dal Responsabile Antiriciclaggio agli Organi aziendali nell'ambito delle proprie relazioni. A tal fine, le relazioni del Responsabile della Funzione Antiriciclaggio vengono trasmesse con congruo preavviso anticipato all'Esponente Responsabile per l'AML.

L'Esponente Responsabile per l'AML e la Funzione di Internal Audit adottano flussi informativi reciproci e si confrontano periodicamente (con frequenza almeno annuale nell'ambito di apposite riunioni).

#### 4.4 ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza contribuisce in via preventiva alla definizione del Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. n. 231/2001 e monitora nel continuo il rispetto dei processi ivi previsti. Nel caso in cui un reato presupposto sia comunque commesso, ne analizza le cause per individuare le misure correttive più idonee. Per lo svolgimento di tali attività, l'Organismo di Vigilanza riceve idonei flussi informativi dalle diverse funzioni aziendali e può accedere senza limitazioni a tutte le informazioni rilevanti ai fini dell'assolvimento dei propri compiti.

L'Organismo di Vigilanza, infine, inoltra al Delegato alle segnalazioni di operazioni sospette eventuali segnalazioni di operazioni sospette rilevate in modo autonomo nell'esercizio dei propri compiti.

#### 4.5 COLLEGIO SINDACALE

Con specifico riferimento al presidio del rischio di riciclaggio e di finanziamento del terrorismo, il Collegio Sindacale:

- vigila sull'osservanza della normativa e sulla completezza, funzionalità ed adeguatezza dei controlli antiriciclaggio, avvalendosi delle strutture interne per lo svolgimento delle verifiche e degli accertamenti necessari ed utilizzando i flussi informativi provenienti dagli altri Organi aziendali, dal Responsabile della Funzione Antiriciclaggio e dalle altre Funzioni aziendali di controllo. In tale ambito:
  - valuta con particolare attenzione l'idoneità delle procedure in essere per l'adeguata verifica della Clientela, la conservazione delle informazioni e per la segnalazione delle operazioni sospette;
  - analizza i motivi delle carenze, anomalie e irregolarità riscontrate e promuove l'adozione delle opportune misure correttive;
- esprime il proprio parere in ordine alla nomina e alla revoca del Responsabile della Funzione Antiriciclaggio e del Delegato alla Segnalazione di Operazioni Sospette;
- viene sentito in merito alla definizione degli elementi dell'architettura complessiva del sistema di gestione e controllo del rischio di riciclaggio e di finanziamento del terrorismo;
- vigila sull'osservanza delle norme contenute nel Decreto, nell'ambito delle proprie attribuzioni e competenze;
- comunica senza ritardo alla Banca d'Italia tutti i fatti di cui venga a conoscenza nell'esercizio delle proprie funzioni che possano integrare violazioni gravi o ripetute o sistematiche o plurime delle disposizioni di legge applicabili e delle relative disposizioni attuative;
- inoltra, al Delegato alla Segnalazione di Operazioni Sospette, eventuali segnalazioni di operazioni rilevate in modo autonomo nell'esercizio dei propri compiti.

#### 4.6 FUNZIONE INTERNAL AUDIT

La Funzione Internal Audit della Società verifica in modo continuativo, secondo un approccio *risk based*, 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.

Con specifico riferimento alle disposizioni in materia di prevenzione e contrasto dell'utilizzo del sistema finanziario per finalità di riciclaggio e di finanziamento del terrorismo, la Funzione Internal Audit verifica:

- il costante rispetto dell'obbligo di adeguata verifica, sia nella fase di instaurazione del rapporto che nello svilupparsi nel tempo della relazione;
- l'effettiva acquisizione e l'ordinata conservazione dei dati e documenti prescritti dalla normativa;
- il corretto funzionamento del sistema di conservazione e l'allineamento tra le varie procedure contabili settoriali di gestione e quella di alimentazione e gestione del sistema medesimo;
- l'effettivo grado di coinvolgimento del personale dipendente e dei collaboratori nonché dei responsabili delle strutture centrali e periferiche, nell'attuazione dell'obbligo della "collaborazione attiva".

La Funzione Internal Audit è responsabile del processo di *whistleblowing*, al cui interno la Società ha identificato il Responsabile del Sistema Interno di segnalazioni (in seguito anche "Responsabile *Whistleblowing*" o "Responsabile WB"), nominato ad personam dal Consiglio di Amministrazione.

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



La Funzione riporta, almeno annualmente, agli Organi aziendali compiute informazioni sull'attività svolta e sui relativi esiti, fermo restando il rispetto del principio di riservatezza in materia di segnalazioni di operazioni sospette.

#### 4.7 FUNZIONE COMPLIANCE

La Funzione Compliance presiede la gestione dei rischi di non conformità alle norme, secondo un approccio *risk based*, con riguardo a tutta l'attività aziendale, ad esclusione degli ambiti normativi demandati *ex lege* alle altre Funzioni di Controllo.

Si avvale, per il presidio di determinati ambiti normativi per cui sono previste forme di presidio specializzato, di unità specialistiche appositamente individuate nella Policy di Compliance di Gruppo, cui sono attribuite determinate fasi del processo di compliance.

#### 4.8 FUNZIONE ANTIRICICLAGGIO

La Funzione Antiriciclaggio è responsabile, secondo un approccio *risk based*, del presidio del rischio di riciclaggio e finanziamento al terrorismo e degli adeguamenti dei processi all'evoluzione del contesto normativo e procedurale in tale ambito.

Verifica, nel continuo, che le procedure aziendali siano coerenti con l'obiettivo di prevenire e contrastare la violazione di norme di eteroregolamentazione (leggi e norme regolamentari) e di autoregolamentazione in materia di riciclaggio e finanziamento del terrorismo.

Pone particolare attenzione: all'adeguatezza dei sistemi e delle procedure interne in materia di adeguata verifica della Clientela e di conservazione, nonché dei sistemi di rilevazione, valutazione e segnalazione di operazioni sospette; all'efficace rilevazione delle altre situazioni oggetto di obbligo di comunicazione nonché all'appropriata conservazione della documentazione e delle evidenze richieste dalla normativa.

La Funzione Antiriciclaggio:

- costituisce funzione specialistica di controllo di secondo livello e rientra nel novero delle Funzioni Aziendali di Controllo;
- è indipendente ed è dotata di risorse qualitativamente e quantitativamente adeguate ai suoi compiti, comprese quelle economiche, eventualmente attivabili anche in autonomia;
- deve essere dotata di personale adeguato per numero, competenze tecnico – professionali ed aggiornamento, anche attraverso l'inserimento in programmi di formazione nel continuo;
- riferisce direttamente al Consiglio di Amministrazione, al Collegio Sindacale e all'Amministratore Delegato;
- ha accesso a tutte le attività della Società nonché a qualsiasi informazione rilevante per lo svolgimento dei propri compiti;
- collabora con le altre funzioni aziendali di controllo per sviluppare le proprie metodologie di gestione del rischio in modo coerente con le strategie e l'operatività aziendale.

Con specifico riferimento alle attività di adeguata verifica della Clientela, al fine di garantire al tempo stesso l'efficacia e l'efficienza dei processi, il diretto coinvolgimento della Funzione Antiriciclaggio è previsto sulla base di un approccio *risk based*, tenuto conto di eventuali circostanze oggettive, ambientali o soggettive che rendano particolarmente elevato il rischio di riciclaggio.

In attuazione di quanto precede, il modello organizzativo e operativo definito dalla Società prevede che la Funzione Antiriciclaggio proceda all'espletamento degli obblighi rafforzati di adeguata verifica della Clientela – avvalendosi del supporto del Personale responsabile della gestione dei rapporti con la Clientela, nelle ipotesi considerate a rischio più elevato. Nell'ambito della Funzione Antiriciclaggio, sono altresì definiti opportuni meccanismi di *escalation* per le ipotesi in cui il rischio di riciclaggio si presenti particolarmente elevato.

Nei casi diversi dai precedenti, la Funzione Antiriciclaggio verifica – con modalità dalla medesima definite – l'adeguatezza del processo di rafforzata verifica condotto dai soggetti responsabili per la gestione del rapporto e i relativi esiti, individuando – ove ritenuto opportuno – eventuali attività di



controllo e/o supporto da attribuire a strutture di sede della Società diverse dalla funzione antiriciclaggio.

In aggiunta a quanto precede, la Funzione Antiriciclaggio:

- identifica le norme applicabili in tema di presidio del rischio di riciclaggio e valuta il loro impatto sui processi e le procedure interne;
- presta consulenza e assistenza agli Organi aziendali, all'Alta Direzione e alle unità organizzative della Società, per le tematiche di competenza, soprattutto in caso di offerta di nuovi prodotti e servizi di modifica significativa di prodotti o servizi già offerti, all'ingresso in un nuovo mercato o all'avvio di nuove attività, ponendo particolare attenzione nella identificazione e valutazione dei rischi associati a prodotti e pratiche commerciali di nuova generazione che includono l'utilizzo di meccanismi di distribuzione o di tecnologie innovativi;
- collabora alla definizione del sistema di controlli interni, delle procedure e dei controlli finalizzati alla prevenzione e al contrasto del rischio di riciclaggio;
- collabora alla definizione delle politiche di governo del rischio di riciclaggio e delle varie fasi in cui si articola il processo di gestione di tale rischio;
- verifica nel continuo l'adeguatezza del processo di gestione del rischio di riciclaggio e l'idoneità del sistema dei controlli interni e delle procedure e propone le modifiche organizzative e procedurali volte ad assicurare un adeguato presidio di tale rischio;
- cura la definizione e mantenimento dei presidi volti a garantire l'osservanza degli obblighi di adeguata verifica della Clientela, secondo un approccio *risk based* che prevede la graduazione di tali obblighi in funzione del profilo di rischio di riciclaggio attribuito al Clientela;
- può svolgere il processo di adeguata verifica rafforzata nei soli casi in cui – per circostanze oggettive, ambientali o soggettive – è particolarmente elevato il rischio di riciclaggio;
- verifica l'affidabilità del sistema informativo per l'adempimento degli obblighi di adeguata verifica della Clientela, conservazione dei dati e segnalazione delle operazioni sospette;
- verifica il corretto funzionamento del sistema informativo per l'adempimento degli obblighi di invio delle comunicazioni oggettive;
- analizza e istruisce le segnalazioni esogene ed endogene ricevute di presunte operazioni sospette da sottoporre al Delegato alla Segnalazione di Operazioni Sospette per la valutazione delle eventuali segnalazioni alla UIF;
- esamina le evidenze emergenti da sistemi automatici di rilevazione o da sistemi di rilevazione specifici della Funzione Antiriciclaggio stessa e ne approfondisce i risultati per l'eventuale sottomissione al Delegato alla Segnalazione di Operazioni Sospette per la valutazione delle eventuali segnalazioni alla UIF;
- supporta il Delegato alla Segnalazione di Operazioni Sospette nella trasmissione alla UIF delle segnalazioni ritenute fondate;
- conduce, in raccordo con il Delegato alla Segnalazione di Operazioni Sospette, verifiche sulla funzionalità del processo di segnalazione e sulla congruità delle valutazioni effettuate dal primo livello sull'operatività della Clientela;
- presidia la trasmissione mensile alla UIF dei dati aggregati registrati in AUI da parte dell'unità preposta di primo livello tramite *outsourcer* informatico;
- collabora, in relazione alle tematiche antiriciclaggio, con le Autorità di cui al Titolo I, Capo II del Decreto Antiriciclaggio ed evade le richieste di informazioni provenienti dalle medesime;
- cura, in raccordo con le altre funzioni aziendali competenti in materia di formazione, la predisposizione di un adeguato piano di formazione, finalizzato a conseguire un aggiornamento su base continuativa del personale, e di indicatori di efficacia dell'attività di formazione svolta;
- predispose, almeno una volta l'anno, una Relazione sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale, che presenta direttamente al Consiglio di Amministrazione, al Collegio Sindacale e all'Amministratore Delegato;
- conduce, in raccordo con le altre funzioni aziendali interessate e secondo le modalità e le tempistiche definite dalla Banca d'Italia, l'esercizio di Autovalutazione dei rischi di riciclaggio e finanziamento del terrorismo, i cui esiti confluiscono nella Relazione annuale di cui al precedente alinea;

- informa direttamente e tempestivamente gli Organi aziendali di violazioni o carenze rilevanti riscontrate nell'esercizio dei relativi compiti;
- predispone appositi flussi informativi diretti agli Organi aziendali all'Esponente Responsabile per l'AML e all'Alta Direzione;
- informa periodicamente gli Organi aziendali, direttamente, circa lo stato di avanzamento delle azioni correttive adottate a fronte di carenze riscontrate nell'attività di controllo e circa l'eventuale inadeguatezza delle risorse umane e tecniche assegnate alla medesima funzione e alle necessità di potenziarle;
- nell'ambito di competenza, predispone/valida e aggiorna la normativa interna, le Policy ed i regolamenti in materia di antiriciclaggio e antiterrorismo.

