Global Policy

Policy Antiriciclaggio e Antiterrorismo

FB 013_2020

Funzione Approvante	Consiglio di Amministrazione	**Data** Marzo 2020	
Funzione Proponente	Amministratore Delegato e Direttore Generale		

Index

1. Introduzione e finalità della policy

Il Consiglio di Amministrazione di FinecoBank SpA (di seguito, "Fineco", la "Capogruppo" o la "Banca") in qualità di capogruppo del Gruppo Bancario Fineco (di seguito anche il "Gruppo"), allo scopo di garantire uniformità di comportamenti da parte delle Società del Gruppo in materie importanti come il contrasto al riciclaggio ed al finanziamento del terrorismo ha approvato ed emanato in data 12/03/2020, la "*Global Policy - Antiriciclaggio e Antiterrorismo*" (di seguito "Global Policy").

La presente Policy:

1. Illustra e motiva le scelte che il Gruppo compie in materia di riciclaggio e finanziamento del terrorismo in termini di assetti organizzativi, procedure e controlli interni, adeguata verifica e conservazione dei dati, in coerenza con il principio di proporzionalità e con l'effettiva esposizione al rischio di riciclaggio del Gruppo;

2. delinea il Programma Antiriciclaggio definito dalla Capogruppo attraverso la previsione di:

   - valutazione del rischio antiriciclaggio delle attività svolte (AML Business Risk Assessment);
   - monitoraggio delle novità normative in materia misure di adeguata verifica della clientela;
   - screening dei clienti;
   - monitoraggio delle operazioni dopo l'esecuzione;
   - procedure di segnalazione interna e indagine delle operazioni potenzialmente sospette e, se necessario, la segnalazione esterna di tali operazioni alle competenti Autorità;
   - conservazione della documentazione;
   - formazione dei Dipendenti;
   - gestione delle informazioni e della reportistica;
   - procedure di monitoraggio dell'efficacia dei controlli di cui sopra e
   - prevenzione del finanziamento del terrorismo.

3. fornisce il quadro regolamentare di riferimento, per identificare i potenziali rischi di riciclaggio e finanziamento del terrorismo (di seguito, congiuntamente, "rischio di riciclaggio"), definendo *standard* minimi per i Programmi Antiriciclaggio ai quali le Società del Gruppo devono attenersi.

2. Destinatari

La Policy è indirizzata a tutte le Società del Gruppo e si applica a tutti i Dipendenti.

La Società del Gruppo devono far fronte a potenziali rischi normativi, regolamentari e reputazionali, negli ambiti dell'antiriciclaggio e del contrasto al finanziamento del terrorismo, in virtù sia della clientela diversificata situata in paesi con differenti livelli di rischio di criminalità finanziaria e con diversi regimi normativi, sia dell'ampia gamma di prodotti e servizi offerti.

I clienti, gli azionisti e le Autorità si aspettano che la Banca e tutte le Società del Gruppo identifichino, mitighino e gestiscano tali rischi e pertanto, la relativa mancata gestione può danneggiarne la reputazione e dar luogo a conseguenze legali o regolamentari.

La tutela dal riciclaggio deve avvenire nel migliore dei modi, poiché controlli non sufficientemente rigorosi e/o la mancata applicazione delle pratiche antiriciclaggio, potrebbero esporre la Banca e tutto il Gruppo allo sfruttamento da parte di criminali e generare rischi normativi/reputazionali.

I Dipendenti devono sempre prestare attenzione a situazioni che presentino un potenziale rischio di riciclaggio e finanziamento del terrorismo, gestendole in conformità alla presente *Policy* ed alle normative.

Qualora un Dipendente abbia il sospetto di un potenziale riciclaggio è tenuto a segnalarlo immediatamente seguendo le modalità delineate nella presente Policy e della normativa interna definita dalla Capogruppo. In caso contrario, le Società del Gruppo e/o i Dipendenti possono incorrere in sanzioni amministrative e penali.

Il mancato rispetto della presente *Policy,* nonché qualsiasi violazione della stessa, può dar luogo ad azioni disciplinari - oltre a quelle previste dalla normativa – compresa, nei casi gravi, la risoluzione del rapporto di lavoro.

Offrire supporto a riciclatori o a finanziatori del terrorismo, non individuare e/o segnalare operazioni sospette o informare il soggetto coinvolto dell'avvenuta segnalazione dell'operazione sospetta, può avere serie conseguenze legali, tra cui la reclusione.

3. Il contesto normativo di riferimento

La presente Policy è scritta in conformità alle disposizioni normative vigenti in ambito comunitario e nazionale di cui si riportano qui di seguito quelle principali:

- Direttiva (UE) 2015/849 o IV Direttiva AML/CFT relativa alla prevenzione dell'uso del sistema finanziario ai fini di riciclaggio o finanziamento del terrorismo;

- Regolamento CE 2015/847 riguardante i dati informativi che accompagnano il trasferimento dei fondi;

- Direttiva(UE) 2018/843 o V Direttiva AML/CFT che abroga le Direttive 2005/60/CE e 2006/70/CE e integra la IV Direttiva AML.

- Decreto Legislativo 231/2007 così come modificato dal D. Lgs 90 del 2017 recante attuazione in Italia alla IV Direttiva AML/CFT

- Decreto Legislativo 109/2007 relativo alle misure per prevenire contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE.

- Decreto Legislativo 125/2019 recante attuazione in Italia alla V Direttiva AML/CFT

- Provvedimento della Banca d'Italia del 26 marzo 2019 recante disposizioni su Organizzazione, Procedure e Controlli in materia antiriciclaggio

- Provvedimento della Banca d'Italia del 30 luglio 2019 recanti disposizioni attuative in materia di adeguata verifica della clientela.

4. Glossario e acronimi

Parola chiave	Definizione
Adeguata Verifica o Know Your Customer (KYC)	L'adeguata verifica che la Banca deve eseguire per identificare i propri clienti ed accertare le informazioni rilevanti al fine di eseguire operazioni con loro
Alta Direzione	Il direttore generale, i suoi vicari e chi esercita funzioni equivalenti, nonché i responsabili e i referenti delle funzioni di controllo interno. Per FinecoBank s'intende l'Amministratore Delegato, il Direttore Generale, vice Direttore Generale e i responsabili delle funzioni aziendali di controllo.
Alto Dirigente	Un amministratore o il direttore generale o altro dipendente delegato dall'organo con funzione di gestione o dal direttore generale a seguire i rapporti con la clientela a rischio elevato; l'alto dirigente ha una conoscenza idonea del livello di rischio di riciclaggio o di finanziamento del terrorismo cui è esposto il destinatario ed è dotato di un livello di autonomia sufficiente ad assumere decisioni in grado di incidere su questo livello di rischio.

	Per FinecoBank si tratta dei dipendenti come individuati dal documento dei Poteri Delegati approvato dal Consiglio di Amministrazione.
Autorità di Vigilanza	Autorità preposta alla vigilanza e al controllo di intermediari bancari e finanziari incaricata di emanare normativa specifica in tema di antiriciclaggio e antiterrorismo e che pertanto deve essere rispettata da parte del Gruppo Fineco, ove applicabile. Per l'Italia, le le Autorità di cui al Titolo I, Capo II del d.lgs. 231/2007.
Azionista Intermedio	Entità giuridica in posizione intermedia nella catena di controllo tra il Cliente e l'ultimo proprietario, la quale detiene o controlla almeno il 25% del capitale del Cliente.
Banca di Comodo	Banca (o l'intermediario finanziario che svolge funzioni analoghe ad una banca) priva di una struttura significativa nel paese in cui è stata costituita e autorizzata all'esercizio dell'attività e non appartenente ad un gruppo finanziario soggetto a un'efficace vigilanza su base consolidata.
Capogruppo	Fineco S.p.A. (di seguito anche Fineco" o la "Banca")
Cliente	Il soggetto che instaura o ha in essere rapporti continuativi o compie operazioni occasionali con i soggetti a cui si applicano le presenti disposizioni della normativa antiriciclaggio e antiterrorismo in caso di rapporti continuativi o di operazioni occasionali cointestati a più soggetti, si considera cliente ciascuno dei contestatari
Clienti Corporate	Clienti diversi dalle persone fisiche (società e istituti giuridici) generalmente, ma non esclusivamente, con un'identità separata e distinta da quella dei loro proprietari e soggetti controllanti. I Trust, per esempio, non hanno sempre un'identità separata, ma questa denominazione comprende anche i Trust.
Clienti Private Banking	Allo stato attuale, per Fineco sono i clienti persone fisiche con: i) asset uguale o superiore a 500.000 EUR; ii) associati a un Consulente Finanziario o clienti diretti; iii) il cui conto corrente è associato a una delle convenzioni specificamente individuate dalla Banca. Tale clientela non è destinataria di "servizi bancari personalizzati", ma è esclusivamente destinataria di alcune condizioni agevolate connesse ai medesimi prodotti e servizi offerti a tutta la clientela. In virtù di ciò, le misure definite per i soggetti Private[1] così come definiti nella normativa vigente non sono applicabili alla clientela Private di Fineco. Ove venissero sviluppati i servizi bancari personalizzati, si provvederà ad adeguare tali misure. *1 "Clienti con elevato patrimonio netto, a cui sono dedicati servizi personalizzati (compresi, tra l'altro, conto corrente, transazioni di importo elevato, uso di prodotti sofisticati, soluzioni di investimento non standard; società off-shore o estere, trust/amministrazioni fiduciarie o veicoli di investimento personali, cassette di sicurezza), ulteriori rispetto a quelli standard offerti a clienti al dettaglio, da parte di Relationship Managers dedicati. Non tutti i clienti ricompresi nella Divisione Private Banking si qualificano automaticamente come clienti Private Banking ai sensi della presente Policy."*
Controllata	Entità direttamente o indirettamente controllata da FinecoBank S.p.A. (di seguito anche "Entità controllata" o "Società controllata" o in breve "LE")
Controlli Addizionali dei Nominativi	Ricerca, condotta tramite un media provider esterno, al fine di individuare problemi reputazionali e/o normativi collegati ad un Cliente, quali informazioni negative, sanzioni, PEP, ecc. Un esempio di media provider esterno è World Check, gestito da Global World-Check Holdings Limited. Anche internet può essere utilizzato per ulteriori ricerche di informazioni. Si veda di seguito i "Controlli Standard sui Nominativi".
Controlli Standard sui Nominativi	Vaglio dei nominativi dei clienti e dei Soggetti Collegati con i nominativi contenuti sia nelle pertinenti liste dei soggetti sanzionati, sia in quelle interne di Fineco.

Dipendenti	Ai fini di questa Rule e indipendentemente dalla legislazione laburistica vigente si intendono come Dipendenti tutti i membri degli organi di supervisione strategica, di gestione e di controllo, i dipendenti, agenti monomandatari (ad es. consulenti finanziari abilitati all'offerta fuori sede), lavoratori autonomi o a contratto, qualsiasi altro individuo con un rapporto lavorativo (compresi gli stagisti) e lavoratori temporanei.
Entità Regolamentata	Ente creditizio o finanziario (comprese banche la cui licenza non sia limitata all'attività bancaria offshore), intermediari, società assicurative, società di gestione collettiva e fondi regolamentati che sono soggetti alla disciplina emessa da un'autorità di vigilanza.
Finanziamento del terrorismo	Erogazione o raccolta di fondi, in qualsiasi modo effettuata, direttamente o indirettamente, con la finalità o nella consapevolezza che essi sono destinati in tutto o in parte al compimento di atti terroristici. I fondi utilizzati per il finanziamento del terrorismo possono provenire tanto da attività lecite quanto da attività illecite.
Firmatario	Delegato o rappresentante dotato del potere di impegnare la società in un accordo o in una transazione.
Fonte Dati Riconosciuta	Una fonte che la Banca o il Gruppo riconosce tale per la raccolta di informazioni e/o la verifica di elementi relativi all'identità di un Cliente.
Gruppo	Gruppo Fineco, composto da Fineco S.p.A. e dalle Società del Gruppo (di seguito anche "Gruppo Fineco")
Indirizzo della sede principale di attività	La sede principale delle attività ordinarie condotte dal Cliente. Normalmente coincide con la sede centrale della società (es. la direzione generale).
Operazione Occasionale	Operazione non riconducibile ad un rapporto continuativo in essere con un cliente, sia che venga effettuata con una transazione unica, sia che comprenda più transazioni che appaiono collegate.
Organi Aziendali	Il complesso degli organi con funzioni di supervisione strategica, di gestione e di controllo. In FinecoBank tali organi sono da intendersi rispettivamente il Consiglio di Amministrazione, l'Amministratore Delegato e Direttore Generale, il Collegio Sindacale.
Origine dei Fondi	L'origine dei fondi oggetto di un rapporto commerciale o di un'operazione occasionale. Include sia le attività che hanno generato i fondi utilizzati nel Rapporto Commerciale, sia le modalità attraverso le quali i fondi del Cliente sono stati trasferiti.
Origine del Patrimonio	Attività economica o attività che ha generato il patrimonio netto di un Cliente persona fisica o Corporate. Questo, per esempio, potrebbe provenire da attività di impresa, vendita di un'attività o di beni, risparmi da lavoro dipendente , un prestito, etc.
Paesi terzi ad Alto Rischio	Paesi non appartenente allo Spazio economico europeo con carenze strategiche nei rispettivi regimi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo, come individuati dalla Commissione europea nell'esercizio dei poteri disciplinati dagli articoli 9 e 64 della direttiva antiriciclaggio;
Operatività a Distanza	Per operatività a distanza si intende quella svolta senza la compresenza fisica, presso l'intermediario, del cliente, dei dipendenti dell'intermediario o di altro personale incaricato dall'intermediario (es., attraverso i sistemi di comunicazione telefonica o informatica); quando il cliente è un soggetto diverso da una persona fisica, esso si considera presente quando lo è l'esecutore.
Persona Politicamente Esposta (PEP)	Qualsiasi persona che occupi (o abbia occupato) una posizione pubblica preminente/importante, o che sia in strettamente collegata o in rapporto di parentela diretto con una persona in tale posizione.

