



Global Policy

Policy Antiriciclaggio e Antiterrorismo

FB 035_2024

Funzione Approvante

Consiglio di Amministrazione

Data Luglio 2024

Funzione Proponente

Amministratore Delegato e Direttore Generale

ANAGRAFICA

Owner	Direzione Antiriciclaggio e Anticorruzione		
Process Tree	Process Type: Governo e controllo MG: Gestione dei rischi e dei controlli MP: Gestione dei rischi di compliance EP: Gestione delle attività in ambito Antiriciclaggio, Antiterrorismo, Sanzioni Finanziarie e Anticorruzione (AML, CTF, FS, AC) SP: Identificazione degli obiettivi di controllo su antiriciclaggio, antiterrorismo, sanzioni finanziarie e comportamenti illegittimi		
Contatti	<i>Chiarimenti sui contenuti del documento</i>	Struttura: Governance e Controlli per Antiriciclaggio e Anticorruzione e-mail: governanceaml@fineco.it	
	<i>Assistenza operativa</i>	servizioantiriciclaggio@fineco.it	
Funzioni di Capogruppo coinvolte nel processo di condivisione	Organizzazione e Operations Banca Corporate Law & Board Secretary's Office Operations Banking e Rete		
Certificazione in Capogruppo per profili di competenza			
Entità coinvolte nel processo di condivisione			
Entità destinatarie (perimetro minimo)¹	Controllate dirette	Controllate indirette	Altre indicazioni
	Fineco Asset Management DAC (FAM)		

¹ In aggiunta alle Entità indicate, ogni Entità può distribuire la *Global Rule* ad ulteriori proprie controllate.

Normative sostituite/revisionate e principali cambiamenti apportati

<u>Normativa sostituita/revisionata</u>	Data normativa sostituita/revisionata	Razionale/Riassunto delle principali modifiche	Tipo modifica²
FB 040_2023 Global Policy “Policy Antiriciclaggio e Antiterrorismo”	Novembre 2023	Aggiornamento della Global Policy al fine di recepire i chiarimenti di Banca d’Italia comunicati con nota del 9 gennaio 2024 in merito all’applicazione delle Disposizioni in materia di organizzazione, procedure e controlli interni per finalità antiriciclaggio del 26 marzo 2019, come modificate dal Provvedimento del 1° agosto 2023, in recepimento degli Orientamenti EBA inerenti alle politiche e le procedure relative alla gestione della conformità e al ruolo e alle responsabilità del responsabile antiriciclaggio (EBA/GL/2022/05).	Sostituzione

Normativa di Gruppo collegata

Titolo	Numero Rule	Breve spiegazione del legame
Global Operational Regulation “Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio”	FB 004_2024	La GOR ha lo scopo di definire i criteri di classificazione e di profilatura del rischio della clientela ed i requisiti di adeguata verifica della clientela.
Global Policy “Sanzioni Finanziarie”	FB 046_2023	La GP ha l’obiettivo di garantire la conformità alle disposizioni di natura normativa e regolamentare in materia di Sanzioni Finanziarie; di evitare l’insorgenza di possibili violazioni; di proteggere la reputazione del Gruppo e definire i principi e le regole per limitare le attività con i paesi, le entità e i soggetti che sono sottoposti a sanzioni finanziarie.
Global Operational Regulation “Sanzioni Finanziarie”	FB 006_2024	La GOR definisce i principi e le regole di gestione dei rischi relativi alle Sanzioni Finanziarie, e stabilisce gli standard minimi dei controlli da implementare. È applicabile a FinecoBank e alle società destinatarie del Gruppo.
Global Operational Regulation “Valutazione dei rischi di riciclaggio e sanzioni finanziarie di Gruppo”	FB 016_2024	La GOR definisce i principi e le regole per il Risk Assessment AML/FS a cui ciascuna Società del Gruppo è esposta e al contempo disegna la metodologia di valutazione dei rischi di riciclaggio di Gruppo, tenendo conto dei risultati derivanti dagli

² Modifica minor: approvazione Entità destinatarie non necessaria. Prima release/Sostituzione: approvazione Entità destinatarie necessaria.

Titolo	Numero Rule	Breve spiegazione del legame
		<p>esercizi di Risk Assessment AML di ciascuna Società del Gruppo, delle interrelazioni tra le stesse e del loro impatto sull'esposizione al rischio a livello di Gruppo.</p>
<p>Global Operational Regulation “Le procedure di acquisizione della clientela a distanza”</p>	<p>FB 041_2023</p>	<p>La GOR definisce i requisiti e le misure che le Società del Gruppo prevedono per adempiere agli obblighi di adeguata verifica della clientela laddove acquisiscano nuovi clienti a distanza nonché le procedure i controlli da adottare in tali circostanze ovvero nei casi di ricorso a terzi in tutto o parte del processo di onboarding a distanza della clientela.</p>
<p>Global Operational Regulation “Screening dei pagamenti e dei clienti”</p>	<p>FB 034_2022</p>	<p>La GOR definisce i requisiti minimi per lo screening dei pagamenti e dei clienti. È applicabile a FinecoBank e alle società destinatarie del Gruppo.</p>
<p>Global Operational Regulation “Monitoraggio delle transazioni per la prevenzione del riciclaggio e del finanziamento del terrorismo”</p>	<p>FB 024_2022</p>	<p>La GOR definisce i requisiti da rispettare per garantire la conformità con la normativa vigente di monitoraggio delle transazioni per identificare attività di riciclaggio e finanziamento del terrorismo.</p>

Indice

1. Introduzione.....	7
1.1 Scopo del documento	7
2. Destinatari	8
3. Il contesto normativo di riferimento	8
4. Glossario e acronimi.....	9
5. Ruolo e responsabilità degli Organi Aziendali della Capogruppo	17
5.1. Organo con funzioni di Supervisione Strategica.....	17
5.2. Organo con funzioni di Gestione.....	18
5.3. Esponente Aziendale responsabile per l'antiriciclaggio	19
5.4. Organo con funzioni di Controllo.....	21
6. Disposizioni generali applicabili al Gruppo Fineco	21
6.1 Ruolo e responsabilità delle Funzioni Aziendali: la Funzione Antiriciclaggio	22
6.2. Il Responsabile Antiriciclaggio	24
6.5. Altre Funzioni.....	25
7. AML Business Risk Assessment e valutazione del rischio	26
7.1. Valutazione del rischio e classificazione del cliente	27
8. Adeguata verifica della clientela	30
8.1. Tipi di adeguata verifica e attribuzione e gestione del profilo di rischio del cliente.....	31
8.1.1. <i>Adeguata verifica semplificata – Rischio Basso</i>	32
8.1.2. <i>Adeguata verifica rafforzata – Rischio Alto</i>	32
8.1.3. <i>Adeguata verifica ordinaria – Rischio Medio</i>	34
8.1.4 <i>Adeguata verifica – Monitoraggio continuo</i>	34
8.2. Identificazione e verifica della clientela	36
8.3. Identificazione e verifica del titolare effettivo	37
8.4. Identificazione a distanza.....	38
8.5. Scopo/natura dell'attività economica e fonte del patrimonio	39
8.6. Potere di Rappresentanza	39
8.7. Controlli dei nominativi.....	40
8.8. Approvazione della relazione	40
8.9. Relazioni d'affari vietate.....	40
8.10. Controlli nel corso del rapporto d'affari.....	41
8.11. Condivisione delle informazioni riguardanti il Cliente nel Gruppo	41
8.12. Escalation	41
9. Conservazione della documentazione delle informazioni e delle operazioni e messa a disposizione di dati e informazioni alle autorità	42
9.1. Capogruppo - Messa a disposizione dei dati: il Nuovo Archivio Unico Informatico	43
9.2 Capogruppo - Esenzioni	43
9.3 Capogruppo - Le Comunicazioni Oggettive, le Segnalazioni Antiriciclaggio Aggregate (S.AR.A.), flussi DEPRU e TRU.....	44
10 Segnalazione di operazioni sospette e segnalazione di violazioni	44
10.1. <i>Individuazione e segnalazione delle operazioni sospette</i>	44
10.2. <i>Segnalazione di violazioni</i>	45
11. Obblighi di formazione.....	45
12. Sistemi informativi a supporto	46
13. Capogruppo - Limitazioni all'uso del contante e dei titoli al portatore.....	47
13.1. Obbligo di comunicazione delle infrazioni al ministero dell'economia e delle finanze	47
14. Esternalizzazione	48
15. Misure di contrasto finanziario del terrorismo e dell'attività di paesi che minacciano la pace e la sicurezza – linee guida	49
16. Capogruppo - Trasferimenti di fondi	49
16.1. Casi di esclusione.....	50
16.2. Gli obblighi del prestatore di servizi di Pagamento.....	50
16.2.1. <i>Gli obblighi del prestatore dei servizi di pagamento dell'ordinante (PSP dell'ordinante)</i>	51

16.2.2. <i>Gli obblighi del prestatore dei servizi di pagamento del beneficiario (PSP del beneficiario)</i>	51
16.2.3. <i>Obblighi di monitoraggio, valutazione e segnalazione</i>	52
16.2.4. <i>Controlli e monitoraggio</i>	52
16. <i>Valutazioni e segnalazioni</i>	52
17. <i>Monitoraggio dei controlli</i>	52
18. <i>Sanzioni</i>	53

1. Introduzione

FinecoBank S.p.A, in qualità di Capogruppo - in conformità alle leggi e regolamenti vigenti³ ed in coerenza con il sistema di coordinamento manageriale di gruppo definito dalle Group Managerial Golden Rules - emette linee guida, nell'interesse della stabilità del Gruppo, allo scopo di esercitare compiutamente il proprio ruolo di gestione e coordinamento.