Al fine di consentire agli Organi aziendali l'accesso diretto alle relazioni in materia antiriciclaggio, alle pertinenti comunicazioni intercorse con le Autorità e alle misure di vigilanza imposte o alle sanzioni irrogate, la Funzione Antiriciclaggio si avvale, quale sistema di condivisione della documentazione, della piattaforma Sherpany, in uso presso la Divisione Affari Societari per la divulgazione del materiale ai diversi componenti degli Organi aziendali.

Gli addetti della Funzione Antiriciclaggio devono essere in una posizione sufficientemente indipendente da poter manifestare il proprio giudizio, esprimere pareri e fornire raccomandazioni in modo imparziale; indipendentemente dal proprio inquadramento all'interno dell'organizzazione, devono essere scevri da qualsiasi effettivo conflitto di interesse derivante da relazioni professionali o personali o interessi pecuniari o di altro tipo, che potrebbero contrastare con i doveri ai quali sono sottoposti; inoltre, devono essere immuni da indebite interferenze che possono limitare o modificare la loro sfera d'azione o lo svolgimento delle proprie funzioni, o ancora che possano intaccare o influenzare significativamente il loro giudizio ovvero il contenuto del proprio lavoro.

Il sistema di remunerazione e incentivazione del personale della Funzione Antiriciclaggio deve essere conforme alla regolamentazione di Vigilanza nonché alle politiche interne.

#### 4.8.1 RESPONSABILE DELLA FUNZIONE ANTIRICICLAGGIO

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

Il Responsabile Antiriciclaggio deve possedere i necessari requisiti di indipendenza, competenza, professionalità e reputazionali, autorevolezza, professionalità nonché di professionalità e onorabilità individuati dalla presente Policy, la cui sussistenza – sia al momento di assunzione dell'incarico che nel continuo – è valutata dal Consiglio di Amministrazione.

Per garantire la necessaria indipendenza ed autorevolezza, il Responsabile Antiriciclaggio è collocato in posizione gerarchico-funzionale adeguata, non ha responsabilità dirette di aree operative né è gerarchicamente dipendente da soggetti responsabili di queste aree.

Il Responsabile Antiriciclaggio dispone del tempo necessario all'efficace adempimento dei propri compiti.

Per ciò che attiene ai profili di professionalità e competenza, il Responsabile Antiriciclaggio deve essere in possesso delle seguenti caratteristiche:

- conoscenza approfondita delle disposizioni normative e regolamentari in materia antiriciclaggio e antiterrorismo e/o precedenti esperienze in materia di gestione del rischio e/o nell'ambito delle Funzioni di Controllo;
- conoscenza approfondita del settore bancario-finanziario;
- capacità di relazionarsi con le Autorità di Vigilanza, le Autorità Inquirenti e gli Organi Aziendali.

Relativamente ai profili di onorabilità e correttezza, il Responsabile Antiriciclaggio deve essere in possesso dei medesimi requisiti previsti dall'art. 20 di onorabilità stabiliti dal Ministero dell'Economia e delle Finanze in attuazione di quanto previsto dall'art. 26 del Testo Unico Bancario per i soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche e ai requisiti specifici descritti nell'art. 20 del DM 169/2020<sup>1</sup>.

Il Consiglio di Amministrazione valuta le caratteristiche del candidato e sentito l'Organo di controllo il Collegio Sindacale ne autorizza l'assegnazione dell'incarico.

Il Responsabile Antiriciclaggio:

- partecipa, ove richiesto, alle riunioni degli Organi aziendali e riferisce direttamente agli stessi, senza restrizioni o intermediazioni;
- ha accesso a tutti i necessari documenti aziendali per potere adempiere ai propri compiti previsti dalla regolamentazione di Vigilanza;
- verifica la funzionalità di procedure, strutture e sistemi, prestando supporto e consulenza sulle scelte gestionali;
- rappresenta l'interlocutore della UIF per tutte le questioni attinenti alla trasmissione delle comunicazioni oggettive e per le richieste di eventuali informazioni.

La Società ha adottato misure e presidi organizzativi finalizzati a garantire la continuità operativa della Funzione Antiriciclaggio della Banca capogruppo, anche in casi di assenza o impedimento, di natura temporanea, del Responsabile Antiriciclaggio.

La Funzione Antiriciclaggio della Banca capogruppo è articolata in Unità di Controllo e Unità di Staff, con compiti e responsabilità ben definiti e dettagliatamente illustrati nella normativa interna predisposta (e periodicamente aggiornata) dalla medesima Funzione<sup>2</sup>.

Anche in caso di assenza o impedimento temporaneo del Responsabile Antiriciclaggio, gli addetti della Funzione Antiriciclaggio della Banca capogruppo sono in grado di garantire su base continuativa il monitoraggio del quadro normativo di riferimento e la compliance con i requisiti espressi dalle Autorità di Vigilanza, l'analisi degli impatti sui processi aziendali derivanti da eventuali nuovi adempimenti afferenti agli ambiti normativi di pertinenza, lo svolgimento dei controlli di secondo livello e l'adempimento degli obblighi di reporting, l'analisi e l'istruttoria delle segnalazioni esogene ed endogene ricevute in merito a presunte operazioni sospette.

In caso di assenza o impedimento temporaneo del Responsabile Antiriciclaggio, l'Esponente Responsabile per l'AML, ai fini dell'esercizio delle proprie funzioni, si interfaccia con i referenti delle Unità di Controllo e Unità di Staff della Funzione Antiriciclaggio della Banca capogruppo, ciascuno per quanto di propria competenza e nel caso, anche con il Responsabile Antiriciclaggio di Gruppo.

Laddove l'assenza o l'impedimento del Responsabile Antiriciclaggio si protragga per oltre 3 mesi, il Consiglio di Amministrazione si riunisce al fine di procedere alla sostituzione del Responsabile Antiriciclaggio o alla nomina di un Responsabile Antiriciclaggio pro tempore<sup>3</sup>.

---

<sup>1</sup> Per maggiori dettagli si rimanda alla normativa interna "Policy per la nomina, rimozione e sostituzione dei Responsabili delle Funzioni aziendali di Controllo".

<sup>2</sup> Come più dettagliatamente illustrato nell'Ordinamento dei Servizi di Banca Mediolanum S.p.A. e nel Regolamento della Funzione Antiriciclaggio.

<sup>3</sup> Cfr. Policy per la nomina, rimozione e sostituzione dei Responsabili delle Funzioni Aziendali di Controllo

#### 4.8.2 RESPONSABILE DELLA SEGNALAZIONE DI OPERAZIONI SOSPETTE

Compete al titolare dell'attività, al legale rappresentante dell'impresa ovvero ad un suo delegato valutare le segnalazioni di operazioni sospette pervenute e trasmettere alla UIF le segnalazioni ritenute fondate.

Al fine di garantire l'opportuna indipendenza del soggetto segnalante e il possesso di requisiti di professionalità e onorabilità adeguati, il ruolo di Responsabile della Segnalazione delle Operazioni Sospette è attribuito al Responsabile Antiriciclaggio.

Il ruolo e le responsabilità del Delegato devono essere adeguatamente formalizzati e resi pubblici all'interno della struttura.

Il Responsabile della 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 (es., richieste pervenute dall'autorità giudiziaria o dagli organi investigativi);
- nel rispetto degli obblighi di riservatezza previsti dal Decreto Antiriciclaggio sull'identità dei soggetti che prendono parte alla procedura di segnalazione delle operazioni, fornisce – anche attraverso l'utilizzo di idonee basi informative – informazioni sui nominativi dei Clienti oggetto di segnalazione di operazioni sospette ai responsabili delle strutture competenti per l'attribuzione o l'aggiornamento del profilo di rischio dei Clienti stessi;
- conosce e applica con rigore ed efficacia istruzioni, schemi e indicatori emanati dalla UIF;
- svolge, per quanto di competenza, un ruolo di interlocuzione con la 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 e all'eventuale astensione dal compimento delle operazioni;
- valuta, alla luce di tutti gli elementi disponibili, le segnalazioni di operazioni sospette pervenutegli dalle strutture operative di primo livello e le comunicazioni inoltrategli da parte del Collegio Sindacale, dell'Organismo di Vigilanza e/o della Funzione Internal Audit nonché quelle di cui sia altrimenti venuto a conoscenza nell'ambito della propria attività;
- trasmette alla UIF le 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, mantenendo evidenza delle valutazioni effettuate nell'ambito della procedura;
- utilizza nelle valutazioni anche eventuali elementi desumibili da fonti informative liberamente accessibili;
- comunica, con modalità organizzative idonee ad assicurare il rispetto degli obblighi di riservatezza previsti dal Decreto Antiriciclaggio, l'esito della propria valutazione al soggetto responsabile di primo livello che ha dato origine alla segnalazione;
- contribuisce all'individuazione delle misure necessarie a garantire la riservatezza e la conservazione dei dati, delle informazioni e della documentazione relativa alle segnalazioni, da sottoporre all'approvazione del Consiglio di Amministrazione.

Il Delegato, nel processo di valutazione delle operazioni sospette, può acquisire informazioni utili dalla struttura che svolge il primo livello di analisi delle operazioni anomale e avvalersi del supporto della Funzione Antiriciclaggio della Capogruppo, che svolge in outsourcing le attività operative afferenti all'ambito in oggetto.

Il Delegato può abilitare gli addetti della Funzione Antiriciclaggio della Capogruppo 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 e (3) nel sistema GE.SA.FIN. di richieste preventive di autorizzazione per operazioni/pagamenti sui documenti rappresentativi di merci in caso di paesi embargati/sanzionati/aventi restrizioni e/o nel sistema S.I.G.M.A. per operazioni/pagamenti avente

per oggetto materiali d'armamento, nonché (4) abilita gli addetti della Funzione Antiriciclaggio della Capogruppo ad operare, sempre sotto la propria responsabilità, nel sistema di gestione delle segnalazioni aggregate (S.A.R.A.).

## 4.9 STRUTTURE DELLA BANCA CAPOGRUPPO

### 4.9.1 DIREZIONE AFFARI SOCIETARI, LEGALE E CONTENZIOSO

L'Ufficio Atti Giudiziari della Direzione Affari Societari, Legale e Contenzioso della Banca capogruppo, cura la ricezione e l'evasione di richieste o provvedimenti da parte degli Organi Investigativi e dell'Autorità Giudiziaria, provvedendo al censimento delle medesime nel gestionale di riferimento, e comunica, alla struttura Banking Services & Controls, lo specifico provvedimento pervenuto al fine 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'Ufficio Atti Giudiziari provvede, inoltre, a comunicare tempestivamente, alla Funzione Antiriciclaggio, specifiche richieste e provvedimenti, secondo quanto previsto dal Regolamento di processo Segnalazione Operazioni Sospette in vigore.

### 4.9.2 DIREZIONE RISORSE UMANE

Il Settore Formazione Risorse Umane, presso la Direzione Risorse Umane assicura, in collaborazione con la Funzione Antiriciclaggio, la pianificazione e l'erogazione dei corsi specialistici di formazione ed aggiornamento professionale in materia di contrasto al riciclaggio e al finanziamento del terrorismo ai dipendenti della Società.

### 4.9.3 DIREZIONE SERVICE, OPERATIONS & ICT

L'Unità Devops & Engineering della Direzione Service, Operations & ICT della Banca capogruppo, è assegnata l'amministrazione e la gestione concreta dei rapporti con la Clientela, alla medesima compete il processo di identificazione (sul processo di *onboarding*) e di adeguata verifica della Clientela (sul monitoraggio transazionale), nonché le attività di monitoraggio e controllo sul sistema di conservazione (Archivio Unico Informatico), assegnate 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 essa 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<sup>4</sup> 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.

## 4.10 UNITA' BANKING SERVICES & CONTROLS

La Funzione 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.

---

<sup>4</sup> 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'operazione non possa essere rinviata tenuto conto della normale operatività, ovvero nei casi in cui differimento dell'operazione possa ostacolare le indagini.

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.

Alla Funzione Banking Services & Controls è assegnata l'amministrazione e la gestione concreta dei rapporti con la Clientela, alla medesima compete il processo di identificazione e di adeguata verifica della Clientela 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 essa 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<sup>5</sup> 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, nonché di monitoraggio delle attività date in *outsourcers* su strutture operative della Banca Capogruppo.

Qualora la decisione di avviare o proseguire un rapporto continuativo sia sottoposta dal Decreto Antiriciclaggio all'autorizzazione di un alto dirigente, Nel caso di rapporti od operazioni con clientela a più alto rischio, la Funzione Antiriciclaggio esprime un proprio parere sull'applicazione delle misure di adeguata verifica rafforzata da applicare e su eventuali azioni di mitigazione del rischio da adottare qualora emergano situazioni di rischio particolarmente elevato durante l'iter di autorizzazione all'avvio, alla prosecuzione, o al mantenimento di un rapporto continuativo o all'esecuzione di una operazione occasionale con Persone Esposte Politicamente, nonché all'avvio, alla prosecuzione o al mantenimento di un rapporto continuativo che coinvolga Paesi Terzi ad alto rischio o all'esecuzione di un'operazione che coinvolga tali Paesi..