Reato Finanziario	Ogni tipo di condotta criminosa relativa all'uso del sistema finanziario, tra cui, non a titolo esaustivo: • frode o disonestà; • illecito o abuso di informazioni nel mercato finanziario; • utilizzo dei proventi del reato; • corruzione; • concussione; • reati fiscali; • finanziamento del terrorismo; • reati relativi alle sanzioni.
Red flag/Indicatori di anomalia	Tipologie o indicatori di rischio utilizzati per identificare comportamenti generalmente riconducibili ad attività di riciclaggio o di finanziamento del terrorismo.
Relazioni d'Affari Vietate	Relazioni bancarie che non si devono instaurare o che devono essere chiuse in virtù di requisiti normativi o di policy interne.
Remote Banking	Operazione bancaria effettuata tramite mezzi elettronici da una postazione remota (ad esempio banca telefonica, internet banking tramite PC o dispositivi mobili) in cui il contratto con il cliente viene eseguito senza incontri di persona.
Riciclaggio del denaro	Attività volta a nascondere la provenienza illecita dei proventi del crimine, creando la parvenza di un'origine lecita, anche quando le attività che hanno generato i capitali da riciclare siano state condotte all'estero. Ai sensi dell'articolo 2, comma 4, del decreto antiriciclaggio, il riciclaggio include: 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 agevolarne l'esecuzione;
Servizio Fiduciario	Servizio di gestione degli asset che consiste nella nomina, da parte del proprietario dell'asset, di una terza parte che gestisca tali asset attraverso una combinazione di servizi di consulenza ed investimento.
Settore ad Alto Rischio	Settore definito dalla Banca come esposto alla corruzione, alla concussione, alla frode, ad altri reati finanziari, a comportamenti finalizzati a riciclare proventi illeciti, o fondi destinati a finanziare il terrorismo.
Società Fiduciaria	Società costituita per detenere (intestatario registrato) e amministrare in qualità di custode attività per conto di un'altra persona o società.
Società del Gruppo	Società del Gruppo FinecoBank, intendendo la stessa Capogruppo FinecoBank e le sue Società controllate.
Soggetto Collegato	I soggetti individuati all'interno della catena partecipativa e di controllo che esercitano il controllo quotidiano, i firmatari autorizzati, il rappresentante

	legale e i Titolari Effettivi.
Soggetto Sanzionato	Persona o società o nazione con cui è vietato/limitato per legge intrattenere rapporti commerciali e compiere transazioni (Unione Europea, OFAC-USA, o altre autorità o agenzie governative internazionali o locali).
Titolare Effettivo	La persona fisica o le persone fisiche per conto delle quali il Cliente instaura un rapporto continuativo o realizza un'operazione (in breve, "titolare effettivo sub 1"); Nel caso in cui il Cliente o il soggetto per conto del quale il Cliente instaura un rapporto continuativo ovvero realizza un'operazione siano entità diverse da una persona fisica: la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile la proprietà diretta o indiretta dell'entità oppure il relativo controllo o che ne risultano beneficiari (in breve, "titolare effettivo sub 2"). In particolare, in caso di società di capitali o altre persone giuridiche private, anche se con sede all'estero, e trust espressi, indipendentemente dal relativo luogo di istituzione e dalla legge ad essi applicabile, il titolare effettivo sub 2) è individuato secondo i criteri previsti dagli articoli 20 e 22, comma 5, del decreto antiriciclaggio; gli stessi criteri, si applicano, in quanto compatibili, in caso di società di persone e di altri soggetti giuridici, pubblici o privati, anche se privi di personalità giuridica.
Trasferimento di fondi	Qualsiasi operazione eseguita con mezzi elettronici per conto di un ordinante attraverso un prestatore di servizi di pagamento, con lo scopo di rendere i fondi disponibili ad un beneficiario presso un Prestatore di Servizi di Pagamento, indipendentemente dal fatto che l'ordinante e il beneficiario siano la stessa persona.
Verifica	Controllo di veridicità delle prove documentali presentate da un Cliente o da una Fonte Dati Riconosciuta per convalidare le informazioni sull'identità.

Acronimo	Definizione
AFC	Anti-Financial Crime
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CTF	Countering of Terrorist Financing
CPI	Corruption Perception Index
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know Your Customer
KYT	Know Your Transaction
OFAC	US Office of Foreign Assets Control of the US Department of the Treasury
PEP	Politically Exposed Person
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
SPV	Special Purpose Vehicles
STR	Suspicious Transaction Report
UIF	Unità d'Informazione Finanziaria istituita presso Banca d'Italia

5. Ruolo e responsabilità degli Organi Aziendali della Capogruppo

5.1. *Organo con funzioni di Supervisione Strategica*

Il Consiglio di Amministrazione di Fineco, quale organo con funzione di supervisione strategica, approva e riesamina periodicamente gli indirizzi strategici e le politiche di governo dei rischi connessi con il riciclaggio; in aderenza all'approccio basato sul rischio, le politiche sono adeguate all'entità e alla tipologia dei rischi cui è concretamente esposta l'attività della Banca, come rappresentati nel documento di autovalutazione dei rischi.

In particolare, il Consiglio di Amministrazione di Fineco

- approva la presente policy ed ogni successivo aggiornamento della stessa che illustra e motiva le scelte che la Banca compie sui vari profili rilevanti in materia di assetti organizzativi, procedure e controlli interni, adeguata verifica e conservazione dei dati, in coerenza con il principio di proporzionalità e con l'effettiva esposizione al rischio di riciclaggio;
- 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 di controlli interni organico e coordinato, funzionale alla pronta rilevazione e alla gestione del rischio di riciclaggio e ne assicura l'efficacia nel tempo;
- approva i principi per la gestione dei rapporti con la clientela classificata ad "alto rischio";
- nomina e revoca il responsabile delle segnalazioni di operazioni sospette e il responsabile antiriciclaggio, sentito l'organo con funzioni di controllo;
- assicura che i compiti e le responsabilità in materia antiriciclaggio siano allocati in modo chiaro e appropriato, garantendo che le funzioni operative e quelle di controllo siano distinte e 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 la tutela della riservatezza nell'ambito della procedura di segnalazione di operazioni sospette;
- con cadenza almeno annuale, esamina le relazioni relative all'attività svolta dal responsabile antiriciclaggio e ai controlli eseguiti dalle funzioni competenti, nonché il documento sui risultati dell'autovalutazione dei rischi di riciclaggio;
- 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;
- valuta i rischi conseguenti all'operatività con paesi terzi associati a più elevati rischi di valuta i rischi di riciclaggio, individuando i presidi per attenuarli, di cui monitora l'efficacia.

5.2. *Organo con funzioni di Gestione*

L'Organo con Funzione di Gestione di Fineco è costituito dall'Amministratore Delegato e dal Direttore Generale.

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. Nella predisposizione delle procedure operative tiene conto 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, l'Organo con Funzione di Gestione 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

Inoltre, l'Organo con Funzione di Gestione:

- assicura il tempestivo assolvimento degli obblighi di comunicazione alle Autorità previsti dalla normativa antiriciclaggio.
- definisce la policy antiriciclaggio sottoposta all'approvazione dell'organo con funzione di supervisione strategica 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 dall'organo di supervisione strategica;
- stabilisce i programmi di addestramento e formazione del personale sugli obblighi previsti dalla disciplina antiriciclaggio; l'attività di formazione deve rivestire carattere di continuità e sistematicità e tenere conto dell'evoluzione della normativa e delle procedure predisposte dal destinatario;
- 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 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.

5.3. *Organo con funzioni di Controllo*

L'Organo con Funzione di Controllo (il Collegio Sindacale) vigila sull'osservanza della normativa e sulla completezza, funzionalità e adeguatezza dei sistemi di controllo antiriciclaggio. Nell'esercizio delle proprie attribuzioni, si avvale delle strutture interne per lo svolgimento delle verifiche e degli accertamenti necessari e utilizza flussi informativi provenienti dagli altri Organi Aziendali, dal Responsabile Antiriciclaggio e, ove presenti, dalle altre funzioni di controllo interno.

In tale ambito, l'organo con funzione di controllo:

- valuta l'idoneità delle procedure per l'adeguata verifica della clientela, la conservazione delle informazioni e la segnalazione delle operazioni sospette;
- analizza i motivi delle carenze, anomalie e irregolarità riscontrate e promuove l'adozione delle opportune misure correttive;
- è sentito nelle procedure di nomina del responsabile della funzione antiriciclaggio e del responsabile delle segnalazioni di operazioni sospette e nella definizione degli elementi dell'architettura complessiva del sistema di gestione e controllo del rischio di riciclaggio.
- comunica senza ritardo alla Banca d'Italia tutti i fatti di cui vengano 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.

6. Ruolo e responsabilità delle Funzioni Aziendali

6.1. La Funzione Antiriciclaggio della Capogruppo e delle Controllate

La Funzione Antiriciclaggio è la funzione deputata a prevenire e contrastare la realizzazione di operazioni di riciclaggio.
La Funzione Antiriciclaggio è indipendente, dotata di risorse qualitativamente e quantitativamente adeguate ai compiti da svolgere, riferisce direttamente agli organi con funzioni di supervisione strategica, gestione e controllo e ha accesso a tutte le attività nonché a qualsiasi informazione rilevante per lo svolgimento dei propri compiti.

La Funzione Antiriciclaggio ha il compito di:

a) identificare leggi, regolamenti e linee guida, a livello locale e valutare il loro impatto sui processi e le procedure interne e monitorarne le modifiche per garantire i relativi aggiornamenti interni;
b) collaborare alla definizione del sistema dei controlli interni e delle procedure finalizzati alla prevenzione e al contrasto dei rischi di riciclaggio;
c) verificare nel continuo l'adeguatezza del processo di gestione dei rischi di riciclaggio e l'idoneità del sistema dei controlli interni e delle procedure adottate dalle e proporre, coinvolgendo le altre strutture aziendali interessate, le modifiche organizzative e procedurali necessarie od opportune al fine di assicurare un adeguato presidio dei rischi;
d) condurre, in raccordo con il responsabile delle segnalazioni sospette ("SOS"), verifiche sulla funzionalità del processo di segnalazione e sulla congruità delle valutazioni effettuate dal primo livello sull'operatività della clientela;
e) collaborare 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;
f) condurre, in raccordo con le altre funzioni aziendali interessate, l'esercizio annuale di autovalutazione dei rischi di riciclaggio ove la stessa sia richiesta dalla normativa locale;
g) prestare supporto, assistenza e consulenza agli Organi Aziendali e all'Alta Direzione (anche in caso di offerta di prodotti e servizi nuovi), nonché su tematiche connesse all'apertura e chiusura di rapporti con i clienti;
h) valutare in via preventiva il rischio di riciclaggio connesso all'offerta di prodotti e servizi nuovi;
i) verificare l'affidabilità del sistema informativo per l'adempimento degli obblighi di adeguata verifica della clientela, conservazione dei dati e segnalazione delle operazioni sospette;
j) trasmettere mensilmente alle autorità locali (UIF per la Capogruppo) i dati aggregati concernenti l'operatività complessiva della Banca, ove richiesti dalla normativa locale;
k) trasmettere alle autorità locali (UIF per la Capogruppo), sulla base delle istruzioni dalla stessa emanate, le comunicazioni oggettive concernenti operazioni a rischio di riciclaggio, ove richiesto dalla normativa locale;
l) curare, 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 dipendente e dei collaboratori e ad una loro sensibilizzazione alla conformità con la presente Policy e con gli adempimenti normativi;
m) informare tempestivamente gli Organi Aziendali di violazioni o carenze rilevanti riscontrate nell'esercizio dei relativi compiti e in generale;
n) predisporre flussi informativi diretti agli Organi Aziendali e all'Alta Direzione.

La Funzione Antiriciclaggio della Capogruppo, e ove previsto dalla normativa locale delle Società Controllate, redige e trasmette all'organo con funzione di gestione e a quello con funzione di supervisione strategica un documento che definisce dettagliatamente responsabilità, compiti e modalità operative nella gestione del rischio di riciclaggio (cd. Manuale Antiriciclaggio). Il documento - costantemente aggiornato - è disponibile e facilmente accessibile a tutto il personale.