Il presente documento integra la normativa di Gruppo, è direttamente applicabile alla Capogruppo⁴ ed è indirizzato alle Entità del Gruppo (Entità o Società) destinatarie secondo un principio di proporzionalità⁵, vale a dire considerando la rilevanza economica, la dimensione e la complessità operativa e organizzativa.

Come previsto dalla Global Policy di Gestione della Normativa di Gruppo, il presente documento sarà adottato in conformità ai requisiti e alle normative vigenti localmente; in caso di qualsiasi conflitto tra codesta Global Rule (di seguito anche GR) e la legge locale applicabile (o in caso di maggiori restrizioni), quest'ultima prevale.

Dopo l'approvazione da parte degli organi deputati di Fineco, la stessa, in qualità di Capogruppo, trasmette la GR alle Entità destinatarie per l'approvazione da parte dei rispettivi Organi Societari e ne monitora la corretta e tempestiva implementazione anche avvalendosi delle sue funzioni interne di volta in volta identificate. In seguito alla distribuzione della normativa, l'attività di monitoraggio inerente il recepimento delle presenti disposizioni risulta in capo al Responsabile Antiriciclaggio di Capogruppo.

In particolare, per l'approvazione del presente documento è prevista la competenza per tutte le Società del Gruppo in capo ai rispettivi Organi con funzione di supervisione strategica.

Le Società del Gruppo sono pertanto tenute ad avviare tempestivamente – dopo l'opportuna valutazione ed approvazione da parte dei propri Organi competenti – le necessarie attività finalizzate alla corretta applicazione del presente documento.

Nel caso in cui la Società ritenesse:

- la presente Global Rule non applicabile, ovvero
- necessario apportare delle modifiche/deroghe alle previsioni contenute nella presente Global Rule,

ai fini della conformità con la normativa locale (se più restrittiva) o in ragione di vincoli di natura organizzativa ed operativa, la Società, ai sensi di quanto disposto dalla normativa di Gruppo vigente (Gestione della Normativa di Gruppo), dovrà formulare alla Direzione Antiriciclaggio e Anticorruzione di Capogruppo una richiesta di Non Binding Opinion (NBO).

1.1 Scopo del documento

La Capogruppo FinecoBank, 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, emette la presente *Global Policy "Policy Antiriciclaggio e Antiterrorismo"* (di seguito anche "Global Policy" o "Policy").

In particolare, la presente Global Policy:

³ Normative interne ed esterne vigenti alla data di emanazione del presente documento; successivi aggiornamenti, ove tempo per tempo applicabili.

⁴ In caso divergenza tra le Responsabilità della Capogruppo indicate nella presente normativa e quelle riportate nel Regolamento degli Organi Aziendali, Statuto, Regolamento Interno, Poteri Delegati di FinecoBank tempo per tempo vigenti, prevalgono sempre queste ultime.

⁵ Tale principio mira ad assicurare che i singoli dispositivi di governance siano coerenti con il profilo di rischio individuale, con la natura e il modello di business della Società del Gruppo nonché con la portata e la complessità delle proprie attività, ai fini dell'effettivo conseguimento degli obiettivi previsti dagli obblighi normativi.

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 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 del 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 di 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 presente Global Policy è indirizzata a tutte le Società del Gruppo e si applica a tutti i Dipendenti. Le 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 considerazione 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 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 ad essa collegate. Qualora un Dipendente abbia il sospetto che una determinata attività/comportamento possa essere associata/o ad una fattispecie di riciclaggio è tenuto a fare opportuna segnalazione seguendo le modalità previste 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.

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 e successive modifiche, come implementata localmente negli stati in cui operano le Società del Gruppo (per l'Italia, il D. Lgs. n. 231/2007 e successive modifiche)
- Regolamento UE 2015/847 riguardante i dati informativi che accompagnano il trasferimento dei fondi e successive modifiche
- Regolamento UE 2024/886 che modifica i Regolamenti n. 260/2012 e 2021/1230 e le direttive 98/26/CE e 2015/2366 per quanto riguarda i bonifici istantanei in euro
- Direttiva (UE) 2018/843 o V Direttiva AML/CFT, come implementata localmente negli stati in cui operano le Società del Gruppo, che abroga le Direttive 2005/60/CE e 2006/70/CE e integra la IV Direttiva AML
- Direttiva (UE) 2018/1673 in tema di lotta al riciclaggio mediante il diritto legale, come implementata localmente negli stati in cui operano le Società del Gruppo (per l'Italia, il D. Lgs. n. 195/2021)

- Orientamenti EBA in materia di adeguata verifica della clientela e di individuazione dei fattori di rischio di riciclaggio e di finanziamento del terrorismo del 1° marzo 2021 come recepiti dai singoli stati membri (EBA/GL/2021/02)
- Orientamenti EBA sulle politiche e le procedure relative alla gestione della conformità e al ruolo e alle responsabilità del responsabile antiriciclaggio ai sensi dell'articolo 8 e del capo VI della direttiva (UE) 2015/849 (EBA/GL/2022/05), come recepiti dai singoli stati membri
- Orientamenti EBA sull'utilizzo di soluzioni di onboarding a distanza del cliente (EBA/GL/2022/15), come recepiti dai singoli stati membri
- Orientamenti sulle politiche e sui controlli per la gestione efficace dei rischi di riciclaggio e di finanziamento del terrorismo nel fornire accesso ai servizi finanziari (EBA/GL/2023/04).

In particolare, per la sola Capogruppo, sono stati altresì considerati i seguenti riferimenti normativi nazionali:

- 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 della Banca d'Italia in materia di organizzazione, procedure e controlli interni per finalità antiriciclaggio” e successive modifiche tra cui il Provvedimento del 1° agosto 2023.
- Provvedimento della Banca d'Italia del 30 luglio 2019 recante disposizioni attuative in materia di adeguata verifica della clientela e successive modifiche tra cui il Provvedimento del 13 giugno 2023.
- Provvedimento della Banca d'Italia del 24 marzo 2020 recante disposizioni per la conservazione e la messa a disposizione dei documenti, dei dati e delle informazioni per il contrasto del riciclaggio e del finanziamento del terrorismo.
- Provvedimento UIF del 25 agosto 2020 relativo alla produzione e all'invio delle segnalazioni antiriciclaggio aggregate S.A.R.A.
- Provvedimento del 12 maggio 2023 della UIF di emanazione dei nuovi indicatori di anomalia per l'individuazione delle operazioni sospette ai fini antiriciclaggio.
- Il Decreto nr. 55 del Ministero dell'Economia e delle Finanze del'11 marzo 2022 MEF in materia comunicazione, accesso e consultazione dei dati e delle informazioni relativi alla Titolarità Effettiva di Imprese dotate di personalità giuridica, di Persone Giuridiche Private, di Trust Produttivi di effetti giuridici rilevanti ai fini fiscali e di Istituti Giuridici affini al Trust.

4. Glossario e acronimi

Parola chiave	Definizione
Adeguata Verifica o Know Your Customer (KYC)	L'adeguata verifica che le Società del Gruppo devono eseguire per identificare i propri clienti ed accertare le informazioni rilevanti al fine di eseguire operazioni con loro.
Alta Direzione	Nella presente normativa, per Alta Direzione s'intende l'Amministratore Delegato, il Direttore Generale, Vice Direttore Generale e i responsabili delle funzioni aziendali di controllo.

Parola chiave	Definizione
Alto Dirigente	Nella presente normativa, per Alto Dirigente s'intende 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 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 più del 25% del capitale del Cliente.
Attività Criminosa	Ai sensi dell'art. 2 della Direttiva (UE) 2018/1673: qualsiasi tipo di coinvolgimento criminale nella commissione di un qualsiasi reato punibile, conformemente al diritto nazionale, con una pena detentiva o con una misura privativa della libertà di durata massima superiore a un anno ovvero, per gli Stati membri il cui ordinamento giuridico prevede una soglia minima per i reati, di un qualsiasi reato punibile con una pena detentiva o con una misura privativa della libertà di durata minima superiore a sei mesi. I reati che rientrano nelle seguenti categorie sono considerati un'attività criminosa: partecipazione a un gruppo criminale organizzato e al racket; terrorismo; tratta di esseri umani e traffico di migranti; sfruttamento sessuale; traffico illecito di stupefacenti e sostanze psicotrope; traffico illecito di armi; traffico illecito di beni rubati e altri beni; corruzione; frode; falsificazione di moneta; contraffazione e pirateria di prodotti; reati ambientali; omicidio, lesioni fisiche gravi; rapimento, sequestro di persona e presa di ostaggi; rapina o furto; contrabbando; reati fiscali relativi a imposte dirette e indirette, conformemente al diritto nazionale; estorsione; contraffazione; pirateria; abuso di informazioni privilegiate e manipolazione del mercato; criminalità informatica.
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 a un gruppo finanziario soggetto a un'efficace vigilanza su base consolidata.
Capogruppo	FinecoBank S.p.A. (di seguito anche "FinecoBank", "Fineco" o "Banca").