#### 4.10.1 RESPONSABILE UNITA' BANKING SERVICES & CONTROLS

Il Responsabile della Unità Banking Services & Controls ha apposita delega per il rilascio:

- dell'autorizzazione, ex art. 25, comma 4, lettera a) del d.lgs. 231/07, prima di avviare o proseguire o intrattenere un rapporto continuativo, una prestazione professionale o effettuare un'operazione occasionale con persone esposte politicamente, come definite ai sensi dell'art. 1, comma 2, lettera dd) del d. lgs. 231/07, nel rispetto del vigente "Regolamento del processo di gestione delle Persone Esposte Politicamente".
- dell'autorizzazione ex art. 25, comma 4-bis, lettera d) del d.lgs. 231/07, prima di effettuare un'operazione che coinvolga paesi terzi ad alto rischio, come definiti ai sensi dell'art. 1, comma 2, lettera bb) del d. lgs. 231/07.

Qualora il Responsabile dell'Unità Banking Services & Controls decida di non attenersi al parere della Funzione Antiriciclaggio, il medesimo Responsabile è tenuto a formalizzare e motivare la

---

<sup>5</sup> 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'operazione non possa essere rinviata tenuto conto della normale operatività, ovvero nei casi in cui differimento dell'operazione possa ostacolare le indagini.



decisione e a individuare le misure che saranno adottate per mitigare i rischi segnalati. tenere traccia di tale scelta, motivandola opportunamente.

#### 4.10 ALTRE STRUTTURE OPERATIVE

Il Responsabile della singola struttura operativa 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 quelle emanate dalla società di appartenenza.

A ciascun Responsabile delle varie strutture operative della Società, è comunque attribuita 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, rilevano 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 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.

## 5 I PRINCIPI IN TEMA DI CONTRASTO DEL RICICLAGGIO E DEL FINANZIAMENTO DEL TERRORISMO

La Società adotta procedure e metodologie commisurate alla natura dell'attività svolta e alle proprie dimensioni per l'analisi e la valutazione dei rischi di riciclaggio e finanziamento del terrorismo cui sono esposte nell'esercizio della propria attività, tenendo conto di molteplici fattori di rischio. La Società ha definito apposite linee guida – recependo le linee guida fornite dalla Capogruppo - basate sui più elevati standard di contrasto del riciclaggio e del finanziamento del terrorismo, a cui i componenti degli Organi aziendali, i dipendenti ed i collaboratori sono chiamati ad attenersi, per evitare il coinvolgimento, anche inconsapevole, della Società stessa in fenomeni di riciclaggio e di finanziamento del terrorismo.

Di seguito, si forniscono le linee guida per l'adempimento degli obblighi in modo conforme alle disposizioni normative, i quali saranno declinati, ai fini di una compiuta attuazione, negli specifici Regolamenti di processo e nelle procedure interne adottate dalla Società.

### 5.1 PROFILATURA DELLA CLIENTELA

Al fine di graduare la profondità e l'estensione degli obblighi di adeguata verifica, la Società adotta idonee procedure volte a profilare ciascun Clientela in funzione del rischio di riciclaggio e finanziamento del terrorismo.

Tale approccio costituisce una applicazione del più ampio principio di proporzionalità richiamato dalle vigenti disposizioni normative, il cui obiettivo è quello di massimizzare l'efficacia dei presidi aziendali e razionalizzare l'uso delle risorse.

A tal riguardo, l'informazione relativa al profilo di rischio di riciclaggio e finanziamento del terrorismo è resa disponibile alle Strutture Operative (in particolare la Funzione Banking Services & Controls) che hanno in carico la gestione e l'amministrazione, nel concreto, dei rapporti con la Clientela. In linea con quanto previsto dalla normativa vigente, il Personale che ha accesso all'informazione sul



profilo di rischio dei Clienti, deve mantenere la massima riservatezza, astenendosi dal comunicare tale informazione ai Clienti medesimi o a terzi.

La profilatura del rischio, articolata su quattro fasce di rischio - irrilevante, basso, medio e alto - è basata, sull'analisi dei fattori di rischio:

- relativi al Clientela, all'Esecutore e Titolare effettivo;
- relativi a prodotti, servizi, operazioni o canali di distribuzione;
- geografici.

I presidi informatici adottati permettono di determinare, sulla base dell'elaborazione dei dati e delle informazioni a disposizione della Società ed acquisite in sede di instaurazione di rapporti continuativi e di monitoraggio dell'operatività posta in essere, un "punteggio" rappresentativo del livello di rischio di riciclaggio o di finanziamento del terrorismo e di classificare i Clienti in modo da poter eseguire, nei loro confronti, verifiche più o meno incisive e commisurate ad una delle quattro tipologie di profilo di rischio.

Si riportano, nella tabella seguente, i possibili profili di rischio attribuibili alla Clientela e la frequenza di aggiornamento dei dati relativi alla adeguata verifica.

Rif.	Classe di rischio	Frequenza aggiornamento
I	Irrilevante	Ogni 48 mesi
B	Basso	Ogni 36 mesi
M	Medio	Ogni 24 mesi
A	Alto	Annuale (ogni 12 mesi)

La Società monitora e aggiorna periodicamente i punteggi e le regole attribuite al sistema di profilatura del rischio, avendo anche a riferimento l'evoluzione del contesto di riferimento, delle *leading practice* di mercato e delle linee guida o indicazioni ricevute dalla Capogruppo.

In quanto parte di un Gruppo, la Società (come le altre società del Gruppo) assume, in ogni caso, per uno stesso Clientela, il profilo più elevato tra quelli assegnati a tutte le società del Gruppo medesimo.

Al fine di valutare i rischi relativi al Cliente, all'Esecutore e al Titolare effettivo, la Società prende in considerazione ulteriori fattori di rischio, valorizzando il patrimonio informativo disponibile, valutando le notizie negative provenienti dai media o da altre fonti informative considerate fondate e attendibili, esaminando le segnalazioni di comportamenti anomali provenienti dai dipendenti delle Strutture Operative che gestiscono e amministrano, nel concreto, i rapporti con la Clientela. In particolare, deve essere opportunamente considerato, dal dipendente che gestisce e amministra, nel concreto, i rapporti con la Clientela, il comportamento tenuto dal Cliente o dall'Esecutore, quale, ad esempio (elenco non esaustivo, per ulteriori indicatori di anomalia si rimanda al provvedimento contenente indicatori di anomalia pubblicato dalla UIF - <https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia>):

- 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 erranee;
- 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 erranee e/o significativamente difformi, 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 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 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.

Sulla base di tutte le informazioni acquisite, qualora il dipendente ritenga anomalo il comportamento del Cliente o l'operazione non ragionevole, provvedono a trasmettere tempestivamente una segnalazione di operazione sospetta alla Funzione Antiriciclaggio, affinché svolga gli approfondimenti del caso e sottoponga la pratica al Delegato alla segnalazione delle operazioni sospette per le valutazioni di competenza, tra cui rientra anche l'eventuale innalzamento del profilo di rischio del Cliente, mantenendo evidenza delle valutazioni effettuate.

Nella valutazione dei comportamenti anomali dei clienti o della mancata ragionevolezza delle operazioni poste in essere dai medesimi, i dipendenti delle unità coinvolte tengono conto di tutti i dati acquisiti dai clienti e le informazioni in loro possesso, ivi compresi, quelli acquisiti da altri intermediari con il consenso esplicito del cliente che ha aderito al servizio di informazione sui conti detenuti presso uno o più prestatori di servizi di pagamento offerto (Prestatori di servizi di informazione sui conti - AISP).

Con riferimento alla classe di rischio corrispondente al profilo di rischio "alto", la Società considera, indipendentemente dai punteggi attribuiti dal sistema di profilatura della Clientela in uso, a più alto rischio di riciclaggio:

a) i Clienti, i titolari effettivi, i Beneficiari designati in via nominativa 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 dell'applicazione degli obblighi di congelamento previsti dal Consiglio di Sicurezza dell'ONU, dai Regolamenti comunitari o dai decreti adottati ai sensi del decreto legislativo n. 109, del 22 giugno 2007 o con quella dell'Office of Foreign Asset Control (OFAC) del Dipartimento del Tesoro degli Stati Uniti;
- notizie negative provenienti dai *media* o da altre fonti informative pubbliche e ritenute "affidabili"<sup>6</sup>;
- notizie negative fornite direttamente dal Cliente, 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);

<sup>6</sup> In tal caso l'informazione, nonché la notizia "pubblica", viene fornita al cliente/prospect in quanto **non sussiste** uno dei casi di limitazione al diritto di accesso previsti dall'art. 2-undecies del Codice (in attuazione dell'art. 23 del Regolamento (UE) 2016/679), un inidoneo riscontro alle richieste di accesso formulate dall'interessato, in violazione degli artt. 5, par. 1, lett.re a) e c) e 15 e del Regolamento. [rif. Provvedimento del 13 aprile 2023 (9888457) emesso dal GPDP]

- decreti di sequestro, ovvero misure cautelari reali e di prevenzione adottate dall’Autorità Giudiziaria;
- b) i Clienti, i titolari effettivi e gli Esecutori oggetto di segnalazione alla UIF da parte della Società o altra società del Gruppo negli ultimi 5 anni, ovvero che continuano a presentare elementi di criticità;
- c) i Clienti i cui fondi provengono da operazioni di *voluntary disclosure* o analoga procedura per il rimpatrio di capitali legati ad evasione fiscale o altri reati, la cui regolarizzazione è avvenuta nei 5 anni precedenti;
- e) i rapporti continuativi, le prestazioni professionali ed operazioni occasionali con Clienti e relativi titolari effettivi che siano Persone Esposte Politicamente esposte, salve le ipotesi in cui le predette persone politicamente esposte agiscono in veste di organi delle Pubbliche amministrazioni;
- f) i rapporti continuativi, le prestazioni professionali e le operazioni che coinvolgono i Paesi Terzi ad alto rischio, nonché i Clienti e titolari effettivi residenti o aventi sede legale in aree geografiche a rischio elevato;
- g) le strutture qualificabili come veicoli di interposizione patrimoniale, quali trust, società fiduciarie, (indipendentemente dalla relativa iscrizione o meno all’Albo ex art. 106 TUB), fondazioni, società il cui capitale sociale sia detenuto, in tutto o in parte, da una società fiduciaria, da un trust, da un ente o schema giuridico analogo; le società partecipate da fiduciari;
- h) i Clienti che presentino un assetto societario anomalo o eccessivamente complesso, data la natura dell’attività svolta, soggetti esteri diversi dalle persone fisiche;
- i) i Clienti che presentino un tipo di attività economica caratterizzata da elevato utilizzo di contante o riconducibile a settori particolarmente esposti a rischi di corruzione;
- j) i Clienti che beneficiano di servizi con un elevato grado di personalizzazione, offerti ad una Clientela dotata di un patrimonio di rilevante ammontare;

La Società considera, inoltre, a più alto rischio di riciclaggio, i Clienti individuati su disposizione del Delegato alla segnalazione di operazioni sospette a seguito del prudente apprezzamento dello stesso. Il Delegato può altresì diminuire, a seguito di propria valutazione in sede di analisi di specifiche posizioni, i punteggi attribuiti, mantenendo evidenza delle analisi effettuate. Non è consentita, in ogni caso, la modifica in autonomia dei punteggi attribuiti da parte del restante Personale.

Resta comunque ferma la possibilità, da parte della Funzione Antiriciclaggio, di chiedere alla funzione Banking Services & Controls di svolgere il processo di adeguata verifica rafforzata in tutti i casi, anche non rientranti in quelli sopra elencati, in cui appaia particolarmente elevato il rischio di riciclaggio o finanziamento del terrorismo.

## 5.2 ADEGUATA VERIFICA ORDINARIA DELLA CLIENTELA

La Società adotta misure di adeguata verifica della Clientela proporzionali all’entità dei rischi di riciclaggio e finanziamento del terrorismo, tenendo conto di specifici fattori con riferimento al Clientela, all’operazione, al rapporto continuativo.

Gli obblighi di adeguata verifica sono assolti nei confronti dei nuovi Clienti prima di instaurare un rapporto continuativo, nonché di quelli già acquisiti, ogni qualvolta l’adeguata verifica si renda opportuna in considerazione del mutato livello di rischio di riciclaggio o di finanziamento del terrorismo associato al Clientela.

L’acquisizione delle informazioni deve essere finalizzata alla valutazione, durante tutta la durata del rapporto, della coerenza delle transazioni con la conoscenza del Clientela, delle sue attività

commerciali e del suo profilo di rischio. L'identificazione del Clientela, dell'eventuale Esecutore e del Titolare effettivo con la relativa verifica dell'identità e la raccolta delle informazioni deve pertanto avvenire nell'ambito di un confronto dialettico necessario da un lato al Clientela per conoscere la Società e dichiarare lo scopo e la natura del rapporto continuativo che intende instaurare, dall'altro alla Società, per conoscere meglio il Clientela, le sue necessità bancarie, finanziarie e assicurative, potendo offrire i prodotti più adatti.