La Funzione Antiriciclaggio delle Capogruppo e delle Controllate pone particolare attenzione: all'adeguatezza dei sistemi e delle procedure interne in materia di obblighi di adeguata verifica della clientela e di conservazione nonché dei sistemi di individuazione, valutazione e segnalazione delle 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.

Almeno una volta l'anno, la Funzione Antiriciclaggio presenta agli organi con funzione di supervisione strategica, gestione e controllo (per la Capogruppo o organi equivalenti per le Società Controllate) una relazione sulle iniziative adottate, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale e dell'esercizio di autovalutazione, ove tale esercizio sia richiesto dalla normativa locale.

La Funzione Antiriciclaggio della Capogruppo si inserisce nell'ambito della Unit Compliance della Capogruppo.

6.2. Il Responsabile Antiriciclaggio della Capogruppo e delle Controllate

A capo della Funzione Antiriciclaggio, è nominato il Responsabile della Funzione Antiriciclaggio che deve essere in possesso di adeguati requisiti di indipendenza, autorevolezza e professionalità e riferisce direttamente agli Organi di Governo delle rispettive Società del Gruppo.

Il Responsabile della Funzione Antiriciclaggio non ha responsabilità dirette di aree operative, né è gerarchicamente dipendente da soggetti responsabili di dette aree.

Il Responsabile Antiriciclaggio della Capogruppo con il supporto della struttura Advisory & Regulators e del Servizio Antiriciclaggio e Antiterrorismo ha la responsabilità di:

- predisporre un efficace Programma Antiriciclaggio (incluse le Group Rules in materia);
- fornire consulenza, coordinare e supervisionare l'implementazione dei Programmi Antiriciclaggio delle Società del Gruppo;
- analizzare l''informativa periodica ricevuta dalle Società Controllate e attivarsi di concerto con il Responsabili Antiriciclaggio locali per le eventuali azioni migliorative e correttive del caso.

Il Responsabile Antiriciclaggio della Controllata, avvalendosi delle strutture e delle risorse che operano nell'ambito della Funzione Antiriciclaggio locale ha la responsabilità di:

- implementare il Programma Antiriciclaggio coerentemente con le linee di indirizzo definite dalla Capogruppo;
- effettuare controlli in ambito antiriciclaggio e antiterrorismo coerentemente con quanto definito nelle Global Rules;
- effettuare l'esercizio del Business Risk Assessment e la valutazione del rischio di riciclaggio;
- svolgere l'attività di individuazione e analisi di eventuali anomalie e operazioni sospette identificate e riportate alle autorità locali competenti come richiesto dalla normativa locale;
- monitorare gli sviluppi normativi locali e proporre gli eventuali adeguamenti;
- predisporre un'informativa periodica alla Capogruppo contenente almeno le informazioni e i dati di cui sopra.

Relativamente all'eventuale calibrazione e all'implementazione da parte delle Società Controllate, il Responsabile Antiriciclaggio della Capogruppo si avvale del supporto del Servizio Antiriciclaggio e Antiterrorismo, stabilendo degli standard minimi di Antiriciclaggio per ciascuna Legal Entity appartenente al Gruppo.

6.3. Capogruppo - Il Servizio Antiriciclaggio e Antiterrorismo e il Responsabile SOS

Il ruolo operativo della Funzione Antiriciclaggio è principalmente attribuito al Servizio Antiriciclaggio e Antiterrorismo (nel seguito anche il "Servizio Antiriciclaggio") che, come da delibera del Consiglio di Amministrazione del 15 marzo 2010, è allocato in organigramma a riporto diretto della Unit Compliance.
In dettaglio, le attività e i compiti svolti dal Servizio Antiriciclaggio sono definiti nel Manuale Antiriciclaggio della Banca oltre che nei processi aziendali.

Nell'ambito del Servizio Antiriciclaggio opera il team dedicato alle Segnalazioni di Operazioni Sospette con a capo il Responsabile SOS, nominato con delibera del Consiglio di Amministrazione, sentito il Collegio Sindacale. La Banca predispone processi e procedure interne che normano le attività svolte dal Responsabile SOS e del team SOS dedicato alla valutazione di potenziali operazioni sospette per successivo inoltro all'UIF.

6.4. Capogruppo - Altre Funzioni

Fermo l'obbligo di calibrare gli assetti organizzativi antiriciclaggio secondo il principio di proporzionalità e di approccio in base al rischio, la Banca attribuisce specifiche responsabilità (assegnate alla struttura indicata tra parentesi nel seguente elenco) in ordine alla:

- Verifica in modo continuativo del grado di adeguatezza dell'assetto organizzativo antiriciclaggio e la sua conformità rispetto alla normativa (Internal Audit)
- Implementazione delle regole di identificazione e verifica dei dati relativi alla clientela e di quelle relative all'adeguata verifica (Back Office)
- predisposizione e aggiornamento dei processi aziendali che includono i controlli di linea, (a cura di Sviluppo Organizzativo e Business Continuity in collaborazione con il Process Owner di riferimento);
- definizione di specifici programmi di formazione del personale (HR);
- predisposizione e gestione degli strumenti informatici di supporto (ICT).

Le varie strutture aziendali, cui è attribuita la responsabilità di ciascun compito, collaborano con la Funzione Antiriciclaggio ed hanno l'obbligo di trasferire alla stessa qualsiasi informazione relativa a fatti interni o esterni aventi possibili implicazioni in tema di Antiriciclaggio.

7. AML Business Risk Assessment

Le Società del Gruppo valutano il rischio di riciclaggio connesso alle attività svolte/servizi prestati. La valutazione del rischio considera, come minimo, il rischio di riciclaggio presentato dai clienti, prodotti e servizi, dalle giurisdizioni in cui le Società del Gruppo operano od offrono i loro servizi, e dalle transazioni o canali di distribuzione utilizzati al servizio dei clienti. La valutazione del rischio deve essere adeguata alla natura e alle dimensioni delle strutture e del business e viene documentata e fornita, a cura della Funzione Antiriciclaggio delle stesse, almeno annualmente, agli Organi Aziendali.

La valutazione del rischio di riciclaggio è utilizzata per calibrare sia l'adeguata verifica della clientela, sia le procedure di monitoraggio delle operazioni relative ad ogni categoria di rischio della clientela. Completata la valutazione del rischio, le Società del Gruppo si assicurano di avere risorse, normative interne, procedure e controlli adeguati per attenuare, per quanto possibile, i rischi identificati.

Per l'individuazione del profilo di rischio della clientela, le Società del Gruppo, ove opportuno, traggono informazioni da ogni fonte e documento utile, tra cui i rapporti ufficiali pubblicati da autorità europee e nazionali (il cd. Supernational Risk Assessment Report della Commissione Europea, l'Analisi Nazional del Rischio, adottato dal Comitato di Sicurezza Finanziario) e altri documenti provenienti dalle altre autorità di vigilanza e da altre autorità locali.

7.1. Valutazione del rischio e classificazione del cliente

I Clienti devono essere valutati singolarmente al fine di individuare e classificare il livello di rischio di riciclaggio, finanziamento del terrorismo e reati finanziari e per determinare se sia opportuno entrare in rapporto con il Cliente stesso. La valutazione del rischio del Cliente e la sua classificazione in termini di rischio di riciclaggio rappresentano elementi sostanziali dell'approccio basato sul rischio, permettendo di concentrare i controlli (come le misure di Due Diligence e il monitoraggio delle transazioni) e l'uso di risorse, sui clienti più rischiosi. Nell'identificare i fattori di rischio inerenti al Cliente, la Capogruppo considera anche il Titolare Effettivo e, ove rilevante, l'Esecutore come indicato nelle sezioni seguenti.

APPROCCIO BASATO SUL RISCHIO

Per valutare il rischio di riciclaggio e di finanziamento del terrorismo, le Società del Gruppo fanno riferimento alle caratteristiche del Cliente, alla sua condotta e alle specificità dell'operazione o del rapporto continuativo da instaurare.

In particolare, si prendono in considerazione i seguenti fattori di rischio:

- Rischio paese, ossia l'area geografica di residenza o sede del Cliente o del Titolare Effettivo;
- Rischio di settore e la prevalente attività svolta dal Cliente e dal Titolare Effettivo;
- Rischio del prodotto e del servizio richiesto;
- Rischio Entità per clienti diversi dalle persone fisiche;
- Rischio PEP
- Rischio reputazionale (es. informazioni negative).

Le Società del Gruppo, proporzionalmente alla dimensione e tipologia di business svolto, si dotano di procedure volte ad assicurare che tutti i nuovi clienti e, ove rilevante, gli amministratori, i titolari effettivi e altre persone collegate (legale rappresentante, delegato autorizzato, etc.), siano sottoposti a *screening* rispetto a un *database* contenente:

- le liste delle Sanzioni secondo i requisiti della normativa interna sulle Sanzioni Finanziarie";
- le liste PEPs fornite da un'organizzazione commerciale autorevole quale World Check;
- eventuali altre liste interne di volta in volta emanate dalla Capogruppo e/o dalle Società Controllate;
- una lista di notizie negative fornita da un'organizzazione commerciale autorevole quale World Check (nel caso di clienti ad alto rischio, si devono verificare anche i nomi degli azionisti con quote del 10% o superiori).

Le Società del Gruppo valutano la sussistenza del rischio AML per ogni cliente sulla base degli elementi raccolti tramite l'adeguata verifica - anche sulla scorta di apposito questionario - e delle verifiche effettuate e attribuiscono il corrispondente profilo di rischio in base alle tre categorie individuate ("basso"; "medio"; "alto") e descritte più in dettaglio nelle sezioni seguenti.

Il profilo di rischio è consultabile dagli operatori interessati consentendo estrazioni sulla base di diversi parametri di ricerca.
Le Società del Gruppo utilizzano, come minimo, i seguenti fattori, nel determinare una metodologia per la classificazione del profilo di rischio della clientela:

RISCHIO PAESE

Il rischio paese è il rischio di reati finanziari relativo ai paesi da cui i clienti, i titolari effettivi e gli esecutori provengono o dove operano, e cioè il rischio che gli stessi, a causa della loro provenienza o luogo di attività, siano coinvolti in qualche tipo di Reato Finanziario: riciclaggio, finanziamento del terrorismo, corruzione, frode o una combinazione di questi.

La normativa sulle Sanzioni Finanziarie identifica i paesi sanzionati mentre la classificazione della rischiosità dei Paesi nelle categorie a basso, medio o alto rischio è indicata nella GOR – Requisiti di Adeguata Verifica della Clientela in materia di Antiriciclaggio. La classificazione tiene conto della stabilità politica di un Paese, dei suoi controlli e dei sistemi di prevenzione antiriciclaggio, e della vulnerabilità a reati finanziari.

Ai fini della classificazione del rischio Cliente, hanno rilievo (con riferimento al cliente stesso, al titolare effettivo e ove rilevante l'esecutore) i seguenti criteri:

- per le persone fisiche: il Paese in cui sono normalmente residenti, la loro cittadinanza o l'area geografica di provenienza (anche dei fondi), i paesi con cui vi siano collegamenti significativi. In particolare, quando il cliente è residente in un'area geografica a rischio elevato, le Società del Gruppo valutano se sussiste una valida ragione economica o legale che giustifica la tipologia di rapporto continuativo o di operazione richiesti ovvero se le necessità del cliente possano essere più propriamente soddisfatte nel paese di residenza.
- per le entità giuridiche:
  - il Paese in cui operano e/o dove sono registrate e/o dove hanno sede;
  - il Paese di cui il Titolare Effettivo ha la cittadinanza,

- il Paese in cui il Titolare Effettivo è residente, e i paesi con cui lo stesso abbia collegamenti significativi

RISCHIO DI SETTORE

Il rischio di settore è il rischio di Reati Finanziari relativo al settore, al tipo di professione o all'attività economica in cui opera il Cliente, il Titolare Effettivo e ove rilevante l'Esecutore. Alcuni settori economici presentano un elevato rischio di riciclaggio (rilevano in tal senso, le attività economiche caratterizzate da elevato utilizzo di contante quali il settore dei compro oro, dei cambiavalute, del gioco o delle scommesse, casinò o money transfer, commercio in antichità, case d'asta e gallerie d'arte; commercio di rottami ferrosi) o risultano essere settori particolarmente esposti a rischi di corruzione (settori economici interessati dall'erogazione di fondi pubblici, anche di origine comunitaria, quali ad esempio commercio di armi e dual use; raccolta e smaltimento di rifiuti; produzione di energie rinnovabili); alcuni settori hanno una maggiore propensione alla corruzione (es. edilizia, telecomunicazioni, ecc.) laddove dipendano da appalti o licenze pubbliche; altri settori possono presentare un basso rischio di reati finanziari ma, nei paesi ad alto livello di corruzione, il rischio può salire notevolmente a causa dell'alto grado di dipendenza da licenze o appalti pubblici.
Laddove un'entità dovesse essere coinvolta in più di un'attività o settore, prevarrà il settore primario o quello dove la maggior parte delle attività è svolta.
I settori classificati e valutati dalla Capogruppo come ad alto rischio sono riportati nella GOR- Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio.

RISCHIO DI PRODOTTO E DI SERVIZIO

Alcuni prodotti e servizi sono intrinsecamente più vulnerabili a reati finanziari, ad esempio perché la natura del prodotto permette la rapida trasmissione di fondi tra soggetti diversi.
La GOR- Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio fornisce l'elenco dei prodotti e dei servizi classificati ad alto rischio.