Parola chiave	Definizione
Cliente	Il soggetto che instaura o ha in essere rapporti continuativi (per la Capogruppo, con o senza un rapporto di conto corrente) 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.
Clients Corporate	Clients 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.
Clients Private ai fini AML ⁶	Clients che dispongono di ingenti patrimoni, assistiti da un Relationship Manager (es. un Consulente Finanziario) che cura in maniera continuativa la relazione personalizzata con i medesimi e che sono destinatari di servizi bancari e finanziari personalizzati. La definizione include i Clients Corporate.
Società Controllata	Entità direttamente o indirettamente controllata da FinecoBank S.p.A. (di seguito anche "Entità controllata" o "Società controllata" o in breve, "LE").
Controlli di Linea	Controlli effettuati dalle strutture operative (ad es., controlli di tipo gerarchico, sistematici e a campione), anche attraverso unità dedicate esclusivamente a compiti di controllo che riportano ai responsabili delle strutture operative, ovvero eseguiti nell'ambito del back office, incorporati nelle procedure informatiche e diretti ad assicurare il corretto svolgimento delle operazioni.
Dati Biometrici	Dati personali relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali immagini del volto o dati dattiloscopici, ottenuti e trattati con mezzi tecnici.
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 – PFA), 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.

⁶ I Clients qualificati come Private esclusivamente per finalità di natura commerciale, ai quali sono riservate condizioni economiche di maggior favore ma che non sono destinatari di servizi bancari personalizzati, non rientrano in tale definizione.

Parola chiave	Definizione
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.
Funzioni Aziendali di Controllo	La Funzione antiriciclaggio, la funzione di conformità alle norme (compliance), la funzione di controllo dei rischi (risk management) e la funzione di revisione interna (internal audit).
Gruppo	Gruppo FinecoBank, composto da FinecoBank S.p.A. e dalle Società/Legal Entities del Gruppo (di seguito anche "Gruppo Fineco" o "Gruppo FinecoBank").
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).
Operatività a Distanza	Operatività 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.
Operazione Occasionale	Operazione non riconducibile a un rapporto continuativo in essere con un cliente, sia che venga effettuata con una transazione unica, sia che comprenda più transazioni che appaiono collegate (es. operazioni di cessione del credito da parte di controparti non correntiste, negoziate nell'ambito dello stesso contratto).
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.
Organo di gestione	L'organo o gli organi di un ente creditizio o un istituto finanziario designati conformemente al diritto nazionale ai quali è conferito il potere di stabilire gli indirizzi strategici, gli obiettivi e la direzione generale dell'ente creditizio o dell'istituto finanziario, e che supervisionano e monitorano il processo decisionale della dirigenza. La definizione comprende anche le persone che dirigono di fatto l'attività dell'ente o dell'istituto. (rif. EBA/GL/2022/05).
Organo di gestione nella sua funzione di supervisione strategica	L'organo di gestione che agisce nel suo ruolo di supervisione e controllo del processo decisionale della dirigenza. (rif. EBA/GL/2022/05).

Parola chiave	Definizione
Organo di gestione nella sua funzione di gestione	L'organo di gestione che agisce nel suo ruolo di amministrazione quotidiana dell'ente creditizio o dell'istituto finanziario. (rif. EBA/GL/2022/05).
Organizzazioni senza scopo di lucro (o Organizzazioni non profit, in breve NPO)	Una persona non fisica o un istituto giuridico o un'organizzazione che si occupa principalmente della raccolta o dell'erogazione di fondi a fini caritativi, religiosi, culturali, educativi, sociali o solidali.
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 Cliente 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 ad Alto Rischio	I Paesi identificati ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2015/849 e presenti nelle liste del FATF-GAFI, ossia i paesi che presentano carenze strategiche in particolare per quanto riguarda il quadro legale ed istituzionale AML/CFT del paese, i poteri e le procedure di cui dispongono le autorità competenti del paese ai fini della lotta al riciclaggio e al finanziamento del terrorismo, l'efficacia del sistema AML/CFT per contrastare i rischi di riciclaggio o di finanziamento del terrorismo del paese.
Persona Politicamente Esposta (PEP)	Qualsiasi persona che occupi (o abbia cessato di occupare da meno di 12 mesi) una posizione pubblica preminente/importante, o che sia in strettamente collegata o in rapporto di parentela diretto con una persona in tale posizione.
Red flag/Indicatori di anomalia	Tipologie o indicatori di rischio utilizzati per identificare comportamenti e transazioni 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.

Parola chiave	Definizione
Riciclaggio del denaro	<p>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 della normativa antiriciclaggio applicabile alle Società del Gruppo il riciclaggio include:</p> <p>a. la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da <i>un'attività criminosa</i> 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;</p> <p>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;</p> <p>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;</p> <p>d. la partecipazione a uno degli atti previsti dalle lettere precedenti, l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolare l'esecuzione.</p>
Rischio di riciclaggio	<p>Il rischio derivante dalla violazione di previsioni di legge, regolamentari e di autoregolamentazione funzionali alla prevenzione dell'uso del sistema finanziario per finalità di riciclaggio, di finanziamento del terrorismo o di finanziamento dei programmi di sviluppo delle armi di distruzione di massa, nonché il rischio di coinvolgimento in episodi di riciclaggio e di finanziamento del terrorismo o di finanziamento dei programmi di sviluppo delle armi di distruzione di massa.</p>
Sanzioni Finanziarie	<p>Restrizioni all'attività economica, finanziaria e commerciale dirette contro specifici governi di paesi terzi, persone fisiche o entità, settori o tipi di attività, attuate da organismi internazionali (quali ad esempio l'ONU, l'UE, il Regno Unito e il Consiglio Europeo) o dagli organismi competenti statali/federali degli Stati Uniti o di altri paesi mediante leggi e regolamenti. Le Sanzioni sono misure o pacchetti di misure decise per colpire la proliferazione delle armi di distruzione di massa, aggressioni, atti di terrorismo, azioni criminali e violazioni dei diritti umani. Tali misure intendono incentivare un cambiamento nel comportamento da parte del regime o del paese sottoposti a Sanzioni o privare i terroristi e i criminali dell'accesso ai fondi.</p>
Settore ad Alto Rischio	<p>Settore definito dalla Banca come esposto alla corruzione, alla concussione, alla frode, ad altre attività criminali, a comportamenti finalizzati a riciclare proventi illeciti, o fondi destinati a finanziare il terrorismo o programmi di sviluppo delle armi di distruzione di massa.</p>
Società Fiduciaria	<p>Società costituita per detenere (intestataro registrato) e amministrare in qualità di custode attività per conto di un'altra persona o società.</p>

Parola chiave	Definizione
Società del Gruppo	Società del Gruppo FinecoBank, intendendo la stessa Capogruppo FinecoBank e le sue Società controllate.
Società controllata del Gruppo	Entità direttamente o indirettamente controllata da FinecoBank S.p.A. (di seguito anche "Entità controllata" o "Società controllata" o "Entità" o "Legal Entity" in breve "LE").
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").
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 sull'identità	Controllo di veridicità delle prove documentali presentate da un Cliente o da una Fonte Dati Riconosciuta per convalidare le informazioni.

Acronimo	Definizione
AFC	Anti-Financial Crime
AML	Anti-Money Laundering
CDD	Customer Due Diligence
CTF	Countering of Terrorist Financing
EBA	Autorità Bancaria Europea
EDD	Enhanced Due Diligence

FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
DEPRU	Depositi russi e bielorusi
KYC	Know Your Customer
OFAC	US Office of Foreign Assets Control of the US Department of the Treasury
PEP	Politically Exposed Person
SOS	Segnalazione di Operazione Sospetta
SDD	Simplified Due Diligence
SPV	Special Purpose Vehicles
STR	Suspicious Transaction Report
TRU	Trasferimenti Russi
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 rischio⁷, 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 e ogni successivo aggiornamento della stessa che illustra e motiva le scelte che la Banca e il Gruppo compiono 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 Antiriciclaggio, sentito l'organo con funzioni di controllo con il supporto del Comitato Nomine e previo parere del Comitato Rischi e Parti Correlate ("CRPC"). La verifica del possesso dei requisiti deve risultare analiticamente nel verbale di nomina;
- nomina e revoca il responsabile delle segnalazioni di operazioni sospette, sentito l'organo con funzioni di controllo, con il supporto del Comitato Nomine e previo parere del CRPC;
- 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 nonché un sistema di condivisione della documentazione che consenta agli organi aziendali accesso diretto alle relazioni delle Funzioni di Controllo in materia antiriciclaggio, alle pertinenti comunicazioni intercorse con le Autorità e alle misure di vigilanza imposte o alle sanzioni irrogate;
- 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;
- con cadenza almeno annuale, valuta l'attività della funzione antiriciclaggio e l'adeguatezza delle risorse umane e tecniche a essa assegnate anche alla luce della periodica verifica svolta dalla funzione di revisione interna;

⁷ Al fine di applicare le disposizioni normative coerentemente con il principio di proporzionalità, la Banca considera almeno: il totale di bilancio, eventualmente consolidato; la presenza geografica e il volume di attività in ciascuna area; il numero dei dipendenti; la forma giuridica adottata e l'appartenenza ad un gruppo; i tipi di attività esercitate nonché la loro natura e complessità; il modello di business scelto e le strategie adottate; il tipo di struttura organizzativa; la strategia complessiva predisposta per l'efficace gestione dei rischi; gli assetti proprietari e le modalità di finanziamento; il numero e la tipologia di clienti e la complessità dei prodotti e dei contratti; le attività esternalizzate e i canali di distribuzione utilizzati

- 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;
- nomina l'Esponente Aziendale responsabile per l'antiriciclaggio (l'“Esponente Responsabile per l'AML”) della Capogruppo e del Gruppo nei tempi previsti dalla normativa di riferimento e verifica che lo stesso soddisfi le condizioni definite nella normativa ivi incluse quelle previste al successivo paragrafo 5.3 della presente Global Policy;
- assicura che l'Esponente Responsabile per l'AML sia tempestivamente informato delle decisioni che possono incidere sull'esposizione al rischio di riciclaggio della Banca.