A tal fine, la Società adotta adeguate iniziative di formazione del proprio personale e dei propri collaboratori, secondo quanto descritto dal successivo paragrafo [FORMAZIONE DEI DIPENDENTI E COLLABORATORI](#).

I dipendenti della funzione Banking Services & Controls e/o dell'Unità Devops & Engineering della Direzione Service, Operations & ICT della Banca capogruppo, cui compete la gestione e l'amministrazione concreta dei rapporti con la Clientela, assolvono gli obblighi di adeguata verifica osservando le misure, le modalità e le procedure interne adottate dalla Società, al fine di sviluppare e mantenere aggiornata la conoscenza del Clientela e segnalare eventuali operazioni sospette.

Per garantire il corretto svolgimento dell'adeguata verifica della Clientela le unità coinvolte curano in prima persona (strutture della società o della Banca capogruppo) o monitorano (funzione Banking Services & Controls) la struttura della Banca capogruppo a cui sono demandate dette attività di primo livello in funzione di apposito controllo di outsourcing:

- l'esito del processo rafforzativo utilizzato a seguito processo di identificazione della Clientela, degli eventuali esecutori, dei titolari effettivi realizzato come da par. 6.2.1, nonché delle informazioni aggiuntive necessarie a determinare il profilo di rischio da associare al Clientela, previste nella modulistica della Società e delle società i cui prodotti sono collocati dalla medesima;
- il censimento della Clientela, degli eventuali esecutori e dei titolari effettivi nell'anagrafe della Società e la conservazione della documentazione acquisita per l'identificazione e l'adeguata verifica, secondo le disposizioni e le misure di riservatezza dettate dalla normativa interna, e l'attuazione dei controlli previsti dal processo di *onboarding*;
- l'acquisizione e la valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo;
- il controllo costante dei rapporti continuativi, al fine di aggiornare la conoscenza del Clientela, e dello scopo dichiarato del rapporto, nonché di valutare eventuali operazioni "inattese", anomale o non coerenti al profilo economico e finanziario del Clientela in precedenza conosciuto o di notizie di eventi significativi (ivi compreso il monitoraggio transazionale *real time*);
- l'aggiornamento dei dati e delle informazioni raccolte, con frequenza dipendente dal profilo di rischio precedentemente associato ai Clienti, chiedendo a questi ultimi di fornire, sotto la propria responsabilità, tutte le informazioni necessarie e aggiornate per consentire l'assolvimento degli obblighi di adeguata verifica.

Non è richiesta l'adeguata verifica per le attività finalizzate o connesse all'organizzazione, al funzionamento o all'amministrazione della Società, tenuto conto che esse non rientrano nelle attività istituzionali della medesima e che, nello svolgimento delle stesse, le controparti della Società si configurano come prestatori di beni o servizi su iniziativa della Società stessa, piuttosto che come Clienti che richiedono di instaurare un rapporto continuativo o di effettuare un'operazione occasionale.

### 5.2.1 PROCESSO DI *DIGITAL ONBOARDING*

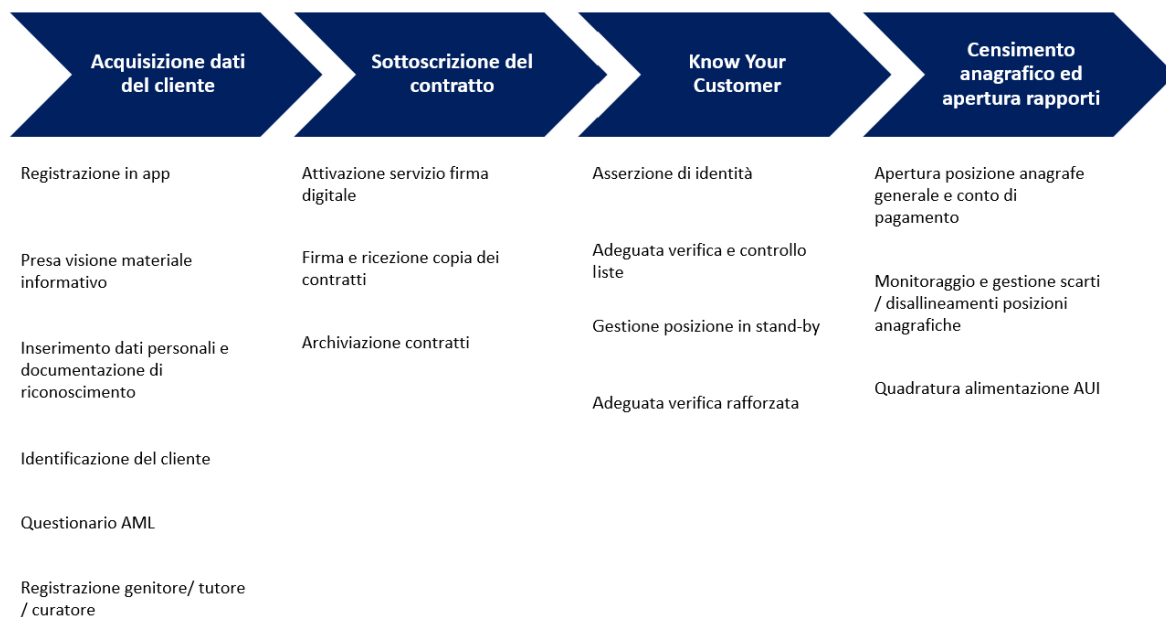
Per operatività a distanza si intende quella complessivamente svolta senza la compresenza fisica del Clientela e del Personale incaricato della Società, ovvero attraverso i sistemi di comunicazione informatica tipici messi a disposizione (es. APP, sito internet, Mobile etc..) dalla Società stessa.

La Società ha definito l'intensità e l'estensione dei presidi organizzativi e di controllo per la prevenzione del riciclaggio e del finanziamento del terrorismo alla luce delle caratteristiche del prodotto offerto e del segmento di Clientela cui esso è destinato.

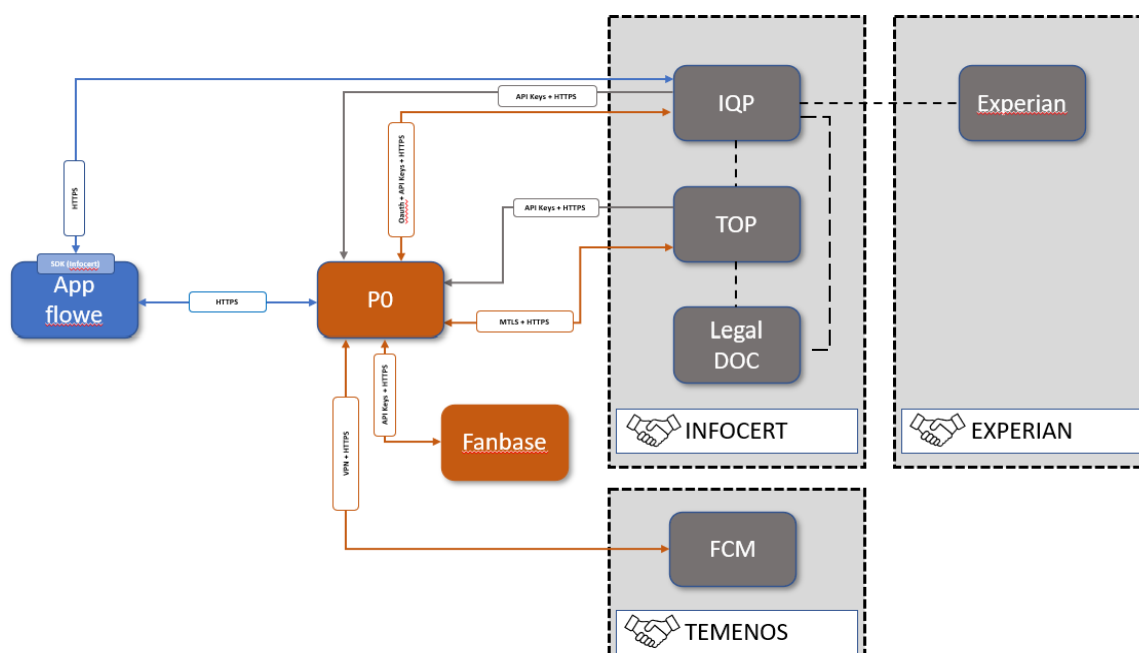
La Società ha previsto un processo di *onboarding* basato esclusivamente sul canale mobile APP (mediante tablet e smartphone) e articolato nelle seguenti fasi:

- 1) Acquisizione dati del cliente
- 2) Sottoscrizione del contratto
- 3) Fase di *Know Your Customer*
- 4) Censimento anagrafico ed apertura rapporti

Ogni fase si compone di una serie di sotto processi specifici sui quali sono stati implementati controlli applicativi.



Schema processo di onboarding e relativi sotto processi



Schema delle interfacce applicative e modello di integrazione

Il processo di *onboarding* in estrema sintesi, prevede quindi l'acquisizione di dati e documenti dalla Clientela che vengono raccolti e confermati/certificati dalla stessa nel corso del processo medesimo, all'esito del quale il set contrattuale viene sottoscritto mediante firma elettronica qualificata rilasciata da *Certification Authority (CA)* ai sensi del Regolamento (UE) n. 910/2014 (c.d. eIDAS).

Il *prospect*, dopo aver installato l'APP, inserisce le informazioni necessarie a registrare il *device* ed assicurare i presidi di sicurezza dello strumento sul quale è scaricata l'app, quali:

- "pass code";
- numero di cellulare, certificato inserendo il codice OTP ricevuto via sms;
- indirizzo e-mail, certificato inserendo il codice OTP ricevuto via e-mail.

Qualora il *prospect* avesse difficoltà nell'inserimento delle informazioni richieste, può avvalersi delle funzioni di supporto quali ad. es Chatbot, gestite dagli operatori della funzione Banking Services & Controls dedicati alle attività di Customer Interaction.

Il *prospect* conferma la presa visione del materiale informativo relativo all'offerta di Flowe (es.: norme contrattuali in bianco idonee alla stipula e il foglio informativo) e prosegue con l'accettazione in app dell'informativa privacy (principi e modalità di utilizzo dei dati personali da parte di Flowe).

Ai fini dell'identificazione al potenziale cliente è richiesto:

- il codice fiscale (può essere inserito dal *prospect*, fotografato o calcolato automaticamente in app);
- una fotografia chiara del documento identificativo scelto per la registrazione; i dati anagrafici sono acquisiti automaticamente dal documento identificativo, tramite l'Optical Character Recognition (c.d. OCR).

Il *prospect*, inoltre, conferma o completa le sue informazioni personali quali indirizzo di residenza ed eventuale domicilio (se diverso da residenza). In caso di anomalie/incongruenze sui dati inseriti, il processo di apertura conto non arriva a finalizzarsi.

Nel caso di utilizzo di documento elettronico ed attivazione della tecnologia Near Field Communication (c.d. NFC), il *prospect* può decidere di far leggere elettronicamente i dati del documento (i dati dei documenti contraffatti non vengono letti). In questo caso, PO Platform acquisisce automaticamente i dati del documento (inclusa la foto del soggetto) senza necessità di digitarli/caricare una foto. Si specifica che i dati dei documenti letti tramite NFC non sono modificabili negli step successivi da parte del *prospect*.

Per procedere con l'identificazione il *prospect* viene guidato, attraverso l'app, nella realizzazione di un video selfie (nr. 5 selfie in sequenza) così da consentire, tramite sistemi biometrici<sup>7</sup>, la verifica della corrispondenza tra le immagini acquisite e la foto presente nel documento identificativo; viene valutato l'esito del "face-matching" in base alla percentuale di corrispondenza (score) tra l'immagine del *prospect* riportata sul documento identificativo e il video selfie realizzato. Nel caso in cui la percentuale di corrispondenza sia inferiore alle soglie minime definite dalla Società, il *prospect* deve ripetere l'inserimento delle informazioni identificative avvalendosi, ove necessario, del supporto del *Chatbot* (dove sono fornite soluzioni standard per risolvere problemi di riconoscimento). Qualora la soglia di

---

<sup>7</sup> Dati biometrici: Dati personali relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali immagini del volto o dati dattiloscopici, ottenuti e trattati con mezzi tecnici.



corrispondenza venga raggiunta, il *prospect* può proseguire il processo di *onboarding* e contemporaneamente la Platform provvede ad inviare i dati raccolti in App Flowe alla CA.