RISCHIO ENTITÀ

Alcune entità presentano un maggiore rischio di reati finanziari a causa della mancanza di trasparenza riguardo alla proprietà o a causa di strutture societarie e *trust* qualificabili come veicoli di interposizione patrimoniale.
La GOR- Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio. identifica le tipologie di clienti/entità o persone giuridiche considerate ad alto rischio dalle Società del Gruppo.

RISCHIO DI PERSONA POLITICAMENTE ESPOSTA E DI CARICA PUBBLICA RICOPERTA

Le Persone Politicamente Esposte (o PEP) sono considerate a più alto rischio riciclaggio in quanto maggiormente esposte ai potenziali rischi di corruzione. La qualificazione di PEP assume rilievo per il Cliente della Banca, per il Titolare Effettivo e per l'Esecutore.
Quando il Cliente, il Titolare Effettivo o l'Esecutore rientrano nella definizione di PEP, le Società del Gruppo assicurano che l'avvio o la prosecuzione del rapporto continuativo, ovvero l'esecuzione dell'operazione occasionale siano autorizzati da un Alto Dirigente che valuta l'esposizione al rischio di riciclaggio della PEP e il grado dei presidi aziendali in essere per mitigare il rischio.

In linea con la normativa locale di riferimento, la Capogruppo identifica come PEP le persone fisiche che occupano o che hanno cessato di occupare da meno di un anno le cariche pubbliche indicate come da art. 1, lettera dd) del decreto antiriciclaggio, nonché i loro familiari e coloro che con i predetti intrattengono notoriamente stretti legami.

Maggiori dettagli sono forniti nella_GOR - Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio.

RISCHIO REPUTAZIONALE

I Clienti e/o Titolari Effettivi e gli Esecutori possono rappresentare un rischio maggiore quando sono oggetto di informazioni negative che possono danneggiare la reputazione del Gruppo nel caso in cui si instauri un rapporto di Clientela con loro. Non è possibile elencare tutti i tipi di informazioni negative che possono rappresentare un rischio reputazionale, ed è necessario esercitare una buona capacità di giudizio. Particolarmente rilevanti sono le accuse o le condanne per Reati Finanziari, nello specifico la sussistenza di procedimenti penali, quando l'informazione è nota alle Società del Gruppo e non coperta da obblighi di segretezza che ne impedirebbero l'utilizzo, procedimenti per danno erariale, procedimenti per responsabilità amministrativa, sanzioni amministrative irrogate per violazione delle disposizioni antiriciclaggio a carico del cliente o del titolare effettivo.

Il rischio reputazionale esiste quando il Cliente, il suo Titolare Effettivo o l'Esecutore sono oggetto di informazioni negative rilevanti. Il grado di rischio reputazionale deve essere valutato in base ad una combinazione della nostra esposizione al rischio (compreso il volume di attività che avremo con il Cliente, il livello di riservatezza dell'operazione, ecc.) e la probabile reazione dei nostri clienti, delle autorità di vigilanza e degli altri stakeholder (inclusa la possibile copertura mediatica).
Per assicurarsi che la reputazione del Gruppo non venga danneggiata, le informazioni negative individuate devono essere valutate per determinare il potenziale riciclaggio di denaro o rischio reputazionale insito nella scelta di instaurare o continuare un rapporto. Anche se le informazioni negative hanno vari livelli di gravità, ciascun nuovo caso deve essere valutato per determinare innanzitutto se un rapporto di Clientela sia legalmente ammissibile, e se il caso debba essere portato all'attenzione di un livello di approvazione superiore. Qualora si stabilisca che un rapporto è legalmente ammissibile, le informazioni negative devono essere valutate come descritto nella GOR - Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio.

Ulteriori informazioni sulla rilevanza o irrilevanza di informazioni relative ad un nuovo cliente o cliente in essere sono fornite nella GOR - Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio.

Quando il Servizio Antiriciclaggio e Antiterrorismo locale, ove presente in sede di Controllata, ha dei dubbi circa la rilevanza delle informazioni negative, tali informazioni negative devono essere riportate al Responsabile Antiriciclaggio locale il quale può richiedere ulteriori approfondimenti al fine di proporre all'Alto Dirigente, a seguito dell'esito dell'valutazione, l'apertura/mantenimento del rapporto o il rifiuto/recesso. Nel caso di autorizzazione all'apertura/mantenimento del rapporto, il Responsabile Antiriciclaggio locale e/o l'Alto Dirigente possono imporre i requisiti aggiuntivi di Adeguata Verifica del Cliente (come un maggior monitoraggio delle transazioni) che ritengono necessari.

8. Adeguata verifica della clientela

Conoscere l'identità dei Clienti, del Titolare Effettivo e dell'Esecutore è fondamentale per prevenire che le Società del Gruppo vengano utilizzate dai riciclatori e da coloro che intendano finanziare il terrorismo. Pertanto, le Società del Gruppo non instaureranno rapporti di affari con un Cliente senza prima avere la ragionevole certezza della sua identità, del suo Titolare Effettivo e del suo Esecutore. Le Società del Gruppo non intrattengono rapporti anonimi né instaura relazioni in cui non sia possibile stabilire l'identità del relativo Titolare Effettivo.

Il programma di adeguata verifica del Cliente implementato dalle Società del Gruppo mira a:

- acquisire l'identità del Cliente, del Titolare Effettivo e dell'Esecutore;
- verificare l'identità del Cliente, dell'eventuale Esecutore e dell'eventuale Titolare Effettivo sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;
- acquisire e valutare le informazioni sullo scopo e sulla natura del rapporto continuativo nonché, in presenza di un rischio elevato di riciclaggio e di finanziamento del terrorismo, dell'operazione occasionale; individuare il tipo di entità del cliente (per es. entità regolamentata, società quotata, società privata, ente pubblico, fondo sovrano, trust/fondazione, SPV o fondo, etc.)
- acquisire e valutare le informazioni in merito alle relazioni tra il Cliente e l'Esecutore e tra Cliente e Titolare Effettivo;
- stabilire quali prodotti e servizi sono richiesti dal cliente;
- svolgere l'esercizio di un controllo costante del rapporto con il cliente per tutta la durata del rapporto.

Ulteriori informazioni da acquisire secondo l'approccio in base al rischio possono riguardare, a titolo esemplificativo:

- l'origine dei fondi utilizzati nel rapporto;
- le relazioni d'affari e i rapporti con altri destinatari;
- la situazione economica e patrimoniale.

I clienti forniscono, sotto la propria responsabilità, tutte le informazioni necessarie e aggiornate per consentire alle Società del Gruppo di adempiere agli obblighi di adeguata verifica della clientela.
La considerazione dei fattori sopra menzionati consentirà di determinare se il cliente in questione abbia i requisiti necessari affinché le Società del Gruppo possano instaurare un rapporto con lui.
Le misure di adeguata verifica della clientela devono essere applicate nelle seguenti circostanze:

- in occasione dell'instaurazione di un rapporto continuativo;
- in occasione dell'esecuzione di un'operazione occasionale, ove si verifichi e che comporti la trasmissione o la movimentazione di mezzi di pagamento per importi pari o superiori a 15.000 euro, indipendentemente dal fatto che sia effettuata con un'operazione unica o con più operazioni frazionate, o comporti in un trasferimento di fondi superiore a 1.000 euro;
- quando ci sia il sospetto che un'operazione sia collegata ad attività di riciclaggio o di finanziamento al terrorismo indipendentemente da qualsiasi deroga, esenzione o soglia minima applicabile;
- quando ci siano dubbi sulla veridicità o adeguatezza dei dati identificativi precedentemente ottenuti ai fini dell'identificazione (ad esempio nel caso di mancato recapito della corrispondenza all'indirizzo comunicato o di incongruenze tra i documenti presentati dal cliente o comunque acquisiti dall'operatore)

Se durante il processo di adeguata verifica riferito ad un Cliente esistente o nuovo dovessero emergere elementi di sospetto, il soggetto non deve essere né informato né portato a conoscenza in alcun modo di tali elementi, in quanto questa azione potrebbe costituire condotta penalmente perseguibile.

Quando le Società del Gruppo non sono in grado di rispettare gli obblighi di adeguata verifica della clientela non instaura il rapporto continuativo ovvero non eseguono l'operazione richiesta dal Cliente. Se l'impossibilità si verifica per un rapporto continuativo in essere, la Società del Gruppo si astengono dal proseguire il rapporto avviando la procedura di recesso unilaterale per i soggetti ad alto rischio ovvero introducendo blocchi all'operatività dei rapporti continuativi per i soggetti a basso e medio rischio.

Le Società del Gruppo valutano inoltre se inviare una segnalazione di operazione sospetta all'autorità competente locale (UIF per la Capogruppo).

8.1. Tipi di adeguata verifica e attribuzione e gestione del profilo di rischio del cliente

Sulla base delle informazioni acquisite in sede di adeguata verifica (es. attraverso la compilazione del questionario AML), tenuto conto dei dati conosciuti sulla clientela (es. notizie crime, procedimenti penali in corso, etc.), sul Titolare Effettive e sull'Esecutore, le Società del Gruppo attribuiscono un profilo di rischio al Cliente attraverso procedure informatiche automatizzate, all'atto dell'onboarding (prima dell'instaurazione del rapporto continuativo),ove le stesse siano disponibili proporzionalmente alla dimensione e tipologia di business svolto. La procedura informatica automatizzata, ove in essere, assicura inoltre, in continuità di rapporto, l'aggiornamento del profilo di rischio associato al Cliente in funzione dell'operatività posta in essere e degli eventuali aggiornamenti intervenuti sul profilo soggettivo.

8.1.1. Adeguata verifica semplificata – Rischio Basso

L'Adeguata Verifica Semplificata (SDD – Simplified Due Diligence) può applicarsi (nella misura ammessa dai requisiti normativi locali) quando i rischi di riciclaggio/finanziamento del terrorismo associati ad un Cliente sono bassi ovvero il Cliente è classificato a basso rischio.
Il rischio di riciclaggio di denaro e finanziamento del terrorismo è basso per alcune entità grazie al livello di regolamentazione o sorveglianza sui mercati, o all'attenzione pubblica a cui sono sottoposte, in una giurisdizione che si ritiene abbia leggi e regolamenti adeguati in questa materia. La valutazione del rischio

Cliente sarà bassa nelle circostanze in cui è possibile identificare una delle fattispecie di "Fattori di rischio Basso" previsti dalla normativa antiriciclaggio, inclusi nell'Appendice 3 della GOR Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio.

Le misure di adeguata verifica semplificata che si applicano ai clienti a basso rischio di riciclaggio, consistono in una riduzione dell'estensione ovvero della frequenza degli adempimenti previsti dalla normativa antiriciclaggio, avendo riguardo:

- alla modulazione dei tempi di esecuzione delle attività per l'identificazione del Cliente, dell'Esecutore o del Titolare effettivo.
- alla riduzione della frequenza dell'aggiornamento dei dati raccolti per l'adeguata verifica.

La Capogruppo non applica una riduzione delle informazioni da raccogliere nel caso di Clienti a rischio basso e in adeguata verifica semplificata.

8.1.2. Adeguata verifica rafforzata – Rischio Alto

Le Società del Gruppo eseguono una Adeguata Verifica rafforzata (EDD - Enhanced Due Diligence) quando il rischio di riciclaggio associato al Cliente è alto, per gestire e mitigare il rischio in modo idoneo.

Le misure di adeguata verifica rafforzata consistono nell'acquisizione di maggiori informazioni sul Cliente e sul Titolare Effettivo e ove rilevante l'Esecutore; in una più accurata valutazione della natura e dello scopo del rapporto; nell'intensificazione della frequenza delle verifiche e in una maggiore profondità delle analisi effettuate nell'ambito dell'attività di controllo costante del rapporto continuativo.

Le misure adottate dalle Società del Gruppo consistono, a seconda della tipologia di cliente a rischio alto:

a) nell'acquisizione di una maggiore quantità di informazioni relative a:
   i. l'identità del Cliente e del Titolare Effettivo o l'assetto proprietario e di controllo del Cliente. In questo ambito è inclusa l'acquisizione e la valutazione di informazioni sulla reputazione del Cliente e del Titolare effettivo e dell'Esecutore;
   ii. il rapporto continuativo, per comprenderne appieno natura e scopo. Rientrano in questo ambito l'acquisizione di informazioni su:
   - il numero, l'entità e la frequenza delle operazioni attese, per poter individuare eventuali scostamenti che potrebbero determinare elementi di sospetto;
   - le ragioni per cui il cliente chiede un determinato prodotto o servizio, specie se le sue necessità finanziarie potrebbero essere soddisfatte al meglio in altro modo o in un altro paese;
   - la destinazione dei fondi;
   - la natura dell'attività svolta dal Cliente, dal Titolare Effettivo e dall'Esecutore;

b) in una migliore qualità delle informazioni da acquisire. Rientrano in tale ambito la verifica dell'origine del patrimonio e dei fondi del cliente, impiegati nel rapporto continuativo.

c) in una maggiore frequenza negli aggiornamenti delle informazioni acquisite tramite controlli più frequenti sul rapporto continuativo e sull'operatività messa in atto dal Cliente, volti a rilevare tempestivamente eventuali variazioni delle informazioni che possano impattare sull'esito della valutazione di mantenimento/recesso dai rapporti e comportare l'invio di una SOS all'autorità locale competente (l'UIF per la Capogruppo);

d) nella richiesta dell'autorizzazione di un Alto Dirigente per l'avvio o la prosecuzione del rapporto continuativo.