In osservanza alle disposizioni previste in tema, l'Esponente Responsabile per l'AML sarà nominato non oltre il primo rinnovo degli organi sociali e comunque non oltre il 30 giugno 2026. In tale ottica, le statuizioni previste nel presente documento relative all'Esponente Responsabile per l'AML si intendono applicabili solo dopo la sua nomina.

5.2. Organo con funzioni di Gestione

L'Organo con funzione di Gestione di Fineco è costituito dall'Amministratore Delegato e 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 tutte le misure necessarie ad assicurare l'efficacia dell'organizzazione e del sistema dei controlli antiriciclaggio; a tal fine esamina le proposte di interventi organizzativi e procedurali presentate dal responsabile della funzione antiriciclaggio e formalizza, motivandola, l'eventuale decisione di non accoglierle. 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:

- definisce e cura l'attuazione delle iniziative e delle procedure necessarie per assicurare il tempestivo assolvimento degli obblighi di comunicazione alle Autorità previsti dalla normativa antiriciclaggio;
- definisce la policy antiriciclaggio sottoposta all'approvazione dell'organo con funzione di supervisione strategica e ne cura l'attuazione;
- definisce e cura l'attuazione di flussi e 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 dalla Capogruppo;
- 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;
- assicura, nei casi di esternalizzazione dei compiti operativi della funzione antiriciclaggio, il rispetto della normativa applicabile e riceve periodiche informazioni sullo svolgimento delle attività esternalizzate.

5.3. Esponente Aziendale responsabile per l'antiriciclaggio

L'incarico di Esponente Responsabile per l'AML ha natura esecutiva e i compiti assegnati non possono essere delegati a terzi (ad es. dirigenti incardinati nell'organizzazione dell'intermediario).

L'Esponente Responsabile per l'AML:

- deve essere in possesso di adeguate conoscenze teoriche e pratiche riguardo ai rischi di riciclaggio, le politiche, i controlli e le procedure antiriciclaggio nonché il modello di business della Capogruppo e del settore in cui opera;
- possiede competenze circa la gestione dei rischi (individuazione, valutazione, monitoraggio, controllo e mitigazione delle principali tipologie di rischio della Banca) nonché dei sistemi di controllo interno;
- dispone di risorse adeguate ad assolvere efficacemente ai propri compiti.

L'Esponente Responsabile per l'AML possiede i requisiti di onorabilità e professionalità correttezza, rispetta i criteri di correttezza e competenza previsti dal Decreto MEF n. 169/2020 e dedica tempo adeguato allo svolgimento dell'incarico agendo con indipendenza di giudizio⁸.

In quest'ottica, all'atto della nomina e tempestivamente in caso di fatti sopravvenuti, l'Esponente Responsabile per l'AML comunica all'Organo con funzione di Supervisione strategica gli incarichi ricoperti all'interno della Banca e del Gruppo, e/o in altre società, imprese o enti, le altre attività lavorative e professionali svolte e le altre situazioni o fatti attinenti alla sfera personale o professionale che possano generare conflitti con l'incarico di Esponente Responsabile per l'AML.

Sul punto, si ha un conflitto di interesse quando il perseguimento degli ulteriori interessi possa inficiare la sua indipendenza di giudizio in qualità di Esponente Responsabile per l'AML.

Ferme restando le ipotesi di potenziale conflitto di interesse previste in capo agli esponenti dalla disciplina anche regolamentare vigente ed, in particolare, quelle previste dalla Policy "Verifica dei requisiti di idoneità degli Esponenti aziendali e dei Responsabili delle Principali Funzioni Aziendali di FinecoBank S.p.A.", tra le altre ipotesi da valutarsi caso per caso, è possibile che sussista un conflitto di interesse nelle seguenti situazioni:

- l'Esponente Responsabile per l'AML ha legami personali⁹ con il Responsabile della Funzione Antiriciclaggio o con i componenti della Funzione Antiriciclaggio della Banca;

⁸ In particolare, si fa riferimento ai requisiti di onorabilità e professionalità di cui agli artt. 4-10, 15 e 16 del Decreto MEF n. 169/2020 in materia di requisiti e criteri di idoneità allo svolgimento dell'incarico degli esponenti aziendali delle banche, degli intermediari finanziari, dei confidi, degli istituti di moneta elettronica, degli istituti di pagamento e dei sistemi di garanzia dei depositanti come disciplinati dalla Policy "Verifica dei requisiti di idoneità degli Esponenti aziendali e dei Responsabili delle Principali Funzioni Aziendali di FinecoBank S.p.A."

⁹ Per tali intendendosi i familiari stretti (i.e. coniuge, convivente more uxorio, figlio, genitore o altro familiare con cui il soggetto condivide la stessa dimora).

- ricopre incarichi operativi nelle aree deputate al presidio del rischio di riciclaggio e finanziamento del terrorismo o nelle aree oggetto di verifica antiriciclaggio e antiterrorismo;
- è direttamente coinvolto in operazioni, rapporti o clienti che formano oggetto di scrutinio da parte della Funzione Antiriciclaggio;
- è titolare di deleghe dirette ed esclusive su materie che abbiano un'attinenza o si pongano in conflitto con l'incarico di Esponente AML o con i poteri al medesimo attribuiti.

La presenza di un conflitto di interesse non indica di per sé che l'Esponente Responsabile per l'AML non possa essere considerato idoneo. Ciò si verifica solo se il conflitto di interesse pone un rischio rilevante e non sia possibile attenuare, gestire o prevenire adeguatamente il conflitto di interesse.

Al verificarsi di un conflitto di interesse rilevante in caso di fatti sopravvenuti, l'Esponente Responsabile per l'AML comunica la circostanza all'Organo di Supervisione Strategica che, a margine di una valutazione dettagliata, autorizza il protrarsi della situazione rilevata laddove non rilevi un difetto di indipendenza di giudizio individuando misure idonee ad attenuare, gestire o prevenire adeguatamente il conflitto di interesse, ovvero valuta di attribuire l'incarico di Esponente Responsabile per l'AML a un ulteriore membro del Consiglio di Amministrazione, idoneo per requisiti, competenza e disponibilità di tempo.

La Banca può individuare di volta in volta le misure più idonee ad attenuare, gestire o prevenire adeguatamente il conflitto di interesse, tra cui possono figurare la rimodulazione delle deleghe/competenze dell'Esponente Responsabile per l'AML, il monitoraggio da parte dell'Organo di Supervisione Strategica per il tramite di flussi forniti dal Responsabile della Funzione Antiriciclaggio e/o dalla Funzione Antiriciclaggio, ovvero attraverso l'obbligo dell'Esponente Responsabile per l'AML di riferire all'Organo di Supervisione Strategica su eventuali situazioni di conflitto di interesse.

L'Esponente Responsabile per l'AML di Capogruppo, che coincide con l'Esponente Responsabile per l'AML a livello di Gruppo, costituisce il principale punto di contatto tra il Responsabile della Funzione Antiriciclaggio e l'Organo di Supervisione Strategica e di Gestione e assicura che quest'ultimo disponga delle informazioni necessarie per comprendere pienamente la rilevanza dei rischi di riciclaggio cui la Capogruppo e il Gruppo sono esposti.

In particolare, l'Esponente Responsabile per l'AML;

- monitora che le politiche siano adeguate e proporzionate, tenendo conto delle caratteristiche della Capogruppo e dei rischi cui essa è esposta;
- coadiuva il Consiglio di Amministrazione nelle valutazioni concernenti l'articolazione organizzativa e la dotazione di risorse dedicate all'AML/CFT;
- assicura che gli Organi Aziendali siano periodicamente informati in merito alle attività svolte dal Responsabile Antiriciclaggio, nonché in merito alle interlocuzioni con le Autorità, garantendo flussi informativi in coerenza con quanto definito dal framework interno sul sistema dei controlli interni;
- informa gli Organi Aziendali delle violazioni e criticità concernenti l'antiriciclaggio di cui sia venuto a conoscenza e raccomanda le opportune azioni;
- verifica che il Responsabile Antiriciclaggio abbia accesso diretto a tutte le informazioni necessarie per l'adempimento dei propri compiti, che disponga di risorse umane e tecniche e di strumenti sufficienti e sia informato su eventuali carenze relative all'antiriciclaggio individuate dalle altre funzioni di controllo interno e dalle Autorità di Vigilanza;
- assicura che le problematiche e le proposte di intervento rappresentate dal Responsabile Antiriciclaggio siano opportunamente valutate dagli Organi Aziendali.

5.4. Organo con funzioni di Controllo

L'Organo con funzione di Controllo, cioè 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. Disposizioni generali applicabili al Gruppo Fineco

Gli indirizzi strategici in materia di gestione del rischio di riciclaggio e controlli antiriciclaggio applicabili al Gruppo Fineco sono adottati dagli Organi aziendali della Capogruppo.

A tal riguardo, la Capogruppo assicura che gli Organi aziendali delle altre Società del Gruppo attuino nella propria realtà aziendale le strategie e le politiche di gruppo in materia di antiriciclaggio e garantisce che gli Organi aziendali e le strutture interne di ciascuna componente del Gruppo, comprese le funzioni di controllo, dispongano delle informazioni necessarie per poter svolgere i relativi compiti.