La Soluzione adottata prevede utilizzo del servizio "AI Face Matching" della CA, basato sul progetto "Facenet open source". Facenet è l'implementazione TensorFlow<sup>8</sup> del riconoscimento facciale descritto nell'articolo "FaceNet: A Unified Embedding for Face Recognition and Clustering"<sup>9</sup>. Il progetto utilizza anche idee tratte dall'articolo "Deep Face Recognition"<sup>10</sup> del Visual Geometry Group<sup>11</sup> di Oxford.

Nel momento in cui il soggetto instaura un rapporto viene attivata la fase di *enrolment* cioè il processo attraverso il quale avviene l'acquisizione del campione biometrico (riconoscimento facciale) con la sua memorizzazione nel sistema e con l'estrazione dei tratti (*biometric feature*) necessari per la generazione del riferimento biometrico da trattenere come campione per i confronti successivi; il campione (*biometric sample*) è la rappresentazione analogica o digitale di una caratteristica biometrica ottenuta al termine del processo di acquisizione (*biometric capture* e *biometric acquisition*) costituita, nel caso di Flowe, dalla riproduzione dell'immagine del *prospect* richiedente (foto).

La rete neurale è stata integrata con un set di dati standard chiamato: set di dati VGGFace2<sup>12</sup> che include 3,31 milioni di immagini di 9.131 soggetti (identità) e raggiunge un livello di accuratezza del 99,5% per l'attività di identificazione, su un set di test standard chiamato *Labeled Faces in the Wild*<sup>13</sup> (LFW)<sup>14</sup>.

Facenet calcola la distanza del coseno tra gli Embedding<sup>15</sup> (facce): il risultato è un numero che varia tra 0 (identico) e 1.5 (completamente incompatibile): la CA ha normalizzato il numero tra 100% (identico), 75% (soglia di confidenza) e 0% (completamente incompatibile).

Per ciò che attiene alla *liveness detection*, tale funzionalità permette di determinare la "liveness" del cliente che in una determinata sessione sta per sottoporre il proprio volto per una verifica di compatibilità con la foto estratta dal proprio documento. In particolare, tale servizio è in grado di fornire funzionalità per: (a) guidare il cliente nella fase di inquadramento in modo da realizzare il selfie rispettando l'allineamento del volto in fase di scatto; (b) realizzare un riconoscimento *liveness* del volto durante la procedura.

Il modulo di *liveness detection* della Soluzione esegue anche alcuni controlli aggiuntivi per aumentare il livello di sicurezza ed assicurarsi che la persona che sta seguendo la procedura di *onboarding* sia una persona reale, in particolare: (a) la sequenza di movimenti richiesti al cliente è sempre casuale (e ciò impedisce che la Soluzione sia sottoposta ad un video del volto del cliente che esegue esattamente i movimenti richiesti); (b) la procedura deve essere eseguita entro un tempo massimo definito.

---

<sup>8</sup> <https://www.tensorflow.org/>

<sup>9</sup> <https://arxiv.org/abs/1503.03832>

<sup>10</sup> <https://www.robots.ox.ac.uk/~vgg/publications/2015/Parkhi15/parkhi15.pdf>

<sup>11</sup> <https://www.robots.ox.ac.uk/~vgg/>

<sup>12</sup> [https://www.robots.ox.ac.uk/~vgg/data/vgg\\_face2/](https://www.robots.ox.ac.uk/~vgg/data/vgg_face2/)

<sup>13</sup> <http://vis-www.cs.umass.edu/lfw/>

<sup>14</sup> LFW è un database di fotografie di volti progettato per studiare il problema del riconoscimento facciale senza vincoli. Il set di dati contiene più di 13.000 immagini di volti raccolte dal web. Ogni faccia è stata etichettata con il nome della persona raffigurata. 1680 delle persone raffigurate avevano due o più foto distinte nel set di dati.

<sup>15</sup> L'*embedding* è una rappresentazione digitale del volto, sulla base di 512 diverse caratteristiche che, la rete neurale, sceglie autonomamente di tradurre in numeri.



A questo punto il *prospect* compila il questionario antiriciclaggio (c.d. AML) che comprende, ad esempio, domande inerenti all'occupazione, alla fonte di reddito, o se si tratta di un soggetto PEP.

Laddove il potenziale Cliente sia minorenne, le predette attività vengono svolte anche nei confronti di un soggetto maggiorenne (il quale agisce in qualità di genitore, curatore o tutore legale, a seconda dei casi).

Al completamento di tale questionario, ad esclusione del caso in cui il soggetto si dichiari *US Person* per il quale la procedura non permette di proseguire portando al termine il processo di *onboarding*, si prosegue con la sottoscrizione del contratto.

Qualora il *prospect* si dichiari un soggetto PEP, l'*onboarding* viene sospeso in attesa dell'esito della valutazione da parte dell'operatore della funzione Banking Services & Controls.

Al termine del questionario il *prospect* richiede in app il "Certificato Qualificato di Firma Digitale" della CA e in seguito visualizza il modulo di sottoscrizione del servizio precompilato con i dati forniti in precedenza. Il *prospect* prende visione dei documenti contrattuali e delle clausole vessatorie ed accorda la conferma definitiva alla sottoscrizione del contratto firmando digitalmente tramite OTP. Successivamente il modulo firmato viene inviato, tramite e-mail, al *prospect* insieme ai restanti documenti contrattuali. Il *prospect* deve poi confermare in app di aver ricevuto tutto il pacchetto contrattuale via e-mail. Tutto il materiale contrattuale viene reso disponibile al *prospect* all'interno di una sezione dedicata dell'app Flowe. Il *prospect*, perfezionato il contratto, riceve quindi una e-mail che lo informa che la Società provvederà nei giorni successivi a comunicargli l'esito delle ultime opportune verifiche. Solo al termine di questi controlli, in caso di esito positivo, il *prospect* diventa cliente Flowe a tutti gli effetti.

Per il perfezionamento delle attività di *onboarding* è in ogni caso prevista l'esecuzione di ulteriori determinati controlli (di cui alcuni "bloccanti"), finalizzati a verificare, tramite accesso a banche dati affidabili ed indipendenti, con riferimento al *prospect* (e all'eventuale genitore, curatore e/o tutore legale):

- che il soggetto proponente non sia residente estero;
- che i dati raccolti e confermati dal Cliente non presentino incongruenze o anomalie (es. indirizzo sconosciuto, numerazione documento non congruente, etc...) tramite *inquiry* in banca dati indipendente e affidabile;
- che non sia presente in "liste" o "elenchi" (es. PEP, PIL, elenchi di soggetti/persone previsti dai Regolamenti comunitari o dai decreti adottati ai sensi del decreto legislativo 22 giugno 2007, n. 109, per contrastare il finanziamento del terrorismo internazionale, elenchi di soggetti/persone OFAC, etc...);
- che non abbia "pregiudizievoli" e/o "protesti".

Tale ulteriore modalità rafforzativa, che appare in linea con le previsioni dettate dall'articolo 18, comma 1, lettera a)<sup>16</sup> del D.Lgs. 231/2007 modificato da ultimo dall'art. 27, comma 3 della Legge del 11 settembre 2020, n. 120, prevede controlli automatizzati volti a verificare le informazioni e dati acquisiti anche tramite l'acquisizione digitale di copia del documento identificativo del Clientela e da

---

<sup>16</sup> a) l'identificazione del Clientela e la verifica della sua identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente. Le medesime misure si attuano nei confronti dell'Esecutore, anche in relazione alla verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del Clientela;

questi confermati, tramite *una fonte affidabile e indipendente*. Tali controlli sono volti a verificare la correttezza, la validità e la veridicità dei dati e documenti forniti dal Clientela stesso.

In aggiunta a quanto sopra, si evidenzia che, con riferimento alla Soluzione, la Società ha altresì:

- effettuato - con il supporto della Divisione Information & Communication Technology [della Capogruppo] - una apposita valutazione del rischio IT e dei relativi strumenti a mitigazione da implementare;
- richiesto, tra l'altro, al Data Protection Officer e alla Funzione Risk Management di svolgere le proprie analisi e di fornire le relative valutazioni;
- definito che, durante la fase di implementazione e messa in produzione della Soluzione, saranno definite e pianificate le attività di test e fine tuning della soluzione medesima, al fine di mitigarne i rischi e determinarne il piano dei controlli

Il Responsabile Antiriciclaggio sulla base delle conclusioni sopra riportate e sulla scorta della attività di *risk assesment* condotte dalla Funzione Risk Assesment, ritiene complessivamente il processo di *onboarding* della Clientela a distanza tramite riconoscimento biometrico, adottato dalla Società conforme ai requisiti normativi<sup>17</sup>, nonché idoneo a fronteggiare i relativi rischi<sup>18</sup>. L'analisi svolta dalla Funzione Antiriciclaggio ha difatti evidenziato che il processo di *onboarding* definito dalla Società, ivi compreso la eventuale possibilità di estensione a soggetti titolari di identità digitale con il Sistema Pubblico d'Identità Digitale (SPID) e/o con la nuova Identità Digitale Nazionale ("IDN")<sup>19</sup>, prevede misure adeguate a verificare l'identità della Clientela conformemente alla normativa vigente, riservandosi, di tornare in argomento in occasione di eventuali modifiche significative alla normativa di riferimento o al processo in questione, aggiornando di conseguenza, se del caso, la presente Policy.

Per quanto attiene il business "B2B2C" (*Business To Business To Customers*) per quanto attiene la linea di business concernente servizi tecnologici 'verticali' (cd. *Packaged Solution*), volti a soddisfare specifiche esigenze di *business* di *players* del mercato finanziario e non finanziario si prevede altresì, oltre a quanto sopra riportato, una analisi specifica di *pre-assessment* da effettuarsi di volta in volta per singolo 'cliente', volta a verificare la componente di sicurezza dell'accesso ai servizi tecnologici pubblicati da Flowe (es. API) da parte di applicazione / sito web del 'cliente'.

## 5.2.2 PROCESSO EMISSIONE E GESTIONE STRUMENTI DI PAGAMENTO A SPENDIBILITÀ LIMITATA

Per quanto attiene il business "B2B2C" (*Business To Business To Customer*) per quanto attiene la linea di business concernente il servizio di *walleting* (cd. *Payment as a Service*), diretto a *player* non finanziari al fine di fornire alla loro base clienti un servizio di pagamento digitale su circuito privatistico è stato analizzato il relativo processo di emissione e gestione di strumenti di pagamento a spendibilità limitata.

---

<sup>17</sup> La IV Direttiva contro il riciclaggio e il finanziamento al terrorismo (849/2015), recepita in Italia con il Dlgs 90/2017, e attraverso le modifiche apportate al Dlgs 231/07, ha introdotto la possibilità di effettuare il processo di identificazione della clientela con "l'utilizzo di altri meccanismi di riscontro basati su affidabili soluzioni tecnologiche innovative (quali, ad esempio, quelle che prevedono forme di riconoscimento biometrico), purché assistite da robusti presidi di sicurezza".

<sup>18</sup> Anche in funzione delle previsioni contenute negli "Orientamenti sull'utilizzo di soluzioni di onboarding a distanza del cliente per le finalità di cui all'articolo 13, paragrafo 1, della direttiva (UE) 2015/849", pubblicati dall'EBA il 22 novembre 2022

<sup>19</sup> c.d. IT Wallet (portafoglio digitale per conservare tutte insieme le versioni digitali dei propri documenti più importanti: la carta d'identità o lo Spid, ma anche la tessera sanitaria, ad esempio, e la carta delle disabilità).

In relazione all'attività di emissione e gestione di strumenti di pagamento spendibilità limitata (ai sensi dell'art. 2, co. 2 lett. m, del d. lgs. n. 11 del 2010), al fine di verificare gli obblighi antiriciclaggio anche in relazione a tale specifica attività che l'intermediario sia tenuto ad osservare si fa presente che:

- ai sensi delle disposizioni in materia di prevenzione al riciclaggio e finanziamento del terrorismo, gli obblighi si applicano ai “rapporti continuativi”, ovvero “*un rapporto contrattuale di durata, rientrante nell'esercizio dell'attività di istituto svolta dai soggetti obbligati, che non si esaurisce in un'unica operazione*”, e come ripreso anche nel Provvedimento di Adeguata Verifica della clientela nella sezione II “Ambito di applicazione”, al primo capoverso: “*I destinatari procedono all'adeguata verifica della clientela in relazione ai rapporti e alle operazioni che rientrano nella propria attività istituzionale, come definita dalla normativa di settore.*”<sup>20</sup>.
- nel resoconto della consultazione<sup>21</sup> del 30 luglio 2019 al Provvedimento di Adeguata Verifica della clientela pubblicato poi da Banca d'Italia nel luglio 2019, veniva esplicitamente trattato il tema delle “attività di istituto” o “istituzionali” a cui fare specifico riferimento, ovvero (pag. 5):

È stato chiesto se i destinatari debbano applicare gli obblighi di adeguata verifica in relazione a:

- a) i servizi e le attività per il cui esercizio non è richiesta una specifica autorizzazione, quali, ad esempio, i servizi o le operazioni di pagamento espressamente esclusi dall'ambito di applicazione della disciplina dei servizi di pagamento (cfr. articolo 2 del decreto legislativo 27 gennaio 2010, n. 11);
- b) le attività accessorie ai servizi di pagamento che gli istituti di pagamento e gli istituti di moneta elettronica possono esercitare ai sensi del TUB (concessione di crediti strettamente correlati ai servizi prestati, prestazione di garanzie, servizi di cambio, gestione di sistemi di pagamento).