Le Società del Gruppo applicano obblighi rafforzati di adeguata verifica tenuto conto delle specifiche previsioni normative, (incluso i fattori di rischio elevato identificati da Banca d'Italia ed inclusi nell'Appendice 4 della GOR - Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio), ovvero nel caso di presidi rafforzati che si rendono necessari a seguito di valutazioni autonome sul rischio riciclaggio associato al Cliente. Tutti i clienti ad alto rischio devono essere valutati al fine di determinare se sia necessario un monitoraggio mirato rafforzato delle loro attività e, in questo caso, quali debbano essere la natura e la

frequenza di tale monitoraggio. La tipologia e l'entità del monitoraggio dipenderanno dagli specifici fattori di rischio identificati e, in ogni caso non saranno inferiori a 12 mesi.

In sintesi l'EDD si applica a tutti i Clienti ad alto rischio ovvero nei seguenti casi:
:

- il Cliente o il suo Titolare effettivo è una PEP;
- il Cliente è cointestatario di un soggetto PEP o è delegato su un conto di una PEP o ha fornito una delega a una PEP
- la Titolarità Effettiva di un Cliente è detenuta da azioni al portatore
- il cliente è un Private;
- il cliente, il titolare effettivo e l'esecutore ove rilevante abbiano sede nei paesi individuati come paesi ad alto rischio
- Il Cliente compie operazioni caratterizzate da importi insolitamente elevati ovvero rispetto alle quali sussistono dubbi circa la finalità cui le medesime sono in concreto pre-ordinate.
- il Cliente, il Titolare effettivo e l'Esecutore ove rilevante è stato segnalato alle autorità locali per sospetti di riciclaggio (in questo caso il profilo di rischio alto rimane invariato per i 5 anni consecutivi alla segnalazione con proposta di declassificazione all'Alto Dirigente nel caso in cui nei 5 anni successivi alla segnalazione non si presentino nuovi fattori di rischio e in assenza di richieste di approfondimenti da parte delle autorità locali (UIF per la capogruppo o autorità inquirenti);
- il Cliente venga classificato ad alto rischio sulla base dell'operatività posta in essere, informazioni soggettive e al numero di rapporti e servizi in cui risulta intestatario/cointestatario,)
- il Cliente o il suo Titolare effettivo o l'Esecutore ove rilevante è destinatario di provvedimenti dell'autorità giudiziaria o interessato da notizie di cronaca circa l'esistenza di provvedimenti penali a suo carico (in questo caso il profilo di rischio alto rimane invariato per i 5 anni successivi al provvedimento giudiziale o alla notizia di cronaca negativa; decorso tale termine, nel caso in cui nei 5 anni successivi a tali eventi non si presentino nuovi fattori di rischio e in assenza di richieste di approfondimenti da parte dell'UIF o autorità inquirenti, può essere formulata la proposta di declassificazione all'Alto Dirigente);

In questi casi può essere opportuno ottenere maggiori informazioni e documentazioni, effettuare riesami più frequenti ed eseguire un monitoraggio delle transazioni più approfondito. Ciò comprende:

- verificare l'identità del Cliente e del Titolare Effettivo o l'assetto proprietario e di controllo del cliente sulla base di più di una fonte affidabile e indipendente in conformità con le fonti dati di cui all'Appendice 2 della GOR Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio;
- accertare l'origine del Patrimonio del Cliente e l'Origine dei Fondi utilizzati nel rapporto;
- identificare e verificare l'identità degli altri azionisti che non sono Titolari Effettivi del Cliente. Nel caso di clienti ad alto rischio, devono essere raccolti i nomi di qualsiasi persona che possiede o controlla il 10% o più delle azioni o dei diritti di voto;
- ottenere informazioni riguardo al numero, alle dimensioni e alla frequenza prevista delle transazioni che presumibilmente interesseranno il rapporto, per essere in grado di individuare eventuali deviazioni che possono dare vita a sospetti;
- le ragioni per cui il cliente chiede un determinato prodotto o servizio specie se le sue necessità finanziarie potrebbero essere soddisfatte al meglio in un altro modo o in un altro paese
- la destinazione dei Fondi.
- Una maggiore frequenza negli aggiornamenti delle informazioni acquisite.

Per la Capogruppo, l'elaborazione del profilo di rischio si basa su algoritmi e procedure informatiche (Gianos KYC e GPR) opportunamente calibrate al fine di assicurare la corretta attribuzione del profilo di rischio alla Clientela, sulla base delle informazioni acquisite e di volta in volta aggiornate.
La Capogruppo può innalzare il profilo di rischio della Clientela assegnato in automatico dall'applicativo, ove ritenuto necessario. L'eventuale abbassamento del profilo di rischio associato alla Clientela deve essere circoscritto a casi eccezionali e dettagliatamente motivato per iscritto nonché autorizzato dall'Alto dirigente.

Le Società Controllate adottano procedure automatizzate o manuali relativamente all'elaborazione del profilo di rischio del Cliente, proporzionalmente alla dimensione e al business svolto.

8.1.3. Adeguata verifica ordinaria – Rischio Medio

L'Adeguata Verifica Ordinaria si applica, di base, ai clienti a rischio medio quando non vi sono gli estremi per la SDD o la EDD.

8.1.4 Adeguata verifica – monitoraggio continuo

Le informazioni acquisite nell'ambito dell'adeguata verifica (per la Capogruppo tramite compilazione del questionario AML da parte del Cliente, del Titolare Effettivo e dell'Esecutore) devono essere aggiornate periodicamente, come minimo:

- ogni anno per i Clienti a rischio "alto";
- ogni tre anni per i Clienti a rischio "medio";
- ogni cinque anni per i Clienti a rischio "basso"

Nel caso i documenti acquisiti per l'adeguata verifica (per la Capogruppo il questionario AML, il questionario integrativo PEP per le persone politicamente esposte o il documento identificativo) siano scaduti, le Società del Gruppo prevedono l'apposizione automatica di blocchi all'operatività del Cliente. Nel caso di Clienti ad alto rischio, previa autorizzazione da parte dell'Organo con poteri delegati per la Capogruppo o l'organo con funzioni equivalenti nelle Società Controllate, è altresì previsto il recesso dai rapporti e la valutazione di elevare una segnalazione di operazione sospetta all'autorità locale competente (UIF per la Capogruppo).

I seguenti eventi devono far sì che si esegua una revisione dell'adeguata verifica del Cliente,

- è giunto a scadenza il riesame previsto sulla base del rating del rischio Alto;
- è dovuto l'esame dell'operatività anomala (per la Capogruppo estratta dal sistema di transaction monitoring in uso Inattesi, FBI Fineco, rilevazione ad evento, richieste di approfondimento da parte dell'UIF);
- le informazioni in qualsiasi modo ricevute dalla Banca fanno supporre un cambiamento dell'assetto societario o, per es. della residenza, o un cambiamento del tipo di attività economica del Cliente;
- sono state individuate notizie negative sostanziali;
- è richiesto dalla Funzione Compliance.

Il riesame delle informazioni KYC del Cliente deve comprendere:

- la verifica che il rapporto con il Cliente sia ancora attivo;
- la conferma che il rating di rischio del Cliente sia corretto. Se il rating del rischio è cambiato, la KYC deve essere rivista in conformità al tipo di entità del Cliente;
- assicurare che la corretta documentazione della KYC sia in archivio e opportunamente aggiornata, in conformità al tipo di entità del Cliente;
- verificare che i Soggetti Collegati identificati siano gli stessi, ed identificare gli eventuali nuovi soggetti. Se sono cambiati, assicurarsi che venga effettuata una verifica adeguata in conformità al tipo di entità del Cliente (se del caso);
- per tutti i nominativi interessati si devono eseguire adeguati controlli sui nominativi, come descritto nella presente policy e relativa GOR.

Si noti che la Revisione Periodica KYC non comporta che sia necessario ottenere nuovamente la **completa** documentazione del Cliente, se la stessa è rimasta valida, cosi come in fase di *onboarding* (ad esempio documento identificativo valido e questionario AML scaduto).

Quando un Cliente in continuità di rapporto richiede l'apertura un ulteriore rapporto continuativo[1], è tenuto ad aggiornare i dati rilasciati precedentemente (es. il questionario AML per la Capogruppo) in sede di adeguata verifica, o a confermare la validità degli stessi.
Quando è stata superata la scadenza del riesame periodico, le informazioni di KYC precedentemente raccolte non possono essere utilizzate.

[1] un rapporto di durata, rientrante nell'esercizio dell'attivita' di istituto svolta dai soggetti obbligati, che non si esaurisce in un'unica operazione;

Relativamente all'apertura di nuovi rapporti continuativi, si chiarisce che:

- per tutti i rapporti classificati "continuativi" la Capogruppo richiede che, contestualmente alla richiesta di apertura del rapporto, ci sia l'aggiornamento del questionario AML da parte del cliente; nel caso di PEP anche l'aggiornamento/acquisizione del questionario integrativo PEP
- nel caso di:

    - clienti PEP e clienti persone giuridiche ad alto rischio: è necessaria, a seguito della richiesta di apertura di rapporti continuativi, l'esecuzione dell'adeguata verifica rafforzata e l'autorizzazione all'apertura del rapporto da parte di un Alto Dirigente della Capogruppo
    - clienti persone fisiche con profilo ALTO (non PEP): occorre distinguere a seconda della tipologia di rapporto continuativo:

        - nel caso di rapporti che comportano l'erogazione di credito (carta di credito, mutuo, prestito personale) si richiede l'esecuzione dell'adeguata verifica rafforzata e l'autorizzazione all'apertura del rapporto da parte di un Alto Dirigente,
        - nel caso di rapporti che non comportano l'erogazione di credito ovvero che non presentano rischi/valutazioni aggiuntive in tema AML rispetto a quelle già svolte in sede apriconto (Conti Advice, Plus, Credit Lombard) l'esecuzione dell'adeguata verifica rafforzata e dell'autorizzazione all'apertura del rapporto da parte di un Alto dirigente non è necessaria.

8.2. Identificazione e verifica della clientela

L'identificazione e la verifica dell'identità del cliente (e quella del suo Titolare Effettivo e del suo Esecutore), devono avvenire prima dell'instaurazione del rapporto continuativo ovvero prima dell'esecuzione dell'operazione occasionale. Qualora le persone da identificare siano più di una (nel caso di cointestatari o di più esecutori), l'acquisizione dei documenti di identità può avvenire in momenti diversi, purché prima di rendere operativi la cointestazione o i poteri di delega o comunque di rappresentanza.
Nel caso di cliente a basso rischio riciclaggio, assoggettabile a misure semplificate di adeguata verifica, la Banca può rinviare fino ad un massimo di trenta giorni l'effettiva acquisizione della copia del documento d'identità necessario al completamento del processo di adeguata verifica.

L'identificazione consiste nell'acquisizione dei dati identificativi forniti dal cliente stesso, previa esibizione di un documento d'identità o altro documento di riconoscimento equipollente ai sensi della normativa vigente, del quale viene acquisita copia in formato cartaceo o elettronico. Con le stesse modalità i destinatari identificano i cointestatari e l'esecutore. Nel caso dell'esecutore sono altresì acquisite le informazioni relative alla sussistenza e all'ampiezza del potere di rappresentanza.

Se il Cliente è un soggetto diverso da persona fisica, e quindi opera attraverso le persone fisiche dotate del potere di rappresentarlo, l'identificazione si effettua nei confronti:

- del cliente, attraverso l'acquisizione dei dati identificativi nonché di informazioni su tipologia, forma giuridica, fini perseguiti e attività svolta e, se esistenti, degli estremi dell'iscrizione nel registro delle imprese e negli albi tenuti dalle autorità di vigilanza di settore. Nel caso di organizzazioni non profit, è acquisita anche l'informazione circa la classe di beneficiari cui si rivolgono le attività svolte (es., vittime di catastrofi naturali e di guerre). In caso di trust, i destinatari acquisiscono copia dell'ultima versione dell'atto istitutivo, al fine di raccogliere e monitorare nel continuo le informazioni in merito alle finalità in concreto perseguite, all'identità dei beneficiari e del trustee, alle modalità di esecuzione del trust e a ogni altra caratteristica del medesimo;
- dell'esecutore, che è identificato con le stesse modalità previste per il cliente-persona fisica e per il quale sono acquisite anche informazioni circa la sussistenza del potere di rappresentanza.

Sulla base del modello distributivo (on line e offerta fuori sede tramite una rete di consulenti finanziari abilitati all'offerta fuori sede) adottato dalla Capogruppo sono state definite idonee procedure di identificazione, in particolare:

- per l'offerta sul territorio italiano:
    - a distanza
    - *de visu* tramite la rete di PFA
- per l'offerta sul territorio UK (in libera prestazione di servizi):
    - a distanza

L'Appendice 2 della GOR - Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio riporta la documentazione e le fonti attendibili per identificare e verificare l'identità del Cliente, del Titolare Effettivo e dell'Esecutore.