Nell'ottica di sviluppare un approccio globale al rischio riciclaggio di Gruppo, la Capogruppo definisce politiche comuni con riferimento a:

- a) una metodologia di gruppo per la valutazione dei rischi di riciclaggio e l'istituzione di una base informativa comune che consenta di valutare in modo omogeneo la clientela;
- b) procedure formalizzate di coordinamento e condivisione delle informazioni rilevanti fra le società appartenenti al gruppo anche ai fini della individuazione delle operazioni sospette e una linea di riporto diretta tra i responsabili della funzione antiriciclaggio delle componenti, anche estere, del gruppo e il responsabile della funzione antiriciclaggio di gruppo;
- c) standard generali in materia di adeguata verifica della clientela, conservazione dei dati e individuazione e segnalazione delle operazioni sospette;
- d) procedure di controllo in materia di antiriciclaggio a livello di gruppo e attuazione tempestiva delle misure correttive necessarie al superamento delle carenze nei presidi antiriciclaggio riscontrate dalle competenti Autorità.

In particolare, sono fornite le linee guida di cui ai cap. 7 e successivi per l'adempimento degli obblighi in modo conforme alle disposizioni normative, i quali sono declinati, ai fini di una compiuta attuazione, nella specifica normativa interna e nelle procedure adottate da ciascuna Società del Gruppo.

Per il perseguimento delle predette finalità, la Capogruppo nomina il Responsabile della Funzione Antiriciclaggio di Gruppo, identificato nel Responsabile della Direzione Antiriciclaggio e Anticorruzione della

Banca, il quale - tra l'altro - verifica che le politiche e le procedure delle componenti del Gruppo siano in linea con gli standard definiti dalla Capogruppo oltre che conformi alle disposizioni legislative e regolamentari in materia antiriciclaggio loro applicabili.

Il Responsabile Antiriciclaggio di Gruppo riferisce direttamente, agli Organi Aziendali della Capogruppo e, ove richiesto, delle Società controllate. In particolare, il Responsabile Antiriciclaggio di Gruppo:

- predisporre un efficace Programma Antiriciclaggio e Antiterrorismo (incluse le Group Rules in materia) definendone le modalità di implementazione;
- sovrintende all'esercizio di valutazione dei rischi di riciclaggio condotto dalle Società del Gruppo;
- redige una valutazione dei rischi di riciclaggio di gruppo, tenendo conto dei rischi risultanti dagli esercizi individuali, delle interrelazioni tra le singole società del gruppo e del loro impatto sull'esposizione al rischio a livello di gruppo;
- presenta agli organi della capogruppo una relazione annuale, sull'esposizione ai rischi di riciclaggio e sulle attività della funzione antiriciclaggio a livello di gruppo;
- elabora e sottopone agli organi della Capogruppo procedure, metodologie e standard di gruppo in materia di antiriciclaggio e garantisce che le politiche e le procedure delle componenti del gruppo siano in linea con questi standard oltre che conformi alle disposizioni legislative e regolamentari in materia antiriciclaggio loro applicabili;
- fornisce consulenza, coordina e supervisiona l'implementazione dei Programmi Antiriciclaggio delle Società del Gruppo;
- analizza l'informativa periodica ricevuta dalle Società Controllate e si attiva di concerto con i Responsabili Antiriciclaggio locali per le eventuali azioni migliorative e correttive del caso.
- informa tempestivamente gli Organi Aziendali di violazioni o carenze rilevanti riscontrate nell'esercizio dei relativi compiti.

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

- implementare il Programma Antiriciclaggio e Antiterrorismo coerentemente con le linee di indirizzo definite dalla Capogruppo;
- assicurare che i controlli in ambito antiriciclaggio e antiterrorismo siano completati ed effettuati 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 Anticorruzione, stabilendo degli standard minimi di presidi antiriciclaggio per ciascuna Società del Gruppo.

6.1 Ruolo e responsabilità delle Funzioni Aziendali: la Funzione Antiriciclaggio

Fermo restando quanto previsto nel paragrafo precedente con riguardo alle disposizioni applicabili al Gruppo, in conformità al principio di proporzionalità e ove previsto dalle specifiche normative di riferimento, ciascuna Società del Gruppo istituisce un'apposita Funzione Antiriciclaggio, deputata a prevenire e contrastare la realizzazione di operazioni di riciclaggio.

La Funzione Antiriciclaggio delle Società del Gruppo è indipendente, dotata di risorse qualitativamente e quantitativamente adeguate ai compiti da svolgere, riferisce direttamente all'Organo 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 delle Società del Gruppo 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 finalizzate alla prevenzione e al contrasto dei rischi di riciclaggio;
- c) verificare nel continuo l'adeguatezza del processo di gestione dei rischi di riciclaggio e di finanziamento del terrorismo e l'idoneità del sistema dei controlli interni e delle procedure adottate e proporre, coinvolgendo le altre strutture aziendali interessate, le modifiche organizzative e procedurali necessarie ed 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 di finanziamento del terrorismo 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 e di finanziamento del terrorismo 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 e di finanziamento del terrorismo connesso all'offerta di prodotti e servizi nuovi, alla modifica significativa di prodotti o servizi già offerti, all'ingresso in un nuovo mercato o all'avvio di nuove attività e raccomandare le misure necessarie per mitigare e gestire questi rischi¹⁰;
- 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) ove richiesti dalla normativa locale trasmettere flussi periodici alle autorità locali competenti¹¹ ,;
- k) definire d'accordo con il responsabile delle segnalazioni di operazioni sospette, procedure di gestione delle segnalazioni interne (provenienti dal c.d. primo livello) riguardanti situazioni di rischio particolarmente elevato da trattare con la dovuta urgenza, per la successiva approvazione da parte dell'Organo con Funzione di Gestione;
- 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 a una loro sensibilizzazione alla conformità con la presente Policy e con gli adempimenti normativi valutando la stessa anche attraverso indicatori di efficacia dell'attività svolta;
- m) informare tempestivamente gli Organi Aziendali di violazioni o carenze significative riscontrate nell'esercizio dei relativi compiti e in generale;
- n) informare periodicamente gli organi aziendali circa lo stato di avanzamento delle azioni correttive adottate a fronte di carenze riscontrate nell'attività di controllo e circa l'eventuale inadeguatezza delle risorse umane e tecniche assegnate alla Funzione Antiriciclaggio e la necessità di potenziarle;

¹⁰ L'offerta di prodotti o servizi nuovi e l'avvio di nuove operatività che possono incidere sull'esposizione al rischio di riciclaggio del destinatario sono accompagnati da adeguati presidi e misure volte a mitigare questo rischio.

¹¹ Per la Capogruppo, trasmissione mensile alla UIF dei dati aggregati concernenti l'operatività complessiva della Banca; trasmissione delle comunicazioni oggettive

o) predisporre flussi informativi diretti agli Organi Aziendali, all'Esponente Responsabile per l'AML¹² e all'Alta Direzione.

In particolare, la Funzione Antiriciclaggio delle Società del Gruppo attiva processi di comunicazione in favore di questi ultimi prevedendo i seguenti flussi informativi:

- con cadenza periodica¹³, l'informativa dei flussi AML sulle attività di verifiche svolte, sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale;
- con cadenza almeno annuale, l'informativa annuale della Funzione Antiriciclaggio, riassuntiva delle attività svolte durante l'anno, le carenze e le disfunzioni accertate, le attività pianificate per il prossimo anno, completa dei risultati dell'esercizio di autovalutazione dei rischi di riciclaggio e finanziamento del terrorismo;
- specifiche informative su tematiche, carenze e violazioni considerate di particolare rilevanza;
- solo in favore dell'Esponente Responsabile per l'AML¹⁴, flussi informativi con cadenza trimestrale dedicati alle tematiche AML/CFT, al fine di garantire informazioni e dati sufficientemente esaurienti e tempestivi sui relativi rischi e sulla conformità ai requisiti normativi.

Inoltre, la Funzione Antiriciclaggio delle Società del Gruppo 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.

6.2. Il Responsabile Antiriciclaggio

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

Il Responsabile della Funzione Antiriciclaggio di ciascuna Società del Gruppo rientra nel novero dei responsabili di Funzioni Aziendali di Controllo, non ha responsabilità dirette di aree operative, né è gerarchicamente dipendente da soggetti responsabili di dette aree. La nomina e la revoca, adeguatamente motivate, sono di competenza dell'Organo di Supervisione Strategica, sentito l'Organo con funzioni di Controllo.

Il Responsabile della Funzione Antiriciclaggio delle Società del Gruppo ha la responsabilità di:

- fornire consulenza e supporto al Top Management relativamente a tematiche AML, coordinare e supervisionare l'implementazione dei Programmi Antiriciclaggio e Antiterrorismo;
- preparare politiche e procedure per l'onboarding a distanza del cliente, ove presenti, per ottemperare ai requisiti di adeguata verifica della clientela, per la successiva approvazione da parte dell'Organo con Funzione di Gestione; quindi, assicurare che le stesse siano attuate in modo efficace, riesaminate periodicamente e modificate se necessario;
- assicurare adeguati flussi informativi nei confronti degli organi aziendali, incluso, con cadenza almeno annuale la Relazione sulle attività svolte dalla Funzione AML e la Relazione di autovalutazione dei rischi di riciclaggio e di finanziamento al terrorismo cui è esposta la banca in relazione al business svolto per successivo inoltro all'autorità nazionale competente;

¹² Successivamente alla sua nomina, come rappresentato nei paragrafi che precedono.

¹³ Trimestrale per la Capogruppo.

¹⁴ Cfr. nota precedente.

In caso di esternalizzazione delle attività, il Responsabile della Funzione Antiriciclaggio delle Società del Gruppo è tenuto quantomeno a:

- monitorare, attraverso controlli periodici, il rispetto degli obblighi contrattuali e la corretta esecuzione del servizio da parte del fornitore;
- verificare che il servizio erogato dal fornitore consenta l'efficace adempimento degli obblighi antiriciclaggio;
- riferire regolarmente agli organi in merito allo svolgimento dei compiti esternalizzati in modo da assicurare che le misure correttive eventualmente necessarie siano tempestivamente adottate.