Nel riscontro, Banca d'Italia indica:

In relazione al quesito sub a), in linea con quanto previsto dal Decreto, le Disposizioni chiariscono che i destinatari applicano gli obblighi di adeguata verifica in relazione ai servizi e alle attività “istituzionali”, cioè quelle attività per il cui esercizio abbiano ottenuto l'autorizzazione ai sensi del TUB o del TUF.

Con riferimento al quesito sub b), si ritiene che le attività accessorie esercitate in stretta connessione con i servizi di pagamento:

- siano incluse nel perimetro dell'attività istituzionale nella misura in cui esse costituiscano un'attività finanziaria riservata (es. concessione di finanziamenti);
- non rientrino invece nel perimetro dell'attività istituzionale, laddove si tratti di attività che, considerate autonomamente, non siano coperte da riserva (es. attività di custodia, registrazione e trattamento di dati).

Tutte le attività esercitate, anche se non rientranti in quelle istituzionali, dovrebbero essere comunque presidiate dagli intermediari in un'ottica di contenimento del rischio legale e reputazionale cui essi sono esposti.

- nel resoconto della consultazione del 24 febbraio 2022 delle Linee Guida dell'EBA sugli strumenti a spendibilità limitata (o *limited network exemption*)<sup>22</sup> a pag. 29 (descrizione Option

<sup>20</sup> <https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/disposizioni/20190730-dispo/Disposizioni.pdf>

<sup>21</sup> [https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2018/disposizioni-adequata-verifica/resoconto\\_consultazione.pdf](https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2018/disposizioni-adequata-verifica/resoconto_consultazione.pdf)

<sup>22</sup> <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-limited-network-exclusion-under-psd2>

1), viene espressamente indicato che “al contrario, l’articolo 18, paragrafo 1, lettera c), della PSD2 prevede esplicitamente che “*gli istituti di pagamento regolamentati possano svolgere attività commerciali diverse dalla fornitura di servizi di pagamento.*”

Si ritiene pertanto, sulla scorta di quanto sopra riportato, che il contenuto della prima FAQ presente sul sito di Banca d’Italia<sup>23</sup> sia da ritenersi superata.

Non risultano pertanto applicabili obblighi specifici in materia di prevenzione al fenomeno del riciclaggio e del finanziamento del terrorismo all’attività di emissione e gestione di strumenti di pagamento a spendibilità limitata, fermo restando le accortezze da adottare per presidiare rischi legali e reputazionali (es. ponendo dei limiti di importo all’operatività del prodotto/servizio, sia in termini di massimale di ricarica mensile che di eventuale rimborso mensile in contanti presso la cassa dell’esercente).

### 5.2.3 MOTORE DI ADEGUATA VERIFICA

#### 5.2.3.1 SCADENZA DOCUMENTO IDENTIFICATIVO

Flowe, al fine di permettere la gestione della scadenza del documento identificativo, ha realizzato un “motore di adeguata verifica”, prevedendo uno “scadenziere” automatizzato (processo di *countdown*) che prevede informative verso il cliente coinvolto.

Il processo di *countdown* prevede una serie di comunicazioni che partono da 90gg prima della scadenza del documento identificativo presenti in anagrafe e precisamente:

- Ante 90 gg il cliente riceve un alert sulla scadenza del proprio documento,
- Ante 60 gg il cliente riceve un alert sulla scadenza del proprio documento,
- Ante 30 gg il cliente riceve un alert sulla scadenza del proprio documento,
- Ante 15 gg il cliente riceve un alert sulla scadenza del proprio documento,
- Dopo 30 gg da scadenza documento il cliente riceve un reminder (dalla data scadenza documento avviene il blocco parziale operatività),
- Dopo 60 gg da scadenza documento il cliente riceve un secondo reminder (blocco parziale operatività),
- Dopo 90 giorni da scadenza documento il cliente riceve una notifica finale e viene completamente bloccata la sua operatività in app.

#### 5.2.3.2 SCADENZA PROFILO DI RISCHIO

Il processo di aggiornamento periodico della profilatura della clientela avviene con una frequenza commisurata al relativo livello di rischio, mediante conferma (o aggiornamento), da parte del cliente, dei dati acquisiti precedentemente (adeguata verifica) e mediante compilazione di apposito questionario di adeguata verifica rafforzata previsto per i clienti aventi profilo di rischio ALTO e MEDIO.

Il processo di aggiornamento della profilatura è gestito informaticamente attraverso apposito strumento (cd. motore adeguata verifica). Lo strumento informatico utilizzato consente di:

---

<sup>23</sup> <https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/riciclaggio-terrorismo/faq/pre-2019>

- a) calcolare la data di scadenza del profilo, sulla base della data dell'ultimo aggiornamento anagrafico e del relativo livello di rischio di riciclaggio secondo la tabella di cui al par. 5.1,
- b) effettuare il ricalcolo automatico della data scadenza del profilo di rischio, a seguito della variazione del relativo livello, assumendo come riferimento la data dell'avvenuta variazione e del tempo trascorso dell'ultimo aggiornamento;
- c) attivare il previsto processo di *countdown* nel caso in cui:
  - a. il profilo di rischio in *onboarding* sia Alto o Medio,
  - b. il profilo di rischio diventi Alto o Medio nel continuum,
  - c. scada il profilo di rischio,
- d) gestire il processo di *countdown* previsto, ovvero nell'avvio di una serie di iniziative propedeutiche all'aggiornamento/conferma dei dati contenuti nella sezione Antiriciclaggio dei dati personali nella APP (e nel caso di cliente a rischio Alto o Medio anche dei dati previsti nella sezione di adeguata verifica rafforzata) e /o del documento identificativo partendo da 90 giorni antecedenti l'evento (scadenza documento e/o scadenza profilo di rischio) e fino a 30 giorni successivi alla scadenza impostata (con previsione di apposizione di blocchi operativi del cliente).

Il processo di countdown prevede che quando il profilo è scaduto al cliente venga mandata una comunicazione, venga applicato un primo set di blocchi in app e successivamente:

- dopo 30 gg il cliente riceve un reminder (da data scadenza profilo avviene il blocco parziale operatività),
- dopo 60 gg il cliente riceve un secondo reminder (blocco parziale operatività),
- dopo 90 giorni il cliente riceve una notifica finale e viene completamente bloccata la sua operatività in app

I profili aggiornati come da processo devono essere validati dall'Operatore di Back Office.

L'aggiornamento dei dati e delle informazioni raccolte in sede di profilatura della clientela è richiesto (i) alla scadenza del documento di identità (par. 5.2.2.1) o (ii) a seconda delle previsioni del succitato punto c), nonché (iii) ogniqualvolta il dipendente incaricato rilevi che non sono più attuali le informazioni precedentemente acquisite.

Non è comunque possibile procedere alla instaurazione di nuovi rapporti continuativi con la Società da parte di clienti con "Documenti identificativi" o aggiornamento del "Profilo di Rischio" scaduto, non eseguito o non validato.

#### 5.2.3.3 CLIENTE CON PROFILO DI RISCHIO "ALTO" IN ONBOARDING

E' stato previsto che il cliente profilato a rischio Alto da processo di onboarding, debba obbligatoriamente effettuare l'adeguata verifica rafforzata con tempistiche leggermente differenti lato motore di adeguata verifica:

- Reminder di valorizzazione dei dati aggiuntivi (AVR) (alla data di notifica, dopo 7 giorni, dopo 14 giorni e dopo 21 giorni),
- Dopo 30 gg da scadenza documento il cliente riceve un secondo reminder (blocco parziale operatività - to-do list/app-push),
- Dopo 60 giorni da scadenza documento il cliente riceve una notifica finale e viene completamente bloccata la sua operatività in app.

### 5.3 ADEGUATA VERIFICA RAFFORZATA DELLA CLIENTELA

In presenza di un elevato rischio di riciclaggio e finanziamento del terrorismo, la Società adotta misure rafforzate di adeguata verifica della Clientela, acquisendo informazioni aggiuntive sul Clientela e sul Titolare effettivo, approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto e intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo.

In base al modello adottato dalla Società le attività di rafforzata verifica della Clientela sono demandate ai dipendenti incaricati, i quali sono tenuti a:

- far compilare ai Clienti apposito questionario di adeguata verifica rafforzata, messo loro a disposizione dalla Società;
- acquisire maggiori informazioni sul Cliente e sul Titolare effettivo;
- acquisire/aggiornare e valutare informazioni sulla reputazione del Cliente e/o del Titolare effettivo (ivi comprese eventuali pregiudizievoli, tramite la consultazione di fonti aperte, attraverso, ad esempio, l'utilizzo di motori di ricerca su internet);
- valutare attentamente le informazioni fornite dal Cliente sullo scopo e sulla natura del rapporto, mettendole in relazione con le altre informazioni conosciute all'atto di apertura del medesimo o, nel caso di Clienti che già intrattengono rapporti con la Società, con l'operatività effettivamente rilevata sullo stesso; a tal riguardo, sono presi in considerazione elementi quali: il numero, l'entità e la frequenza delle operazioni effettuate, la provenienza/destinazione dei fondi, la natura dell'attività svolta dal Cliente e/o dal Titolare effettivo, la ragionevolezza delle operazioni effettuate in relazione al profilo complessivo del Cliente;
- svolgere approfondite verifiche sull'origine del patrimonio e dei fondi impiegati nel rapporto continuativo, attraverso un processo articolato che prenda in considerazione, in primis, la attendibilità delle informazioni a disposizione della Società, tenuto conto della eventuale disponibilità di informazioni economico – patrimoniali prodotte direttamente dal Cliente o rilevabili dalla movimentazione del rapporto (es. accredito emolumenti, accredito dividendi, etc.) o reperibili tramite fonti aperte o banche dati pubbliche (es. bilanci, dichiarazioni IVA e dei redditi, atti notarili, dichiarazioni di successione, dichiarazioni/documenti provenienti dal datore di lavoro o da altri intermediari); a tal riguardo, assumono specifica valenza aspetti, quali il grado di conoscenza del Cliente e/o l'anzianità della relazione, la coerenza tra il profilo del Cliente e la sua situazione economico-patrimoniale;
- condurre in modo più frequente la verifica e l'aggiornamento delle informazioni anagrafiche e di quelle raccolte ai fini della conoscenza del Cliente.

La Società prevede, nel caso di:

- rapporti continuativi o operazioni occasionali con Persone Esposte Politicamente,
- operazione/i che coinvolga/no Paesi terzi ad alto rischio.

l'autorizzazione dei soggetti titolari di poteri di amministrazione o direzione ovvero di loro delegati o, comunque, di soggetti che svolgono una funzione equivalente, per quanto sopra riportato deve essere fornita dal Responsabile della Unità Banking Services & Controls.

Resta comunque ferma la possibilità, da parte della Funzione Antiriciclaggio, di chiedere al dipendente che gestisce e amministra nel concreto i rapporti con la Clientela di svolgere il processo



di adeguata verifica rafforzata in tutti i casi, anche non rientranti in quelli sopra elencati, in cui appaia particolarmente elevato il rischio di riciclaggio o finanziamento del terrorismo.

Come indicato al precedente paragrafo, in caso di circostanze oggettive, ambientali o soggettive che rendano più elevato il rischio di riciclaggio, le attività di rafforzata verifica della Clientela sono svolte direttamente dalla Funzione Antiriciclaggio.

In tali ipotesi, il processo di adeguata verifica rafforzata prevede l'acquisizione di informazioni tramite il dipendente che gestisce e amministra nel concreto i rapporti con la Clientela.

La Funzione Antiriciclaggio svolge ulteriori approfondimenti al fine di accertare la coerenza delle operazioni analizzate e delle informazioni raccolte con il patrimonio informativo di cui dispone la Società e, ove opportuno, richiede al Clientela, per il tramite del dipendente incaricato, specifica documentazione.

La Funzione Antiriciclaggio può individuare ipotesi che prevedano il coinvolgimento di ulteriori strutture operative della Società, cui è richiesto di supportare i dipendenti incaricati nell'espletamento delle attività agli stessi affidati ovvero di svolgere verifiche in merito agli esiti delle attività medesime.

#### 5.4 ADEGUATA VERIFICA SEMPLIFICATA DELLA CLIENTELA

In presenza di un basso rischio di riciclaggio e finanziamento del terrorismo, la Società può applicare misure semplificate di adeguata verifica della Clientela sotto il profilo della estensione e della frequenza degli adempimenti, nei confronti di:

- società ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che impongono l'obbligo di assicurare un'adeguata trasparenza della titolarità effettiva;
- pubbliche amministrazioni, ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea;
- enti creditizi o finanziari residenti in Stati membri o in Paesi terzi dotati di efficaci sistemi di prevenzione del riciclaggio e del finanziamento del terrorismo.