8.3. Identificazione e verifica del titolare effettivo

La Capogruppo raccoglie l'informazione in merito ai Titolari effettivi sulla base della dichiarazione del Cliente acquisendo inoltre la relativa copia di un documento identificativo in corso di validità; verifica tali informazioni sulla base di fonti indipendenti ed autorevoli.

La precisione delle informazioni riguardo alla titolarità effettiva rappresenta un elemento chiave del programma antiriciclaggio. Senza queste informazioni, non è possibile gestire adeguatamente gli aspetti relativi alle sanzioni, alle Persone Politicamente Esposte e al rischio reputazionale, né è possibile profilare correttamente il cliente in termini di rischi riciclaggio né di calibrare correttamente i sistemi di monitoraggio delle transazioni. È pertanto indispensabile, prima di instaurare una relazione di Clientela e di aprire il rapporto, che si effettui l'identificazione dei Titolari Effettivi e che le relative informazioni siano accuratamente vagliate e registrate.

Nel caso in cui il Cliente sia una società **di capitali:**
a) costituisce indicazione di proprieta' diretta la titolarita' di una partecipazione superiore al 25 per cento del capitale del cliente, detenuta da una persona fisica;
b) costituisce indicazione di proprieta' indiretta la titolarita' di una percentuale di partecipazioni superiore al 25 per cento del capitale del cliente, posseduto per il tramite di societa' controllate, societa' fiduciarie o per interposta persona.

Nelle ipotesi in cui l'esame dell'assetto proprietario non consenta di individuare in maniera univoca la persona fisica o le persone fisiche cui e' attribuibile la proprietà diretta o indiretta del Cliente Persona Giuridica, il Titolare Effettivo coincide con la persona fisica o le persone fisiche cui, in ultima istanza, e' attribuibile il controllo del medesimo in forza:
a) del controllo della maggioranza dei voti esercitabili in assemblea ordinaria;
b) del controllo di voti sufficienti per esercitare un'influenza dominante in assemblea ordinaria;
c) dell'esistenza di particolari vincoli contrattuali che consentano di esercitare un'influenza dominante.

Con riferimento alla clientela ad alto rischio, in aggiunta all'identificazione del Titolare Effettivo, sarà necessario identificare (non verificare) i nominativi degli azionisti possessori o che controllino il 10% o più della società cliente.

Nel caso di Entità quali **fondazioni** e accordi giuridici quali i **Trust,** Titolare Effettivo significa:

- il disponente;
- il trustee;
- il protector (se esistente);
- i beneficiari oppure, laddove le persone fisiche che beneficiano dell'accordo giuridico o dell'entità debbano ancora essere individuate, la categoria di persone nell'interesse precipuo delle quali il dispositivo giuridico o l'entità sia stata istituita od operi;
- qualsiasi altra persona fisica che eserciti il controllo effettivo sul trust attraverso un possesso diretto o indiretto o attraverso qualsiasi altro mezzo.

Nel caso in cui il cliente sia una persona giuridica privata[2], sono cumulativamente individuati, come titolari effettivi:
a) i fondatori, ove in vita;
b) i beneficiari, quando individuati o facilmente individuabili;
c) i titolari di poteri di rappresentanza legale, direzione e amministrazione.

In ultimo, qualora l'applicazione dei criteri indicati non consenta di individuare univocamente uno o piu titolari effettivi, il titolare effettivo coincide con la persona fisica o le persone fisiche titolari di poteri di rappresentanza legale, amministrazione o direzione della societa'/ Cliente.

[2] di cui al **decreto del Presidente della Repubblica 10 febbraio 2000, n. 361 (normativa locale italiana)**

6. I soggetti obbligati conservano traccia delle verifiche effettuate ai fini dell'individuazione del titolare effettivo.

Chiarimenti relativamente alle modalità pratiche seguite per l'identificazione del Titolare Effettivo sono forniti nella GOR - Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio.

8.4. Identificazione e verifica in caso di operatività a distanza

Le Società del Gruppo pongono particolare attenzione all'operatività a distanza, in considerazione dell'assenza di un contatto diretto con il Cliente. Relativamente all'operatività a distanza, le Società del Gruppo:

- Acquisiscono i dati identificativi del Cliente e ne effettuano il riscontro su una copia – ottenuta in formato elettronico o con modalità analoghe – di un valido documento di identità, ai sensi della normativa vigente;
- Prevedono ulteriori elementi rafforzativi (quali ad esempio nel caso della Capogruppo webcam, bonifico effettuato dal cliente da un intermediario bancario e finanziario terzo con sede in Italia o in un paese comunitario, meccanismi di riscontro basati su soluzioni tecnologiche innovative e affidabili (es., quelle che prevedono forme di riconoscimento biometrico quali il cd. *videoselfie*[3]), assistite da robusti presidi di sicurezza, etc.)

Tali meccanismi di identificazione a distanza, basati su soluzioni tecnologiche fornite da operatori esterni e riconosciuti dal mercato (Experian Prove-ID per il mercato UK e Infocert per il mercato Italiano) sono assoggettati a preventiva valutazione da parte della Funzione Antiriciclaggio locale in aderenza alle indicazioni di EBA (Opinions on the use of Innovative Solutions by Credit and Financial Institutions in the Customer Due Diligence Process). Per la Capogruppo, l'esito delle valutazioni è formalizzato in apposite Schede aggiornate periodicamente dalla Funzione Antiriciclaggio.

8.5. Scopo/natura dell'attività economica e fonte del patrimonio

Le Società del Gruppo acquisiscono e valutano le informazioni sullo scopo e sulla natura prevista del rapporto. La profondità e l'estensione delle verifiche sono correlate al profilo di rischio. Le Società del Gruppo acquisiscono e valutano, in ogni caso, le informazioni concernenti:

- le finalità relative all'accensione del rapporto;
- le relazioni tra il cliente e l'esecutore;
- le relazioni tra il cliente e il titolare effettivo del rapporto;
- l'attività lavorativa ed economica svolta e, in generale, le relazioni d'affari del cliente.

Ulteriori informazioni da acquisire secondo l'approccio in base al rischio possono riguardare, a titolo esemplificativo:

- l'origine dei fondi utilizzati nel rapporto;
- le relazioni d'affari e i rapporti con altri destinatari;
- la situazione economica (es., fonti di reddito) e patrimoniale (possono essere acquisiti, a titolo esemplificativo, bilanci, dichiarazioni IVA e dei redditi, documenti e dichiarazioni provenienti dal datore di lavoro, da intermediari finanziari o altri soggetti);
- la situazione lavorativa, economica e patrimoniale del titolare effettivo, nonché, nella misura in cui essa sia nota o facilmente conoscibile, di familiari e conviventi.

8.6. Potere di Rappresentanza

Tranne che nei rapporti con le Entità regolamentate, Le Società del Gruppo devono ottenere la prova che il rappresentante del Cliente, con cui la Società del Gruppo dialoga, abbia sufficiente autorità per impegnare il

[3] Soluzione in corso di valutazione per implementazione futura.

Cliente nel rapporto in questione, e la sua identità deve essere verificata. L'autorità può essere implicita nel caso di un Amministratore o esponente equivalente, ma si deve prestare attenzione al fatto che non si tratti di Amministratori Fiduciari.

8.7. Controlli dei nominativi

Al momento dell'instaurazione di un rapporto e su base continuativa vengono effettuati i controlli dei nominativi. Lo screening viene eseguito sui nominativi delle parti identificate, per contribuire ad individuare i potenziali problemi che possono incidere sulla valutazione del rischio del Cliente, e per identificare eventuali Entità direttamente sottoposte a sanzioni.

8.8. Approvazione della relazione

Si può instaurare una nuova relazione di Clientela se (1) le informazioni relative al Cliente, Titolare Effettivo ed Esecutore sono state acquisite in modo completo e corretto, e (2) i controlli eseguiti non abbiano evidenziato elementi ostativi all'apertura del rapporto.

I clienti ad alto rischio, sulla base del principio *four eyes*, non solo devono essere valutati dal Servizio Antiriciclaggio locale, ma anche ottenere l'autorizzazione da parte di un Alto Dirigente locale; tale modalità è prevista per tutti i soggetti PEP. Anche il caso di declassificazione di clientela PEP richiede specifica autorizzazione da parte dell'Alto Dirigente della Società del Gruppo.

8.9. Relazioni d'affari vietate

La Società del Gruppo non instaureranno relazioni d'affari con Banche di Comodo né effettuerà o permetterà transazioni su conti anonimi.
Le Società del Gruppo prendono adeguati provvedimenti per assicurarsi di non instaurare o mantenere rapporti di Correspondent Banking con banche che permettono l'apertura di rapporti con Banche di Comodo.
Le Società del Gruppo non instaureranno, né manterranno relazioni di affari con clienti persone giuridiche quando l'identità del Titolare Effettivo (dei Titolari Effettivi) che debba essere stabilita in base alla presente Policy, non possa di fatto essere stabilita.
Le Società del Gruppo non instaurerà o manterrà relazioni né elaborerà transazioni collegate a persone fisiche o giuridiche nominate nell'Elenco delle Sanzioni Finanziarie dell'Unione Europea o nella Specially Designated Nationals and Blocked Persons List ('lista SDN') dell'Office of Foreign Assets Control (OFAC).

Inoltre le Società del Gruppo non instaureranno rapporti con:

- servizi di cambio e trasferimento valuta (entità non bancarie e non iscritte agli albi tenuti dall'autorità di vigilanza che offrono ai loro clienti meccanismi di trasferimento e cambio valuta, quali il 'money transfer', l'incasso di assegni, il cambio di valuta e l'emissione/riscatto di traveller's cheques);
- provider e piattaforme di cambio di moneta digitale/virtuale.
- persone fisiche o giuridiche delle quali è noto che sono attivamente coinvolte in attività criminose, corrotte o terroristiche
- soggetti operanti nei settori red light business/mariuana/armi.

8.10. Controlli nel corso del rapporto d'affari

Le Società del Gruppo prevedono controlli continuativi nel corso del rapporto in merito all'operatività dei clienti. Oltre alla rilevazione di potenziali anomalie nello svolgimento delle singole operazioni da parte delle strutture preposte alla raccolta ed esecuzione delle stesse (PFA e strutture interne della Capogruppo) le transazioni effettuate dalla clientela devono infatti essere analizzate periodicamente in modo da verificare che esse siano compatibili con la conoscenza che la Banca ha del proprio cliente, delle sue attività commerciali e del suo profilo di rischio.
Nel primo caso, se le anomalie rilevate possono far presupporre attività di riciclaggio, la struttura che ha individuato l'anomalia deve predisporre una segnalazione di operazione sospetta.

8.11. Condivisione delle informazioni riguardanti il Cliente nel Gruppo

Nonostante la maggior parte dei sistemi giuridici dei Paesi non UE non impedisca ai gruppi di implementare AML/CFT policies e procedure di Gruppo più stringenti rispetto alle legislazioni nazionali, potrebbero verificarsi casi dove l'implementazione di una legislazione di Paesi terzi non permetta l'applicazione di alcune parti o di tutta la normativa definita dalla Capogruppo, ad esempio perché la condivisione di alcune specifiche informazioni del cliente all'interno del Gruppo sia in conflitto con la legislazione locale di protezione dei dati o segreto bancario.
Nel caso in cui un Gruppo possieda la totalità o la maggioranza di una Entity che opera in un Paese non EU che impedisca la condivisione delle informazioni dei clienti all'interno del Gruppo, deve essere accertato se il consenso dei clienti e, dove applicabile i titolari effettivi dei clienti, possa essere utilizzato per superare legalmente restrizioni o divieti.

Nei casi in cui ciò non sia possibile, la Controllata deve prendere le seguenti misure aggiuntive:

- informare la Capogruppo attraverso il processo di NBO dei requisiti legali che impediscono la condivisione delle informazioni;
- supportare l'NBO con un parere legale che illustra nello specifico il divieto.

Nel caso in cui la normativa locale applicabile alla Società del Gruppo sia più stringente di quella applicabile alla Capogruppo, la Controllata seguirà la normativa più stringente applicabile a livello locale.

8.12. Escalation

Se il Responsabile della Funzione Antiriciclaggio locale, informato dal Servizio Antiriciclaggio e Antiterrorismo locale, stabilisce che un rapporto, operazione o pagamento potrebbe infrangere le restrizioni previste nel presente documento, dovrà comunicare all'Unità organizzativa coinvolta che l'attività è vietata. Tale decisione sarà da considerarsi definitiva.
Qualora una relazione, transazione o pagamento proposti, anche se consentiti dalla legge e dalle restrizioni interne in materia di Antiriciclaggio, rappresentino un rischio operativo e/o reputazionale rilevante, la decisione di procedere o meno all'apertura o al mantenimento di una particolare relazione o all'esecuzione di un pagamento o una transazione è di competenza dell'Alta Direzione locale.
Le decisioni prese devono essere finali e possono consistere nel respingere l'operazione, approvarla a determinate condizioni o definire specifiche restrizioni.
Qualora la decisione dell'Alta Direzione locale sia divergente rispetto alla proposta del Servizio Antiriciclaggio e Antiterrorismo locale, il Responsabile della Funzione Antiriciclaggio e Antiterrorismo locale può effettuare l'escalation all'Alto Dirigente Locale.
L'escalation dovrà:

- avvenire in forma scritta;
- contenere le motivazioni che portano alla generazione della stessa; e
- essere accompagnata da tutta la documentazione a supporto.