Al Responsabile della Funzione Antiriciclaggio delle Società del Gruppo, che assicura la titolarità e l'implementazione di un programma adeguato alla gestione delle Sanzioni Finanziarie, è assegnata la responsabilità in tema di Sanzioni Finanziarie.

6.3. Capogruppo - Le misure organizzative della Funzione Antiriciclaggio della Capogruppo

La Funzione Antiriciclaggio della Capogruppo è collocata all'interno della Direzione Antiriciclaggio e Anticorruzione e strutturata in tre Unit:

- Servizio Antiriciclaggio e Anticorruzione (nel seguito anche il "Servizio Antiriciclaggio"), che svolge ex-post tutte le attività più operative assegnate alla Funzione Antiriciclaggio, con particolare focus sulla gestione ongoing dei clienti con profilo di rischio alto;
- Governance e Controlli per Antiriciclaggio e Anticorruzione, che si occupa in particolare delle attività connesse alla governance e all'implementazione delle metodologie di valutazione del Rischio di Riciclaggio e di svolgimento dei controlli di secondo livello;
- SOS, dedicato alla gestione delle segnalazioni di operazioni sospette con a capo il Responsabile SOS, nominato con delibera del Consiglio di Amministrazione, sentito il Collegio Sindacale con il supporto del Comitato Nomine e previo parere favorevole del CRPC.

Le attività e i compiti svolti dalle Unit sopra descritte sono definiti in dettaglio nel Manuale Antiriciclaggio¹⁵ della Banca, oltre che nel Regolamento Interno e nei processi aziendali tempo per tempo vigenti.¹⁶

6.5. Altre Funzioni

Un efficace assetto organizzativo antiriciclaggio, si basa su un ampio coinvolgimento di tutte le strutture operative e delle funzioni aziendali e sulla chiara definizione dei compiti e responsabilità delle stesse articolate tra prima, seconda e terza linea di difesa come parte del sistema complessivo dei controlli interni.

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

- verifica del grado di adeguatezza dell'assetto organizzativo antiriciclaggio, dell'efficacia della funzione antiriciclaggio e la sua conformità rispetto alla normativa (Internal Audit);

¹⁵ Il Manuale Antiriciclaggio è il documento che definisce dettagliatamente responsabilità, compiti e modalità operative nella gestione del rischio di riciclaggio; è costantemente aggiornato, disponibile e facilmente accessibile a tutto il personale. E' redatto dalla Funzione Antiriciclaggio della Capogruppo ed è trasmesso all'Organo con funzione di Gestione e a quello con funzione di Supervisione Strategica.

¹⁶ La Funzione Antiriciclaggio della Capogruppo si occupa anche dei presidi relativi ai rischi connessi al terrorismo e alle "Sanzioni Finanziarie".

- implementazione delle regole di identificazione della clientela e verifica dei dati relativi alla clientela e di quelle relative all'adeguata verifica (Strutture di primo livello es, ove applicabile i Consulenti Finanziari, il Back Office);
- implementazione dei controlli di primo livello o Controlli di Linea diretti ad assicurare il corretto svolgimento delle operazioni, contribuendo al presidio del rischio di riciclaggio e finanziamento del terrorismo (strutture operative di primo livello es. 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 e hanno l'obbligo di trasferire alla stessa qualsiasi informazione relativa a fatti interni o esterni aventi possibili implicazioni in tema di Antiriciclaggio. Il personale chiamato a collaborare nella Funzione Antiriciclaggio, anche se inserito in aree operative, riferisce direttamente al Responsabile della Funzione per le questioni attinenti ai relativi compiti.

La Funzione Antiriciclaggio collabora con le altre funzioni aziendali (es. funzione di controllo di conformità, la revisione interna, area legale, organizzazione, gestione dei rischi, risorse umane, sistemi informativi) per sviluppare le proprie metodologie di gestione del rischio in modo coerente con le strategie e l'operatività aziendale, e realizzare processi conformi alla normativa esterna e interna di riferimento.

7. AML Business Risk Assessment e valutazione del rischio

Le Società del Gruppo valutano il rischio di riciclaggio connesso alle attività svolte/servizi prestati secondo una metodologia di risk assessment definita a livello di Gruppo.

La valutazione del rischio considera quantomeno il rischio di riciclaggio presentato dai clienti, prodotti e servizi, dalle giurisdizioni in cui le Società del Gruppo operano e offrono i loro servizi, 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 comunicata, 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 volti ad attenuare, per quanto possibile, i rischi identificati, incluso la valutazione dei rischi emergenti perché questi siano inclusi tempestivamente nelle valutazioni del rischio ML/TF connesso all'area di attività svolta.

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. Supranational Risk Assessment Report della Commissione Europea, l'Analisi Nazionale del Rischio, adottato dal Comitato di Sicurezza Finanziaria per la Capogruppo); i rapporti di valutazione reciproca adottati dal FATF-GAFI o analoghi organismi internazionali; i regolamenti comunitari o la normativa locale emanata a carico di persone e enti associati ad attività di finanziamento del terrorismo o a contrasto di attività che minacciano la pace e la sicurezza internazionale; gli esiti dell'attività di vigilanza e controllo da parte delle Autorità competenti e i documenti provenienti dalle stesse.

La valutazione dei rischi di riciclaggio e sanzioni finanziarie (“AML Business Risk Assessment”) è un processo aggiornato trimestralmente per riflettere eventuali modifiche al disegno e all'efficacia dell'assetto organizzativo e dei presidi di prevenzione e monitoraggio tempo per tempo implementati per la prevenzione dei rischi di riciclaggio e di finanziamento del terrorismo. L'esercizio di autovalutazione definito a livello di Gruppo è sottoposto ad approvazione da parte dell'Organo con funzione di Supervisione Strategica, previa validazione da parte del CRPC (per la Capogruppo) ed è trasmesso annualmente all'Autorità di Vigilanza, ove previsto dalla normativa locale applicabile alle Società del Gruppo.

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 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. L'approccio risk-based adottato dalle Società del Gruppo è comunque sempre rivolto a garantire che singoli clienti o specifiche categorie di soggetti abbiano accesso ai servizi finanziari di cui hanno bisogno e che tale accesso non venga loro negato per motivi di “rischio antiriciclaggio e di contrasto al finanziamento del terrorismo” non comprovati o senza un valido motivo, in linea con quanto previsto dagli Orientamenti EBA 2023/04.

In tale ottica, prima di adottare l'eventuale decisione di rifiutare o interrompere un rapporto continuativo, le Società del Gruppo devono accertarsi di aver preso in considerazione ed escluso tutte le possibili misure di mitigazione che si potrebbero ragionevolmente applicare nella fattispecie, tenendo conto del rischio di ML/TF associato al rapporto continuativo esistente o potenziale.

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, all'attività o professione svolta, alla sua reputazione e alle specificità dell'operazione o del rapporto continuativo da instaurare.

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

- rischio paese, connesso all'area geografica di residenza o sede del Cliente, del Titolare Effettivo e dei soggetti collegati o svolgimento della sua attività o con la quale ha relazioni lavorative;
- rischio di settore connesso con la prevalente attività svolta dal Cliente;
- rischio del prodotto e del servizio richiesto;
- rischio Entità (natura giuridica) per clienti diversi dalle persone fisiche;
- rischio del canale attraverso il quale avviene la prestazione dei servizi;
- rischio PEP e, ove rilevante carica pubblica ricoperta;
- 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 PEP¹⁷ fornite da un'organizzazione commerciale autorevole quale World Check/Refinitiv;
- 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/Refinitiv.

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 conseguente alla connessione del cliente, del titolare effettivo, dell'esecutore con i paesi identificati ai sensi dell'articolo 9, paragrafo 2, della direttiva (UE) 2015/849 e presenti nelle liste del FATF-GAFI, ossia i paesi che presentano carenze strategiche in particolare per quanto riguarda il quadro legale ed istituzionale AML/CFT del paese, i poteri e le procedure di cui dispongono le autorità competenti del paese ai fini della lotta al riciclaggio e al finanziamento del terrorismo, l'efficacia del sistema AML/CFT per contrastare i rischi di riciclaggio o di finanziamento del terrorismo del paese.

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, della vulnerabilità a reati finanziari e alla diffusione del fenomeno della corruzione.

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 di residenza, il paese di domicilio, il paese in cui il cliente o il suo esecutore hanno la sede della loro attività o le loro relazioni commerciali, finanziarie e/o familiari il paese di cittadinanza o l'area geografica di provenienza dei fondi. In particolare, quando il cliente ha collegamenti significativi con un'area geografica a rischio elevato, le Società del Gruppo valutano se sussiste una valida ragione economica o legale che giustifichi la tipologia di rapporto continuativo o di operazione richiesti ovvero se le necessità del cliente possano essere più propriamente soddisfatte nel paese col quale hanno il collegamento significativo.
- per le entità giuridiche:
 - il Paese in cui le stesse hanno relazioni commerciali e/o dove sono registrate e/o dove hanno sede;
 - il Paese di cui il Titolare Effettivo e gli esecutori hanno la cittadinanza;
 - il Paese in cui il Titolare Effettivo e gli esecutori sono residenti, e i Paesi in cui gli stessi abbiano domicilio, relazioni commerciali, finanziarie o familiari, il paese in cui abbiano sede altre attività economiche svolte dagli stessi.