Stante l'attuale target di Clientela in perimetro (solo persone fisiche), al momento la Società non assolve tali adempimenti non avendo Clientela su cui poter applicare dette misure.

#### 5.5 ADEGUATA VERIFICA DELLA CLIENTELA ESEGUITA DA TERZI SOGGETTI

La Società si astiene dall'instaurare rapporti continuativi, prestazioni professionali od operazioni occasionali a distanza da parte di terzi soggetti, non assistiti da adeguati meccanismi e procedure di riconoscimento.

#### 5.6 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'offrire prodotti/servizi o dar corso ad operazioni che potrebbero favorire l'anonimato, ovvero l'occultamento dell'identità del Cliente, nonché dall'instaurare Rapporti continuativi o compiere Operazioni Occasionali a distanza, non assistiti da adeguati meccanismi e procedure di riconoscimento.

La Società, infine, non esclude in via preventiva e generalizzata la possibilità di aprire o mantenere Rapporti continuativi con specifiche categorie di clienti o potenziali clienti residenti o con regolare permesso di soggiorno in Italia, in ragione della loro esposizione potenzialmente elevata al rischio di riciclaggio, ma adotta processi rigorosi per valutare, caso per caso, il rischio associato al cliente o al potenziale cliente, mantenendo evidenza delle decisioni assunte.

## 5.7 CONTROLLI PER IL CONTRASTO AL FINANZIAMENTO DEL TERRORISMO

Al fine di assicurare il corretto adempimento degli obblighi e divieti previsti dalla normativa vigente in materia di antiterrorismo, la Società:

- effettua in via automatizzata controlli anagrafici e confronti con i nominativi presenti nelle liste dei soggetti designati dal Consiglio di Sicurezza dell'ONU, dall'Unione Europea, dai decreti del Ministero dell'Economia e delle Finanze, nonché di quella dell'Office of Foreign Asset Control (OFAC) del Dipartimento del Tesoro degli Stati Uniti;
- si rifiuta di compiere operazioni che coinvolgano a qualunque titolo (presentatori, esecutori, ordinanti o beneficiari) soggetti inseriti nelle liste di cui al precedente alinea;
- applica le restrizioni previste sui rapporti di tutti i Clienti per i quali sia accertata la corrispondenza con le liste di cui al primo alinea;
- comunica alla UIF le misure applicate ai sensi del D. Lgs. 109/2007, indicando i soggetti coinvolti, l'ammontare e la natura dei Fondi o delle Risorse economiche, entro trenta giorni dalla data di entrata in vigore dei regolamenti comunitari, delle decisioni degli organismi internazionali e dell'Unione europea e dei decreti del Ministro dell'economia e delle finanze, ovvero, se successiva, dalla data di detenzione dei fondi e delle risorse economiche;
- ha predisposto uno specifico scenario costituito da peculiari indicatori di anomalia (regole) al fine di monitorare in *real time* e con cadenze mensili le transazioni poste in essere dalla Clientela a valere su determinati soggetti/paesi.

## 5.8 SEGNALAZIONE DI OPERAZIONE SOSPETTA

Ai sensi della vigente normativa, la Società invia senza ritardo alla UIF una segnalazione di operazione sospetta, quando sa, sospetta o ha ragionevoli motivi di 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.

I dipendenti delle strutture operative cui compete, nel concreto, l'amministrazione e la gestione dei rapporti con la Clientela rappresentano, ai sensi della normativa vigente, il primo livello segnaletico. È quindi loro compito monitorare nel continuo l'andamento del rapporto e l'operatività posta in essere, anche tramite gli strumenti e le procedure a disposizione, e trasmettere senza ritardo alla Funzione Antiriciclaggio, secondo le procedure e le modalità operative stabilite internamente, una segnalazione di operazione sospetta prima di compiere l'operazione: 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'operazione non possa essere rinviata tenuto conto della normale operatività, ovvero nei casi in cui differimento dell'operazione possa ostacolare le indagini.

Al fine di agevolare l'individuazione delle operazioni sospette, la Società fa riferimento, in particolare, agli indicatori di anomalia emanati e periodicamente aggiornati dalla UIF, predisponendo apposite linee guida e piani di formazione per i dipendenti delle strutture operative.

La Società, nell'ambito della propria autonomia organizzativa si avvale anche di procedure automatiche di individuazione delle operazioni "anomale". La funzione Banking Services & Controls istruisce tutte le pratiche inerenti le segnalazioni ricevute e le invia per il completamento dell'istruttoria alla Funzione Antiriciclaggio che, terminata l'istruttoria e le verifiche previste le sottopone al Delegato alla segnalazione delle Operazioni sospette che, qualora le ritenga fondate alla luce dell'insieme degli elementi a propria disposizione e delle evidenze desumibili dai dati e dalle informazioni conservati, le trasmette alla UIF, prive del nominativo del segnalante.

La Società adotta misure idonee ad assicurare la riservatezza dell'identità delle persone che effettuano la segnalazione di una operazione sospetta; il nominativo del segnalante può essere rivelato solo quando l'Autorità Giudiziaria, disponendo a riguardo con decreto motivato, lo ritenga indispensabile ai fini dell'accertamento di reati per i quali si procede.

È inoltre fatto divieto, ai soggetti tenuti alla segnalazione di una operazione sospetta e a chiunque ne sia a conoscenza, di dare comunicazione al Clientela interessato o a terzi della avvenuta segnalazione, dell'invio di ulteriori informazioni richieste dalla UIF o della esistenza, ovvero della probabilità di indagini in materia di riciclaggio o finanziamento del terrorismo. Tale divieto non si applica:

- alle comunicazioni effettuate alle Autorità di Vigilanza di settore in occasione dell'esercizio delle funzioni previste dal Decreto Antiriciclaggio;
- alle comunicazioni aventi ad oggetto la condivisione delle informazioni a livello di intermediari bancari e finanziari, idonee a garantire la corretta osservanza delle prescrizioni dettate in materia di prevenzione del riciclaggio e del finanziamento del terrorismo;
- alle comunicazioni con altri intermediari bancari e finanziari esterni al Gruppo appartenenti ad uno Stato membro o situati in Paesi terzi, a condizione che questi applichino misure equivalenti a quelle previste dal Decreto Antiriciclaggio, nei casi relativi allo stesso Clientela o alla stessa operazione, per finalità esclusivamente di prevenzione del riciclaggio o del finanziamento del terrorismo.

## 5.9 OBBLIGO DI CONSERVAZIONE DEI DOCUMENTI, DATI E INFORMAZIONI

La Società conserva i documenti, i dati e le informazioni acquisiti in sede di instaurazione del rapporto ed esecuzione del controllo costante, utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo e a consentire lo svolgimento delle analisi

effettuate, nell'ambito delle rispettive attribuzioni, dalla UIF o da altra Autorità competente come prescritto dalla normativa vigente.

La Società ha istituito idonee misure di controllo interno in materia di conservazione al fine di garantire la corretta e completa registrazione dei dati identificativi e delle altre informazioni relative ai rapporti continuativi e alle operazioni.

Per quanto concerne i contratti di Flowe destinati alla Clientela e da quest'ultima sottoscritti con firma digitale di Infocert, quest'ultima, in forza di autonomo contratto stipulato con Flowe (rif. a Servizio LegalDoc) fornisce un servizio di conservazione sostitutiva attualmente disciplinato dalla seguente normativa:

- D.Lgs 82/2005 Codice dell'Amministrazione Digitale (Il sistema di conservazione, come previsto dall'art.44 del CAD, garantisce autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici),
- Linee Guida dell'AgID (Agenzia per l'Italia Digitale) in vigore dal 01 gennaio 2022<sup>24</sup>,
- Deliberazione CNIPA 19.02.2004 n. 11 (regole tecniche),
- D.M del 23 gennaio 2004 (obblighi per i documenti informatici)

a cui il Fornitore ha dichiarato totalmente di conformarsi (anche in caso di future eventuali variazioni della stessa) nell'erogazione dei servizi oggetto dell'accordo.

Per quanto concerne la conservazione di dati, rapporti e operazioni, la Società si è dotata di un sistema di conservazione presso un autonomo centro di servizi<sup>25</sup>, idoneo a garantire il rispetto delle norme dettate dal codice in materia di protezione dei dati personali nonché il trattamento dei medesimi esclusivamente per le finalità in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

Quanto sopra rappresentato permette anche il corretto assolvimento degli obblighi di comunicazione dei dati aggregati concernenti la propria operatività, al fine di consentire alla Unità di Informazione Finanziaria (c.d. UIF) l'effettuazione di analisi mirate a far emergere eventuali fenomeni di riciclaggio o di finanziamento del terrorismo nell'ambito di determinate zone territoriali.

Per quanto riguarda l'assolvimento degli obblighi di conservazione, la Società conserva:

- la copia o i riferimenti dei documenti richiesti ai fini dell'adeguata verifica, per un periodo di dieci anni dalla fine del rapporto continuativo;
- le scritture e le registrazioni delle operazioni e dei rapporti continuativi, consistenti nei documenti originali o nelle copie aventi analoga efficacia probatoria nei procedimenti giudiziari, per un periodo di dieci anni dall'esecuzione dell'operazione o dalla cessazione del rapporto continuativo.

#### 5.9.1 ESENZIONI IN MATERIA DI CONSERVAZIONE DATI E INFORMAZIONI

Ai sensi dell'art. 8, comma 2 delle *“Disposizioni per la conservazione e la messa a disposizione dei documenti, dei dati e delle informazioni per il contrasto del riciclaggio e del finanziamento del terrorismo”* emesse da Banca d'Italia il 26 marzo 2020 e vigenti dallo scorso 01 gennaio 2021, la Società deve indicare nel documento di policy antiriciclaggio se si avvale di una o più delle esenzioni

<sup>24</sup> ai sensi degli artt. 14-bis e 71 del Codice dell'Amministrazione Digitale - decreto legislativo 7 marzo 2005, n. 82

<sup>25</sup> Il sistema di conservazione è gestito dall'outsourcer Nexi Group S.p.A. (ex SIA)

previste dal comma 1 e che si attiene, di conseguenza, alla scelta effettuata in maniera costante nel tempo.

All'attualità stante il perimetro di clientela *target* delle società che non prevede persone giuridiche la Società non si avvale delle succitate previsioni, con riserva di tornare in argomento, laddove si rendesse necessario in funzione del mutato perimetro della clientela *target*.

#### 5.10 FORMAZIONE DEI DIPENDENTI E COLLABORATORI

La Società adotta programmi di formazione ed aggiornamento professionale permanenti, finalizzati alla corretta applicazione delle disposizioni previste dal Decreto Antiriciclaggio e dalle ulteriori disposizioni attuative in materia, al riconoscimento di operazioni connesse al riciclaggio e al finanziamento del terrorismo e all'adozione dei comportamenti e delle procedure da adottare, nonché alla valutazione di specifici *case studies* su fenomeni e/o operatività anomala.

Specifici programmi di formazione sono attuati per il personale appartenente alla Funzione Antiriciclaggio.

L'attività di qualificazione e aggiornamento professionale del personale riveste carattere di continuità e di sistematicità nell'ambito di programmi organici che tengono conto dell'evoluzione della normativa e delle procedure, nonché a quelli comunque coinvolti nel processo di segnalazione di operazioni sospette.

L'attività di qualificazione e aggiornamento professionale del personale riveste carattere di continuità e di sistematicità nell'ambito di programmi organici che tengono conto dell'evoluzione della normativa e delle procedure.

Nel caso di ricorso a un fornitore esterno, il Responsabile Antiriciclaggio accerta che i soggetti cui sia affidato lo svolgimento dell'attività formativa possiedano le conoscenze in materia di antiriciclaggio richieste per garantire la qualità della formazione e che il contenuto di tale formazione sia adeguato alle specificità della Società.

#### 5.11 SISTEMI INTERNI DI SEGNALAZIONE DELLE VIOLAZIONI

La Società adotta specifiche procedure per la segnalazione al proprio interno, da parte di dipendenti e collaboratori, di violazioni potenziali o effettive delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo (c.d. *whistleblowing*).

Tali procedure garantiscono:

- la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto delle segnalazioni;
- la tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
- lo sviluppo di uno specifico canale di segnalazione, anonimo e indipendente, proporzionato alla natura e alle dimensioni del soggetto obbligato.

Tali procedure sono portate a conoscenza di tutto il personale dalla Funzione Internal Audit.

## 5.12 ESERCIZIO DI AUTOVALUTAZIONE DEI RISCHI DI RICICLAGGIO

Ai sensi dell'articolo 15 del Decreto Antiriciclaggio, la Società conduce, con cadenza annuale, un esercizio di autovalutazione dei rischi di riciclaggio.