.

8.13. Conservazione della documentazione e conservazione delle informazioni e delle operazioni

Le Società del Gruppo implementano e mantengono procedure che garantiscano la conservazione per il periodo di tempo stabilito dalla normativa applicabile, (almeno dieci anni dall'esecuzione di un'operazione occasionale o dalla cessazione del rapporto d'affari nel caso della Capogruppo), dei seguenti documenti.

- copia o riferimenti ai documenti utilizzati per l'adeguata verifica del cliente; e
- documentazione e registrazioni a supporto del rapporto e delle operazioni, che consistono nei documenti originali e/o nelle copie probatorie per procedimenti giudiziari ai sensi della legislazione nazionale vigente.

La documentazione conservata deve consentire, quanto meno, di ricostruire univocamente:

a) la data di instaurazione del rapporto continuativo o del conferimento dell'incarico;
b) i dati identificativi del cliente, del titolare effettivo e dell'esecutore e le informazioni sullo scopo e la natura del rapporto o della prestazione;
c) la data, l'importo e la causale dell'operazione;
d) i mezzi di pagamento utilizzati.

Al fine di garantire che i documenti e le informazioni possano essere utilizzati dalle Autorità nazionali competenti in qualsiasi indagine o nell'analisi di un caso di possibile riciclaggio o di finanziamento del terrorismo, le procedure delle Società devono garantire che le informazioni vengano archiviate nelle rispettive procedure contabili informatizzate e che la documentazione venga conservata in archivi organizzati.

È pertanto necessaria la massima attenzione nell'archiviare, nella posizione del cliente, i questionari, le visure camerali e quant'altro sia stato utilizzato per assolvere gli obblighi di adeguata verifica.

8.14. Segnalazione di operazioni sospette

Si definisce operazione sospetta ogni attività atta, per sua natura, ad avere una connessione con il riciclaggio o con il finanziamento del terrorismo e, in particolare, le operazioni complesse di importo particolarmente rilevante o insolitamente elevato, nonché tutti gli schemi insoliti di operazione che non hanno uno scopo economico evidente o che non hanno uno scopo chiaramente lecito.

8.14.1. Individuazione e segnalazione delle operazioni sospette

La Banca collabora attivamente con le Autorità competenti al fine di individuare le cosiddette "operazioni sospette". Il sospetto deve essere desunto dalle caratteristiche, entità, natura dell'operazione o da qualsivoglia altra circostanza conosciuta, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi a disposizione dei soggetti tenuti alla segnalazione, acquisiti nell'ambito dell'attività svolta.
Inoltre, è considerato "elemento di sospetto" il ricorso frequente o ingiustificato ad operazioni in contante.
Per dare puntuale applicazione all'obbligo di collaborazione attiva, la Banca ha implementato procedure che prevedono:

- la tempestiva segnalazione interna di attività potenzialmente sospette al Responsabile SOS o a suo delegato;
- la valutazione e l'indagine delle attività potenzialmente sospette e la documentazione dei risultati delle indagini;
- la tempestiva segnalazione alle Autorità quando si è in presenza, si sospetta o si ha ragionevole motivo di ritenere di essere in presenza di attività di riciclaggio (commessa, o tentata); e
- la tempestiva risposta alle richieste di informazioni da parte delle Autorità.

In particolare, tali procedure al fine di definire in modo puntuale il processo di segnalazione delle operazioni sospette e gli adempimenti correlati:

a) forniscono dettagliate indicazioni organizzative che regolamentano il processo di segnalazione di operazioni sospette e ne garantiscono la tracciabilità dal momento in cui sorge il sospetto sino al perfezionamento della decisione di procedere o non procedere alla segnalazione;
b) contengono precise disposizioni in ordine alle modalità per assicurare tempestività e segretezza nel processo segnaletico, sia all'interno della Banca sia verso l'esterno, riducendo al minimo indispensabile eventuali passaggi intermedi tra il soggetto/struttura organizzativa segnalante ed il soggetto/struttura organizzativa deputato a valutare la segnalazione;
c) prevedono adeguate misure volte ad arrestare l'esecuzione delle operazioni, nei casi in cui ciò sia possibile in considerazione della concreta operatività e sempre che la loro mancata esecuzione non possa ostacolare le indagini delle Autorità competenti;
d) prevedono l'obbligo di istituire un apposito archivio nel quale devono essere conservati i moduli interni di segnalazione, completi delle osservazioni formulate dai soggetti coinvolti nella procedura e dell'eventuale documentazione allegata, copia delle segnalazioni, di eventuali lettere

accompagnatorie e di ogni altra comunicazione trasmessa alle competenti Autorità nonché ogni ulteriore comunicazione o richiesta pervenuta dalle Autorità competenti;

e) garantiscono la riservatezza sull'identità delle persone che effettuano le segnalazioni.

I Dipendenti sono adeguatamente informati circa il processo interno che porta alla segnalazione sia attraverso la pubblicazione delle relative procedure operative sia mediante appositi programmi di formazione.

La Banca si avvale di metodologie e strumenti in grado di individuare eventuali comportamenti anomali, facendo anche riferimento agli indicatori di anomalia emanati dalla Banca d'Italia e periodicamente aggiornati.

8.15. Obblighi di formazione

La Capogruppo, nell'ambito del piano formativo, cura in via continuativa, e per i neo assunti entro tre mesi dalla data di assunzione, la formazione obbligatoria del proprio personale e dei propri PFA in tema di prevenzione del riciclaggio e finanziamento del terrorismo.

In considerazione dell'attività svolta, la Funzione HR delle Società del Gruppo, con il supporto della Funzione Antiriciclaggio locale individua specifiche iniziative di formazione avuto anche riguardo dei differenti target di dipendenti/Consulenti.

Un primo livello di formazione è assicurato attraverso la diffusione della Policy e della normativa aziendale adottata in attuazione della stessa al personale e ai Consulenti della Capogruppo. Tale documentazione illustra organicamente gli obblighi imposti in materia di antiriciclaggio e di prevenzione dei fenomeni di finanziamento del terrorismo e le relative sanzioni, soffermandosi, in particolare, sui comportamenti da adottare da parte di ciascun dipendente/Consulente in considerazione dell'attività svolta.

La formazione include un test finalizzato a valutare che i Dipendenti ed i Consulenti abbiano effettivamente compreso le materie oggetto della stessa.

Laddove un dipendente o un Consulente non ottenga la formazione prevista entro un determinato termine, è necessario segnalare la questione a livelli gerarchici superiori e prevedere adeguate sanzioni, inclusa, se necessario, l'impossibilità di trattare con clienti o di gestire operazioni.

8.16. Sistemi informativi a supporto

Le Società del Gruppo si dotano di strumenti e procedure idonei a:

- consentire la corretta conservazione ed elaborazione delle informazioni relative all'adeguata verifica della clientela ed alla conservazione delle operazioni
- supportare l'individuazione dei dati mancanti per la completa raccolta delle informazioni di cui al punto precedente, attraverso la produzione di adeguate evidenze, di warning di sistema o di blocchi operativi
- garantire la sicurezza fisica e logica degli archivi (supportare la valutazione delle operazioni sospette, mediante la produzione di indicatori di anomalia al fine della loro eventuale segnalazione alle competenti Autorità;
- consentire, ove applicabile, controlli automatici di coerenza tra le varie informazioni anagrafiche memorizzate, di congruità delle stesse e periodici controlli dei dati
- verificare, automaticamente, che non vengano instaurate relazioni di affari e neppure vengano effettuate singole operazioni con soggetti presenti nelle liste di nominativi sospettati di svolgere attività terroristica, diffusi da Autorità nazionali o internazionali
- consentire di effettuare ricerche in tutti i database clienti, per far fronte a richieste esterne ricevute dal legislatore o da Forze dell'Ordine e per far fronte anche ad indagini interne;
- condividere, in linea con quanto consentito dalla normativa applicabile, le informazioni (relative alle attività sospette individuate dalla Banca) all'interno del Gruppo, ai fini della gestione del rischio antiriciclaggio.

9. Capogruppo - Limitazioni all'uso del contante e dei titoli al portatore

Il D. Lgs 231/2007 prevede importanti limitazioni all'uso del contante e dei titoli al portatore di seguito riportate:

- è vietato il trasferimento di denaro contante e di titoli al portatore in euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi (persone fisiche o giuridiche), quando il valore oggetto di trasferimento è complessivamente pari o superiore a 3.000 euro; si intende superata la soglia anche quando il trasferimento è effettuato con più pagamenti, inferiori alla soglia, che appaiono artificiosamente frazionati;
- il trasferimento superiore al limite dei 3.000 euro può essere eseguito esclusivamente per il tramite di banche, Poste italiane S.p.a., istituti di moneta elettronica e istituti di pagamento mediante disposizione accettata per iscritto dagli stessi intermediari e previa consegna ai medesimi della somma in contanti";
- i moduli di assegni bancari e postali sono rilasciati dalle banche e da Poste Italiane S.p.A. muniti della clausola di non trasferibilità; il cliente può richiedere, per iscritto, il rilascio di moduli di assegni bancari e postali in forma libera;
- gli assegni bancari e postali di importo pari o superiore a 1.000 euro devono recare l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità;
- gli assegni bancari e postali emessi all'ordine del traente possono essere girati unicamente per l'incasso a una banca o a Poste Italiane S.p.A;
- gli assegni circolari, vaglia postali e cambiari sono emessi con l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità.

La violazione delle disposizioni sopra indicate è punita con una sanzione amministrativa pecuniaria da 3.000 a 50.000 euro.

- Il cliente può richiedere per iscritto il rilascio di assegni circolari, vaglia postali e cambiari, di importo inferiore a 1.000 euro, senza la clausola di non trasferibilità. Per ciascun modulo di assegno bancario o postale richiesto in forma libera o per ciascun assegno circolare o vaglia postale o cambiario rilasciato in forma libera è dovuta dal richiedente l'imposto di bollo di 1,50 euro.
- E' ammessa esclusivamente l'emissione di libretti di deposito, bancari o postali, nominativi;
- E' vietato il trasferimento di libretti al portatore (di deposito bancari o postali); questi, ove esistenti, sono estinti dal portatore entro il 31 dicembre 2018; in caso di violazione si applica la sanzione amministrativa pecuniaria da 250 a 500 euro.
- É vietata l'apertura in qualunque forma di conti o libretti di risparmio in forma anonima o con intestazione fittizia: la violazione è punita con una sanzione amministrativa pecuniaria dal 20% al 40% del saldo.
- E' infine vietato l'utilizzo, in qualunque forma, di conti o libretti di risparmio in forma anonima o con intestazione fittizia aperti presso Stati esteri; in caso di violazione si applica una sanzione amministrativa pecuniaria dal 10% al 40% del saldo.

9.1. Obbligo di comunicazione delle infrazioni al ministero dell'economia e delle finanze

La Banca è tenuta a comunicare al Ministero dell'Economia e delle Finanze le infrazioni alle norme sulla limitazione dell'uso del contante e dei titoli al portatore di cui abbia notizia in relazione ai suoi compiti di servizio e nei limiti delle sue attribuzioni ed attività; la comunicazione deve avvenire entro il termine di trenta giorni dalla notizia delle infrazioni stesse[4]. La medesima comunicazione è dovuta dai componenti del collegio sindacale, del consiglio di sorveglianza, del comitato per il controllo sulla gestione presso i soggetti obbligati, quando riscontrano la violazione delle suddette disposizioni nell'esercizio delle proprie funzioni di controllo e vigilanza. Nei casi di infrazioni riguardanti assegni bancari, assegni circolari, libretti al portatore o titoli similari, la comunicazione deve essere effettuata dalla banca che li accetta in versamento (negoziatrice) e dalla banca che ne effettua l'estinzione (trattaria), salvo che il soggetto tenuto alla comunicazione abbia la certezza che la stessa è già stata effettuata dall'altro soggetto obbligato. Qualora oggetto dell'infrazione sia un'operazione di trasferimento già oggetto di segnalazione di operazione sospetta, non sussiste l'obbligo di comunicazione di cui sopra.

[4] Cfr. processi n. 7940 "Controllo degli assegni tratti su FinecoBank"; n. 9120 "Versamenti in conto corrente di assegni tratti e non tratti su FinecoBank".

10. Misure di contrasto finanziario del terrorismo e dell'attività di paesi che minacciano la pace e la sicurezza – linee guida

Nel corso degli anni, si è fortemente rafforzata l'esigenza di contrastare il finanziamento del terrorismo a livello internazionale. Tale circostanza ha portato all'adozione di una serie di misure internazionali (risoluzioni delle Nazioni Unite) e comunitarie (regolamenti comunitari di attuazione delle risoluzioni) volte a contrastare il terrorismo sul piano finanziario.