RISCHIO DI SETTORE

¹⁷ Per la Capogruppo e per le Società del Gruppo eventualmente operanti in Italia è rilevante anche la lista dei Politici Locali (liste PIL).

Il rischio di settore è il rischio di compimento di un'Attività Criminosa relativa 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, a titolo esemplificativo e non esaustivo, 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 (quali i settori economici interessati dall'erogazione di fondi pubblici, anche di origine comunitaria, della raccolta e smaltimento di rifiuti, della produzione di energie rinnovabili); 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 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. Ulteriori rischi associati a prodotti, servizi o operazioni derivano dal livello di trasparenza o opacità del prodotto (es. prodotti o servizi che consentono al cliente di restare nell'anonimato o che favoriscono l'occultamento dell'identità (es. azioni al portatore, depositi fiduciari etc..), dalla complessità dello stesso (es. operazione che coinvolge una pluralità di parti o paesi).

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 es. *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 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. Per le Società del Gruppo valgono le disposizioni applicabili nella normativa di riferimento locale.

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

RISCHIO LEGATO AL CANALE DI DISTRIBUZIONE

Il rischio relativo al canale di distribuzione attiene alle modalità con cui il Cliente ottiene i prodotti o i servizi richiesti (a distanza, in presenza, tramite PFA etc.). Particolare attenzione, infatti, deve essere riposta in relazione all'operatività a distanza in considerazione dell'assenza del contatto diretto con il cliente o con l'esecutore.

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 connessi ad Attività Criminose, 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 del titolare effettivo o dell'esecutore. Quando sorgono dei dubbi circa la rilevanza delle informazioni negative, tali informazioni negative devono essere riportate alla Funzione Antiriciclaggio locale, la 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 instaurano 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 loro 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 vi 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 che scaturiscono in una segnalazione, 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 instaurano il rapporto continuativo ovvero non eseguono l'operazione richiesta dal Cliente. Se l'impossibilità si verifica per un rapporto continuativo in essere, le 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. In caso di rischio ALTO, il blocco dell'operatività può estendersi per 12 mesi, poi deve essere avviato il recesso unilaterale. Le Società del Gruppo documentano qualsiasi decisione di rifiutare o interrompere un rapporto continuativo e le relative motivazioni, nonché essere pronti, su richiesta, a mettere tale documentazione a disposizione della rispettiva Autorità competente.

Le Società del Gruppo valutano inoltre se inviare una segnalazione di operazione sospetta all'Autorità competente locale, se vi siano fondati motivi per sospettare che abbiano luogo o siano stati effettuati tentativi di attività di ML/TF.

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 Effettivo 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.

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:
 - i. all'identità del Cliente e del Titolare Effettivo o all'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. al 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.

Si precisa che l'Alto Dirigente acquisisce il parere della Funzione Antiriciclaggio per l'apertura o la prosecuzione di un rapporto continuativo con tutta la clientela caratterizzata da elevato profilo di rischio. Qualora decida di non adeguarsi al parere della Funzione Antiriciclaggio, l'Alto Dirigente è tenuto a formalizzare e motivare la decisione e a individuare le misure che saranno adottate per mitigare i rischi segnalati.

Le Società del Gruppo applicano obblighi rafforzati di adeguata verifica tenuto conto delle specifiche previsioni normative 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 avranno frequenza superiore a 12 mesi.

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

- il Cliente il suo Titolare effettivo o il suo Esecutore è una PEP;
- il Cliente è cointestatario di un soggetto PEP o ha fornito una delega a una PEP;
- il Cliente è un trust, una Società Fiduciaria o un Mandato Fiduciario;
- nell'assetto proprietario del cliente (Persona Giuridica) sono presenti trust e Società Fiduciarie;
- la Titolarità Effettiva di un Cliente è detenuta da azioni al portatore;
- il Cliente è un Cliente Private ai fini AML¹⁸;
- il Cliente il titolare effettivo e l'esecutore abbiano sede/residenza, domicilio o relazioni commerciali 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 preordinate;
- il Cliente, il Titolare effettivo e l'Esecutore ove rilevante è stato segnalato alle Autorità locali per sospetti di riciclaggio¹⁹;
- 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 carico²⁰.

In questi casi il soggetto incaricato dell'analisi del cliente a rischio alto può valutare le modalità appropriate per 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;

¹⁸ Vedi Glossario. Cfr. Indicazioni per i soggetti obbligati sull'applicazione degli obblighi in materia antiriciclaggio nella prestazione di servizi e attività di private banking, Banca d'Italia, 3 agosto 2023.

¹⁹ Tipicamente il profilo di rischio SOS rimane invariato per 5 anni; le regole per la declassificazione del rischio alto per SOS sono descritte nei processi di riferimento.

²⁰ Tipicamente il profilo di rischio crime rimane invariato per 5 anni; le regole per la declassificazione del rischio alto per notizia crime sono descritte nei processi di riferimento.

- 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;
- 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 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 effettuare una segnalazione di operazione sospetta all'autorità locale competente (UIF per la Capogruppo).

In presenza di clientela non correntista titolare di rapporti continuativi con la Società del Gruppo (es. mutuatari non correntisti e titolari di prestiti personali non correntisti) con profilo di rischio AML pari a "Basso", l'aggiornamento dei dati in esame può non essere richiesto secondo l'ordinaria frequenza quinquennale ma al ricorrere di specifiche circostanze quali, ad es., l'apertura di un nuovo rapporto continuativo.

I seguenti eventi richiedono la revisione dell'adeguata verifica del Cliente:

- revisione periodica dei clienti a profilo AML Alto;
- operatività anomala condotta dal Cliente (per la Capogruppo estratta dal sistema di monitoraggio delle transazioni 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;
- rilevazione di notizie negative rilevanti;
- richiesta specifica da parte della Funzione Antiriciclaggio.

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 secondo la tipologia del Cliente (Persona Fisica o Persona Giuridica);
- la verifica che la corretta documentazione della KYC sia in archivio e opportunamente aggiornata, in conformità alla tipologia del Cliente;

la verifica che i Soggetti Collegati identificati siano gli stessi, e l'identificazione degli eventuali nuovi soggetti.

Qualora i soggetti fossero cambiati, assicurarsi che venga effettuata una verifica adeguata in conformità alla tipologia del Cliente (se del caso); per tutti i nominativi interessati devono essere eseguiti adeguati controlli sui nominativi, come descritto nella presente policy e relativa GOR.

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

Quando un Cliente in continuità di rapporto richiede l'apertura di un ulteriore rapporto continuativo²¹ è tenuto ad aggiornare i dati rilasciati precedentemente (es. il questionario AML per la Capogruppo) in sede di adeguata verifica, o confermare la validità degli stessi.

Quando è stata superata la scadenza del riesame periodico, le informazioni di KYC precedentemente raccolte non possono essere utilizzate.

In fase di apertura di un nuovo rapporto continuativo è prevista l'acquisizione del questionario AML da parte del cliente, del titolare effettivo e dell'esecutore. Nel caso di apertura di un ulteriore rapporto continuativo, riconducibile ad un soggetto già cliente, contestualmente alla richiesta, è prevista la conferma della validità delle informazioni acquisite in precedenza.

In 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;
- clienti persone fisiche con profilo ALTO (non PEP): occorre distinguere a seconda della tipologia di rapporto continuativo/prodotto di riferimento;
- rapporti (mutuo, prestito personale, fidejussione bancaria) che comportino l'esposizione a nuovi rischi AML rispetto a quelli già valutati in occasione dell'apertura del primo conto corrente e deposito titoli, si richiede l'esecuzione dell'adeguata verifica rafforzata e l'autorizzazione all'apertura del rapporto da parte di un Alto Dirigente;
- rapporti (nuovi depositi di strumenti finanziari) che non comportino nuovi rischi AML rispetto a quelli già valutati in occasione dell'apertura del primo conto corrente e deposito titoli, l'esecuzione dell'adeguata verifica rafforzata e dell'autorizzazione di un Alto dirigente non è necessaria. È questo il caso, ad esempio, dei depositi di strumenti finanziari specificatamente dedicati ai servizi Advice, Plus, CashPark; Credit Lombard e richiesta di nuova carta di credito successiva alla prima.

²¹ Un rapporto di durata, rientrante nell'esercizio dell'attività di istituto svolta dai soggetti obbligati, che non si esaurisce in un'unica operazione.

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. Nel caso di cliente minore d'età l'identificazione può essere finalizzata sulla base di un'autocertificazione da parte del soggetto che eserciti la potestà genitoriale sul minore, purché tale soggetto sia cliente della Banca e purché le valutazioni dei rischi connessi a furti di identità e di frode debitamente acquisite, non rilevino una chiara esposizione a tali rischi che la Banca non può assumere.

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 NPO, 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 fisica²² 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

Si precisa che Il processo di onboarding della Clientela Corporate (persone giuridiche) da parte delle Società del Gruppo può avvenire solo tramite identificazione diretta di un Consulente Finanziario abilitato all'offerta fuori sede; pertanto, la procedura di identificazione da remoto tramite canale online non è applicabile a tale cluster di Clienti.

L'Allegato 1 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.

²² Si precisa che l'identificazione degli esecutori dei clienti persona fisica e persona giuridica è sempre prevista in presenza.

All'interno di specifica normativa di gruppo inerente al Remote Onboarding è prevista la descrizione dettagliata delle misure che le Società del Gruppo adottano per adempiere agli obblighi di adeguata verifica della clientela acquisita a distanza, nonché le procedure e i controlli da adottare in tali situazioni.

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 e/o verificando i dati identificativi forniti dal Cliente sulla base di fonti indipendenti ed autorevoli, come ad esempio il registro dei titolari effettivi.