L'autovalutazione è svolta valutando l'esposizione al rischio di coinvolgimento in fenomeni di riciclaggio per ogni linea di business considerata rilevante, in ragione della propria natura, organizzazione, specificità e complessità operativa, tenendo in considerazione i fattori di rischio legati all'operatività, ai prodotti e servizi, alla tipologia di clientela, ai canali distributivi e all'area geografica, nonché fattori di rischio settoriali previsti dal Titolo II degli Orientamenti dell'Autorità bancaria europea in materia di fattori di rischio per l'adeguata verifica della clientela (EBA/GL/2021/02) vigenti.

L'autovalutazione è condotta sulla base di una metodologia che comprende le seguenti macro-attività:

- identificazione del Rischio Inerente;
- analisi delle Vulnerabilità;
- determinazione del Rischio Residuo;
- azioni di rimedio individuate a fronte delle eventuali criticità esistenti e per l'adozione di opportune misure di prevenzione e mitigazione del rischio di riciclaggio.

L'esercizio è tempestivamente aggiornato quando emergano nuovi rischi di rilevante entità o si verificano mutamenti significativi nei rischi esistenti, nell'operatività o nella struttura organizzativa o societaria.

Gli esiti dell'esercizio di autovalutazione e le iniziative di adeguamento definite alla luce delle risultanze del medesimo e relativo stato di avanzamento sono illustrati in appositi capitoli della Relazione annuale prodotta dalla Funzione Antiriciclaggio.

## 5.13 RISCHI SANZIONATORI E REPUTAZIONALI

Gli adempimenti riportati nella presente Policy, finalizzati al corretto assolvimento delle disposizioni in materia di contrasto al riciclaggio e al finanziamento del terrorismo, devono essere scrupolosamente osservati, per quanto di competenza, da tutto il personale e, in particolare, da coloro che gestiscono e amministrano il rapporto con la Clientela, stante la correlazione posta dal Decreto Antiriciclaggio tra l'entità dei rischi di riciclaggio e finanziamento del terrorismo e le misure di prevenzione adottate dai destinatari delle disposizioni; e questo non solo in fase di apertura di un nuovo rapporto o al compimento di un'operazione occasionale, ma costantemente nel corso della durata della relazione con il Clientela.

Si specifica che, ai sensi di quanto previsto dal Decreto Antiriciclaggio:

- laddove la Società sia ritenuta responsabile, in via esclusiva o concorrente, di violazioni gravi, ripetute o sistematiche ovvero plurime delle disposizioni in materia di obblighi di adeguata verifica della Clientela, di conservazione e di segnalazione ovvero in materia di organizzazione, procedure e controlli interni, nonché delle relative disposizioni attuative adottate dalle Autorità di vigilanza si applica la sanzione amministrativa pecuniaria da 30.000 euro a 5.000.000 ovvero pari al dieci per cento del fatturato complessivo annuo, quando tale importo percentuale è superiore a 5.000.000 di euro e il fatturato è disponibile e determinabile;

- fermo quanto disposto dal precedente punto, si applica la sanzione amministrativa pecuniaria da 10.000 euro a 5.000.000 di euro ai soggetti che svolgono funzioni di amministrazione, direzione e controllo della Società che, non assolvendo in tutto o in parte ai compiti direttamente o indirettamente correlati alla funzione o all'incarico, hanno agevolato, facilitato o comunque reso possibili le violazioni di cui al precedente punto, ovvero hanno inciso in modo rilevante sull'esposizione della Società al rischio di riciclaggio o di finanziamento del terrorismo.

Qualora il vantaggio ottenuto dall'autore della violazione sia superiore a 5.000.000 di euro, la sanzione amministrativa pecuniaria è elevata fino al doppio dell'ammontare del vantaggio ottenuto, purché tale ammontare sia determinato o determinabile.

Si ricorda infine che, in caso di non corretta applicazione degli obblighi previsti dalla normativa antiriciclaggio, ulteriori rischi sono legati alle eventuali sanzioni applicabili alla Società a titolo di responsabilità amministrativa delle persone giuridiche, ai sensi del D. Lgs. 231/2001.

#### 5.14 COORDINAMENTO TRA FUNZIONE ANTIRICICLAGGIO ED ALTRE FUNZIONI DI CONTROLLO

L'interazione tra la Funzione Antiriciclaggio e le altre Funzioni di Controllo si inserisce nel più generale coordinamento tra tutte le funzioni e organi con compiti di controllo, come definito dal Consiglio di Amministrazione al fine di assicurare il corretto funzionamento del sistema dei controlli interni.

## 6 NORMATIVA DI RIFERIMENTO

Il complesso delle disposizioni in materia di contrasto al riciclaggio e al finanziamento del terrorismo sono finalizzate a dettare misure volte a tutelare l'integrità del sistema economico e finanziario e la correttezza dei comportamenti degli operatori tenuti alla loro osservanza.

Tali misure sono proporzionate al rischio in reazione al tipo di Clientela, al rapporto continuativo, alla prestazione professionale, al prodotto, o alla transazione e la loro applicazione tiene conto della peculiarità dell'attività, delle dimensioni e delle complessità proprie dei soggetti obbligati che adempiono agli obblighi previsti a loro carico.

### 6.1 NORMATIVA ESTERNA

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

#### **Prevenzione e contrasto del riciclaggio di denaro e del finanziamento del terrorismo**

##### *Normativa Europea*

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/2022/05 - del 14 giugno 2022, sulle politiche e le procedure relative alla gestione della conformità e al ruolo e alle responsabilità del responsabile antiriciclaggio ai sensi dell'articolo 8 e del capo VI della direttiva (UE) 2015/849, dove specificano il ruolo, i compiti e le responsabilità del responsabile della conformità ai requisiti in materia di antiriciclaggio e contrasto del finanziamento del terrorismo (AML/CFT), dell'organo di gestione e dell'alto dirigente incaricato della conformità ai requisiti in materia di AML/CFT nonché le politiche, i controlli e le procedure interni ai sensi degli articoli 8, 45 e 46 della direttiva (UE) 2015/849.

In data 14 giugno 2022 l'EBA ha altresì pubblicato gli "Orientamenti sulle politiche e le procedure relative alla gestione della conformità e al ruolo e alle responsabilità del responsabile antiriciclaggio ai sensi dell'articolo 8 e del capo VI della direttiva (UE) 2015/849" ("Orientamenti EBA su Politiche e Procedure AML"). Con provvedimento del 1° agosto 2023 - pubblicato nella Gazzetta Ufficiale della Repubblica Italiana in data 16 agosto 2023 - la Banca d'Italia ha modificato le Disposizioni al fine di dare piena attuazione nel nostro ordinamento agli Orientamenti EBA su Politiche e Procedure AML.

In data 11 novembre 2022 l'EBA ha inoltre pubblicato gli "Orientamenti sull'utilizzo di soluzioni di *onboarding* a distanza del cliente per le finalità di cui all'articolo 13, paragrafo 1, della direttiva (UE) 2015/849" ("Orientamenti EBA su Soluzioni di *Onboarding* a Distanza"), recepiti dalla Banca d'Italia con Nota n. 32 del 13 giugno 2023.

In data 31 marzo 2023, l'EBA ha altresì pubblicato:

- gli "Orientamenti sulle politiche e sui controlli per la gestione efficace dei rischi di riciclaggio e finanziamento del terrorismo (ML/TF) nel fornire accesso ai servizi finanziari" ("Orientamenti EBA sul de-risking");
- gli "Orientamenti recanti modifiche agli orientamenti EBA/2021/02 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)" ("Orientamenti EBA sui clienti che sono organizzazioni senza scopo di lucro").

#### *Normativa nazionale*

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

- 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 antiriciclaggio aggregate (o "S.AR.A.");
  - comunicazioni oggettive;
  - conservazione e utilizzo dei dati e delle informazioni a fini antiriciclaggio;

- D. Lgs. 109/2007 e successive modifiche ed integrazioni, recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo internazionale.

Si riportano, inoltre, i seguenti provvedimenti/note di Banca d'Italia:

- Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo - 26 marzo 2019.
- Disposizioni in materia di adeguata verifica della clientela di Banca d'Italia - 30 luglio 2019.
- Disposizioni per la conservazione e la messa a disposizione dei documenti, dei dati e delle informazioni per il contrasto del riciclaggio e del finanziamento del terrorismo – 24 marzo 2020;
- Disposizioni della UIF per l'invio delle segnalazioni antiriciclaggio aggregate – 25 agosto 2020;
- Nota n. 15 del 04 ottobre 2021, con la quale Banca d'Italia da piena attuazione degli Orientamenti dell'Autorità bancaria europea in materia di fattori di rischio per l'adeguata verifica della clientela (EBA/GL/2021/02), aggiornando di conseguenza le Disposizioni in materia di adeguata verifica della clientela di Banca d'Italia emesse il 30 luglio 2019.;
- Nota n. 32 del 13 giugno 2023, con la quale la Banca d'Italia attua gli Orientamenti EBA su Soluzioni di *Onboarding* a Distanza;
- Nota n. 34 del 3 ottobre 2023, con la quale la Banca d'Italia attua gli Orientamenti EBA sul *de-risking*;
- Nota n. 35 del 3 ottobre 2023, con la quale la Banca d'Italia attua gli Orientamenti EBA sui clienti che sono organizzazioni senza scopo di lucro

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

### **Gestione degli embarghi e sanzioni finanziarie**

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

- Carta delle Nazioni Unite (1945) relativa alle misure restrittive finalizzate a favorire il mantenimento o il ripristino della pace e della sicurezza internazionale;
- Trattato sull'Unione Europea del 1992, titolo V relativo alle disposizioni in materia di politica estera e sicurezza comune e s.m.i.;
- Trattato sul Funzionamento dell'Unione Europea del 1957, titolo IV relativo alle disposizioni in materia di politica estera e sicurezza comune, in particolare con riferimento all'applicazione delle misure restrittive e s.m.i.;
- Regolamento (UE) 2021/821 del Parlamento europeo e del Consiglio del 20 maggio 2021 che istituisce un regime dell'Unione di controllo delle esportazioni, dell'intermediazione, dell'assistenza tecnica, del transito e del trasferimento di prodotti a duplice uso;
- Regolamenti dell'Unione Europea attuativi sia delle risoluzioni dell'ONU che di decisioni autonome prese nel quadro della politica estera di sicurezza comune (PESC) recanti misure restrittive nei confronti dei regimi coinvolti in gravi violazioni dei diritti umani e dei Paesi coinvolti nello sviluppo di programmi di arricchimento nucleare non autorizzati;
- Raccomandazioni del GAFI volte a fornire indirizzi operativi per l'applicazione delle sanzioni finanziarie;

- *Code of Federal Regulations, Title 31 – Money and Finance: Treasury, Subtitle B – Regulations Relating to Money and Finance, Chapter V – Office of Foreign Assets Control, Department of the Treasury, Part. 501 – Reporting, Procedures and Penalties Regulations;*
- *Appendix A to CFR Part 501 - Economic Sanctions Enforcement Guidelines;*
- *“A Framework for OFAC Compliance Commitments”.*

### *Normativa nazionale*

La normativa primaria italiana si rinviene nei seguenti provvedimenti:

- 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” e s.m.i.. Tale legge costituisce tuttora la base della disciplina in materia di trasferimenti di beni classificati “materiali d’armamento” e s.m.i.;
- 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 fa in particolare riferimento al Provvedimento della Banca d’Italia del 27 maggio 2009 recante indicazioni operative per l’esercizio di controlli rafforzati contro il finanziamento dei programmi di proliferazione di armi di distruzione di massa e s.m.i..

## 6.2 **NORMATIVA INTERNA**

La presente Policy si inserisce nel più ampio contesto della normativa interna, che comprende, in particolare:

- il Regolamento del processo di gestione delle Persone Esposte Politicamente;
- il Regolamento della Funzione Antiriciclaggio che illustra i principi 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 di segnalazione operazione sospette, in cui sono descritte le fasi dei processi interni propedeutici alla segnalazione di operazioni sospette;
- il Regolamento del processo di conservazione dei documenti, dei dati e delle informazioni, segnalazioni AntiRiciclaggio (S.Ar.A.), controlli di secondo livello AML, in cui sono descritte le fasi dei processi inerenti la tracciatura dei controlli di secondo livello in materia di antiriciclaggio, ivi compresi quelli relativi alla conservazione e registrazione, identificando eventuali azioni a mitigazione della rischiosità rilevata;
- i manuali operativi interni alla Funzione Antiriciclaggio e alle Strutture Operative, che descrivono approfonditamente i processi operativi di dettaglio e gli elementi alla base dei modelli di presidio del Rischio di riciclaggio, con particolare riferimento alla procedura operativa “Onboarding *cliente ed apertura conto di pagamento*” tempo per tempo vigente.

Tale complesso normativo, operativo e procedurale è finalizzato non solo ad adempiere alle inderogabili disposizioni di legge, ma ad evitare il coinvolgimento anche inconsapevole della Società in fatti di riciclaggio e terrorismo.