Il finanziamento del terrorismo si differenzia dal riciclaggio del denaro sporco (*money laundering*) in quanto nel *money laundering* i proventi hanno origine da attività illecite per poi essere re-immesse nel circuito legale attraverso operazioni di ripulitura o re-investimento, mentre nel caso del finanziamento di attività terroristiche le attività da cui derivano le disponibilità finanziarie possono anche essere lecite, ma illecito è il loro successivo utilizzo (*money dirtying*).

Peraltro, analogamente a quanto accade per i fenomeni di riciclaggio, anche le attività poste in essere dai gruppi terroristici che operano sullo scenario internazionale richiedono, per la loro realizzazione, l'impiego di ingenti risorse economiche che vengono trasferite anche attraverso i canali bancari e finanziari.

Come esposto nella Global Policy e Global Rules Sanzioni Finanziarie, la Banca non deve instaurare rapporti con persone fisiche o giuridiche presenti nella lista dell'UE o nella lista OFAC. Questo divieto deve essere osservato dalla Banca anche in caso di operatività in paesi fuori della UE e degli USA, poiché la mancata osservanza di tale divieto può comportare un rischio reputazionale e compromettere i rapporti d'affari della Banca.

Le Società del Gruppo implementano e mantengono procedure che prevedano:

- restrizioni sul patrimonio, sulle attività economiche e sulle risorse finanziarie delle persone fisiche e giuridiche incluse nelle Blacklist dell'UE e dell'OFAC, se previsto o richiesto dalla legge;
- la segnalazione alle Autorità competenti delle misure restrittive, oppure delle relazioni esistenti con clienti non soggetti alle misure restrittive ma ricompresi nelle liste Blacklist pubblicate da tali Autorità;
- la segnalazione alle Autorità competenti di qualsiasi attività nota o sospetta (o l'esistenza di ragionevoli motivi di conoscenza o sospetto) che possa essere ricondotta al finanziamento del terrorismo; e
- il divieto di intraprendere determinate attività commerciali, come stabilito dalla UE, con i paesi che minacciano la pace e la sicurezza internazionale.

Per le disposizioni di dettaglio inerenti alle misure di contrasto al finanziamento del terrorismo poste in essere a livello di Gruppo si rimanda alla normativa interna di riferimento.

11. Capogruppo - Trasferimenti di fondi

L'adozione delle misure descritte nei precedenti paragrafi non consente comunque di escludere la possibilità che riciclatori di denaro e sostenitori del terrorismo possano accedere ai sistemi di pagamento per trasferire i propri fondi.
La possibilità di risalire con certezza all'origine dei trasferimenti di fondi costituisce uno strumento particolarmente importante per:

- prevenire gli abusi del sistema finanziario agli scopi di riciclaggio di denaro o di finanziamento del terrorismo;
- investigare e individuare i casi di cui al punto precedente.

Con il Regolamento CE n. 1781 del 15 novembre 2006, l'Unione Europea aveva già stabilito apposite norme riguardanti i dati informativi relativi all'ordinante che devono accompagnare le operazioni di trasferimento di fondi effettuate, in qualunque valuta, da soggetti operanti in qualità di Prestatori di Servizi di Pagamento o di Prestatori Intermediari di Servizi di Pagamento.
Il Regolamento UE n. 847 del 20 maggio 2015, applicabile dal 26 giugno 2017 e che abroga e sostituisce il Regolamento 1781/2006, ha esteso il perimetro di tali controlli anche ai dati informativi relativi al beneficiario e ai pagamenti intermediati.
Il Regolamento UE 847/2015 si applica ai trasferimenti di fondi in qualsiasi valuta, inviati o ricevuti da un Prestatore di Servizi di Pagamento o da un Prestatore Intermediario di Servizi di Pagamento stabilito nell'Unione.
Gli obblighi che vengono attribuiti ai Prestatori di Servizi di Pagamento sono:

- acquisire e/o fornire le informazioni necessarie relative all'ordinante e al beneficiario;
- verificare che le informazioni siano veritiere, corrette ed aggiornate;
- garantire il corretto trasferimento di tutte le informazioni ricevute;
- effettuare il monitoraggio dei trasferimenti privi di informazioni o con informazioni incomplete effettuando la segnalazione, in caso di sospetto di riciclaggio di denaro o di finanziamento del terrorismo, alle Autorità di Vigilanza.

Tutte le informazioni che accompagnano il trasferimento di fondi e/o le successive comunicazioni devono essere archiviate per almeno 5 anni.

11.1. Casi di esclusione

Il Regolamento non si applica ai trasferimenti di fondi effettuati utilizzando una carta di pagamento, uno strumento di moneta elettronica o un telefono cellulare o ogni altro dispositivo digitale o informatico prepagato o post-pagato con caratteristiche simili, purché le condizioni seguenti siano soddisfatte:

a. la carta, lo strumento o il dispositivo siano utilizzati esclusivamente per il pagamento di beni o servizi;
b. il numero della carta, dello strumento o del dispositivo accompagni tutti i trasferimenti generati dalla transazione.

Tuttavia, il Regolamento si applica quando la carta di pagamento, lo strumento di moneta elettronica o il telefono cellulare o ogni altro dispositivo digitale o informatico prepagato o post-pagato con caratteristiche simili è utilizzato per effettuare trasferimenti di fondi da persona a persona.
Il Regolamento non si applica ai trasferimenti di fondi:

- che comportano il prelievo di contante da parte dell'ordinante dal proprio conto di pagamento;
- che trasferiscono fondi a un'autorità pubblica per il pagamento di imposte, sanzioni pecuniarie o altri tributi in uno Stato membro;
- in cui l'ordinante e il beneficiario sono entrambi prestatori di servizi di pagamento operanti per proprio conto;
- che sono effettuati con la trasmissione delle immagini degli assegni, inclusi gli assegni troncati;
- l'importo del trasferimento di fondi non superi € 1.000.

11.2. Gli obblighi del prestatore di servizi di pagamento

Il Regolamento 847/2015 identifica i ruoli e attribuisce responsabilità ai seguenti soggetti:

- Prestatore Servizi di Pagamento per conto dell'ordinante

- Prestatore Servizi di Pagamento per conto del beneficiario
- Prestatori Intermediari di Servizi di Pagamento

11.2.1. Gli obblighi del prestatore dei servizi di pagamento dell'ordinante (PSP dell'ordinante)

I dati che devono accompagnare i trasferimenti di fondi sono:

a) il nome dell'ordinante;
b) il numero di conto di pagamento dell'ordinante;
c) l'indirizzo dell'ordinante, il numero del suo documento personale ufficiale, il suo numero di identificazione come cliente o la data e il luogo di nascita.

Il prestatore di servizi di pagamento dell'ordinante assicura che i trasferimenti di fondi siano accompagnati dai seguenti dati informativi relativi al beneficiario:

a) il nome del beneficiario;
b) il numero di conto di pagamento dell'ordinante.

Qualora i trasferimenti non siano effettuati a partire da un conto di pagamento o in favore di un conto, il PSP dell'ordinante assicura che il trasferimento di fondi sia accompagnato da un codice unico di identificazione dell'operazione, invece che dal numero o dai numeri di conto di pagamento.
Il PSP dell'ordinante deve garantire che nel messaggio di trasferimento fondi che viene inviato, siano correttamente riportati i dati identificativi dell'ordinante. Nel caso di operazioni disposte con addebito in conto, i dati verranno ricavati automaticamente dalla procedura. Nel caso di un'operazione disposta da clientela occasionale (o per cassa) è necessario verificare ed indicare i dati dell'ordinante quando l'importo dell'operazione è superiore a € 1.000.
La correttezza dei dati relativi all'ordinante viene garantita con l'osservanza dell'obbligo di adeguata verifica, che riguarda sia i nuovi clienti sia i clienti già acquisiti, così come previsto dalla normativa in tema Antiriciclaggio (vedi cap. 6)

- *Trasferimento fondi all'interno dell'Unione Europea*

Per le operazioni di trasferimento fondi disposte a favore di un Beneficiario all'interno dell'Unione Europea, è sufficiente che l'operazione riporti almeno il numero di conto di pagamento dell'ordinante e del beneficiario o nel caso in cui l'operazione avvenga al di fuori di un conto corrente (in addebito o in accredito) dal codice unico di identificazione dell'operazione stessa.
I dati completi dell'ordinante saranno da fornire, in caso di richiesta della Banca del beneficiario o intermediaria, entro tre giorni lavorativi dal ricevimento della richiesta.

- *Trasferimento fondi all'esterno dell'Unione Europea*

Per le operazioni di trasferimento fondi disposte a favore di Beneficiario fuori dell'Unione Europea, l'operazione deve riportare i dati completi dell'ordinante (nome, indirizzo e numero di conto o altra informazione equivalente).
In Fineco, le procedure di trasferimento fondi hanno controlli online finalizzati a garantire la presenza dei dati dell'ordinante e del beneficiario richiesti dal Regolamento 847/2015 prima dell'invio dello stesso messaggio di trasferimento fondi.

11.2.2. Gli obblighi del prestatore dei servizi di pagamento del beneficiario (PSP del beneficiario)

Il PSP del beneficiario deve applicare procedure efficaci per accertare — in relazione ai dati informativi sull'ordinante e sul beneficiario — che i campi del sistema di messaggistica o di pagamento e di regolamento utilizzato per effettuare il trasferimento di fondi siano stati completati con i caratteri o i dati ammissibili, in conformità delle convenzioni di tale sistema.
Inoltre, deve applicare procedure efficaci, comprendenti, ove opportuno, il monitoraggio a posteriori o il monitoraggio in tempo reale, per accertare l'eventuale mancanza dei dati informativi relativi all'ordinante o al beneficiario di cui al precedente paragrafo 9.2.1.
Nel caso in cui tali dati risultino assenti o incompleti o qualora non siano completati con caratteri o dati ammissibili in conformità delle convenzioni del sistema di messaggistica di pagamento e regolamento deve:

- rifiutare il trasferimento dei fondi

- oppure richiedere al PSP dell'ordinante i dati dell'ordinante stesso o del beneficiario, prima o dopo avere messo i fondi a disposizione del beneficiario, in funzione della valutazione del rischio.

Fineco ha definito tramite apposito processo le modalità di gestione dei pagamenti ricevuti privi o incompleti dei dati dell'ordinante e/o del beneficiario (cfr. processi n. 9125 "Gestione dei bonifici Italia in entrata", 9045 "Estero – bonifici in ingresso", 9795 "Bonifici SEPA in ingresso").

11.3. Obblighi di monitoraggio, valutazione e segnalazione

Il Regolamento 847/2015 prevede obblighi di monitoraggio, valutazione e segnalazione in capo al PSP del beneficiario e al PSP intermediario, al fine di individuare

- i pagamenti che pervengono privi di tutti i dati richiesti o con dati non conformi
- i PSP dell'ordinante reiteratamente inadempienti

Infatti, se un Prestatore di Servizi di Pagamento omette ripetutamente di fornire i prescritti dati informativi relativi all'ordinante o al beneficiario, il PSP del beneficiario deve adottare provvedimenti, che possono inizialmente includere richiami e diffide, prima di rifiutare qualsiasi futuro trasferimento di fondi proveniente da quel Prestatore di Servizi di Pagamento o di limitare o porre fine ai suoi rapporti professionali con lo stesso.

Il PSP del beneficiario deve riferire tali inadempimenti e le misure adottate all'autorità responsabile competente per il controllo del rispetto delle disposizioni di contrasto al riciclaggio e al finanziamento del terrorismo.

Il PSP del beneficiario deve tenere conto della mancanza o dell'incompletezza dei dati informativi relativi all'ordinante o al beneficiario per valutare se il trasferimento di fondi, od ogni operazione correlata, sia sospetto e se debba essere segnalato all'Unità di Informazione Finanziaria.

11.3.1. Controlli e monitoraggio

La Banca, sui pagamenti in entrata effettua un monitoraggio sulle operazioni ricevute prive dei dati dell'ordinante e del beneficiario per:

- valutare la relazione/posizione del PSP dell'ordinante ripetutamente inadempiente;
- rivalutare nel complesso la posizione del beneficiario di bonifici privi dei dati dell'ordinante e del beneficiario quando il fenomeno sia fonte di sospetto;
- individuare le operazioni ritenute sospette;
- segnalare alle autorità competenti la sistematica omissione da parte del PSP inadempiente.

Inoltre, la Funzione di Compliance - Unit Risk Assessment & Controls, sulla base dell'approccio basato sul rischio, effettua controlli di secondo livello a campione.

11.3.2. Valutazioni e segnalazioni

Per le operazioni riscontrate incomplete o mancanti dei dati informativi dell'ordinante e/o del beneficiario o con dati non conformi con la messaggistica, la Banca deve valutare la presenza di eventuali indicatori di operatività sospetta da segnalare all'Unità di Informazione Finanziaria. Deve inoltre valutare se limitare o sospendere l'operatività nei confronti delle banche corrispondenti reiteratamente inadempienti.

12. Monitoraggio dei controlli

Le Società del Gruppo definiscono un sistema di controlli di secondo livello finalizzato a testare i controlli Antiriciclaggio di primo livello al fine di garantirne l'efficacia ed il corretto svolgimento.