La precisione delle informazioni riguardo alla titolarità effettiva rappresenta un elemento chiave del programma antiriciclaggio, perché queste informazioni sono necessarie a ricostruire chi sia il beneficiario ultimo del rapporto continuativo e dell'operazione rilevante. 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 rischio di 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, effettuare 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 proprietà diretta la titolarità di una partecipazione superiore al 25 per cento del capitale del cliente, detenuta da una persona fisica;
- b) costituisce indicazione di proprietà indiretta la titolarità di una percentuale di partecipazioni superiore al 25 per cento del capitale del cliente, posseduto per il tramite di società controllate, società 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 è 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, è 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.

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**, 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 più titolari effettivi, il titolare effettivo coincide con la persona fisica o le persone fisiche titolari di poteri di rappresentanza legale, amministrazione o direzione della società/ Cliente.

Le Società del Gruppo conservano traccia delle verifiche effettuate ai fini dell'individuazione del titolare effettivo.

In attuazione di quanto previsto dalla V Direttiva Antiriciclaggio, gli Stati Membri dell'UE sono tenuti ad istituire un Registro dei Titolari Effettivi, dove i soggetti dotati di personalità giuridica, i trust e i soggetti giuridici affini comunicheranno i dati del loro Titolare Effettivo e le successive variazioni in modo da renderli accessibili alle autorità e, secondo specifiche modalità anche al pubblico.

Le Società del Gruppo che presentano le caratteristiche indicate dalla normativa di riferimento, si organizzano al fine di individuare il relativo Titolare Effettivo e darne comunicazione al Registro istituito presso i paesi in cui le stesse hanno sede legale.

Chiarimenti relativamente alle modalità pratiche seguite per l'identificazione del Titolare Effettivo, compreso la consultazione delle informazioni presenti nel registro sulla titolarità effettiva laddove istituito localmente²³, sono forniti nella GOR - Requisiti di Adeguata Verifica della clientela in materia di Antiriciclaggio.

8.4. Identificazione a distanza

Le Società del Gruppo pongono particolare attenzione all'identificazione a distanza, in considerazione dell'assenza di un contatto diretto con il Cliente. L'Organo di gestione (rif. paragrafo n. 4 Acronimi e Glossario) approva le politiche e le procedure di onboarding a distanza del cliente e vigila sulla loro corretta attuazione.

Il Responsabile Antiriciclaggio assicura che le politiche e le procedure di onboarding dei clienti a distanza siano implementate in modo efficace, riviste regolarmente e modificate ove necessario.

Relativamente all'identificazione a distanza²⁴, le Società del Gruppo:

- acquisiscono i dati identificativi del Cliente attraverso i canali online 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 vigente²⁵. La validazione dei documenti identificativi caricati sul sito dal cliente può avvenire senza interrompere il processo di onboarding attraverso controlli automatici delle immagini caricate, analizzate sia da sistemi di intelligenza artificiale che da valutazioni di esperti che forniscono una valutazione in merito all'autenticità degli stessi e all'assenza di contraffazioni. Ulteriori controlli svolti in fase di istruttoria includono le chiamate alle banche dati per la profilatura del cliente ai fini AML. Le Società del Gruppo assicurano che le informazioni ottenute tramite i canali online siano adeguate e aggiornate; le immagini, i video, i suoni e i dati siano acquisiti in formato leggibile e con la qualità sufficiente per riconoscere il Cliente;

²³ Il registro sulla titolarità effettiva, alla data in cui si scrive, è sottoposto ai fini della istituzione/gestione/regolamentazione alle vigenti normative locali. Per la Capogruppo, non sono ancora state rilasciate le modalità operative di consultazione del medesimo e delle eventuali segnalazioni di difformità rilevate.

²⁴ Cfr. Orientamenti EBA – GL 2022/15.

²⁵ In particolare, la copia del documento di identità acquisiti a distanza non deve essere a sua volta la riproduzione di una fotografia o una scansione del documento d'identità originale.

- prevedono ulteriori elementi rafforzativi, quali, ad esempio, nel caso della Capogruppo, bonifico effettuato dal prospect da un intermediario bancario e finanziario terzo con sede in Italia o in un paese comunitario, con obblighi antiriciclaggio analoghi a quelli definiti dalla normativa AML applicabile alla Società del Gruppo²⁶ ovvero meccanismi di riscontro basati su soluzioni tecnologiche innovative e affidabili assistite da robusti presidi di sicurezza (es., quelle che prevedono forme di riconoscimento biometrico quali il cd. videoselfie, invio diretto di comunicazioni al cliente).

Tali meccanismi di remote onboarding, basati su soluzioni tecnologiche fornite da operatori esterni e riconosciuti dal mercato (ad es. Experian e Infocert per il mercato italiano) sono assoggettati a preventiva valutazione (i) sull'adeguatezza della soluzione in ordine alla completezza e all'accuratezza dei dati e dei documenti da raccogliere, nonché dell'attendibilità e indipendenza delle fonti di informazione che utilizzate; (ii) sull'impatto dell'utilizzo della soluzione scelta sui rischi a livello aziendale, compresi i rischi ML/TF, operativi, individuando anche possibili misure di mitigazione e delle azioni correttive per ciascuno dei rischi di cui sopra prevedendo infine l'effettuazione, di test per valutare se la soluzione scelta possa esporsi a frodi compresi i rischi di sostituzione di persona e altri rischi ICT e test end-to-end sulla compatibilità della soluzione scelta con la tipologia di clientela, prodotti e servizi offerti dalla Società del Gruppo. L'esito delle valutazioni è formalizzato in apposite Schede (c.d. "valutazione preliminare sulla soluzione di remote onboarding").

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 l'autorità per impegnare il Cliente nel rapporto in questione, e la sua identità deve essere verificata. L'autorità può essere implicita nel caso di un Amministratore unico o esponente equivalente.

²⁶ Previa esclusione dell'intermediario per motivi reputazionali.

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 dalla Funzione Antiriciclaggio, ma anche ottenere l'autorizzazione da parte di un Alto Dirigente locale.²⁷ La declassificazione di clientela PEP, dopo un anno dalla cessazione dell'incarico per il quale si è classificato PEP non è soggetta a specifica autorizzazione da parte dell'Alto Dirigente della Società del Gruppo, salvo che, in presenza di un elevato rischio di riciclaggio, le Società del Gruppo decidano di voler continuare ad applicare le misure di adeguata verifica rafforzata, nel qual caso il mantenimento della relazione in tali termini sarà soggetta ad approvazione da parte dell'Alto Dirigente della Società del Gruppo.

8.9. Relazioni d'affari vietate

Le Società del Gruppo non instaureranno relazioni d'affari con Banche di Comodo né effettueranno o consentiranno transazioni su conti anonimi. La Capogruppo, inoltre, identifica le relazioni d'affari vietate con le quali le Società del Gruppo Fineco non effettueranno transazioni sia per tener conto dei divieti applicabili in ragione della normativa vigente (es. quella sulle sanzioni finanziarie) sia per tener conto del risk-appetite del Gruppo in ambito di conformità alla normativa antiriciclaggio e antiterrorismo.

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. Altresì, esse non instaureranno, né manterranno relazioni di affari con clienti persone giuridiche quando l'identità del Titolare Effettivo (o dei Titolari Effettivi) che debba essere accertata in base alla presente Policy, non possa di fatto essere stabilita.

Le Società del Gruppo non instaureranno né manterranno relazioni né effettueranno transazioni collegate a persone fisiche o giuridiche individuate nell'Elenco delle Sanzioni Finanziarie dell'Unione Europea, nella Specially Designated Nationals and Blocked Persons List ('lista SDN') dell'Office of Foreign Assets Control (OFAC) nella lista Sanction UK e nelle Liste delle Nazioni Unite.

Inoltre, le Società del Gruppo non instaureranno rapporti con:

- società che svolgono servizi di cambio e trasferimento valuta, cioè offrono servizi di trasferimento e cambio valuta quali il 'money transfer', l'incasso di assegni e l'emissione/riscatto di traveller's cheques, nella misura in cui risultino entità non bancarie e non iscritte agli albi o i registri tenuti dalle Autorità;
- prestatori di servizi relativi all'utilizzo di valuta virtuale e/o di portafoglio digitale, salvo il caso di soggetti obbligati agli adempimenti prescritti dalla normativa antiriciclaggio e iscritti negli appositi albi o registri istituiti dalle Autorità di vigilanza dei paesi in cui gli stessi hanno sede;

²⁷ Salvo quanto previsto nella sezione 8.1.4 con riferimento ai conti Advise, Plus e Credit Lombard.

- persone fisiche o giuridiche delle quali è noto che sono attivamente coinvolte in attività criminose o terroristiche;
- soggetti operanti nei settori red light business/stupefacenti/armi;
- conti “omnibus” intestati a Società Fiduciarie, nella misura in cui non sono “trasparenti” né individuabili i singoli fiduciari titolari effettivi delle operazioni eterogenee che confluiscono sul rapporto omnibus intestato alla Società Fiduciaria cliente, compromettendo il corretto adempimento degli obblighi di adeguata verifica nonché di conservazione dei dati e delle informazioni pertinenti.

8.10. Controlli nel corso del rapporto d'affari

Le Società del Gruppo prevedono controlli continuativi nel corso del rapporto sull'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 per 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.

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 il 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 Società 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 Società controllata seguirà la normativa più stringente applicabile a livello locale.

8.12. Escalation

Se il Responsabile della Funzione Antiriciclaggio locale, stabilisce che un rapporto, operazione o pagamento potrebbe infrangere i divieti previsti nel presente documento, dovrà comunicare all'Unità organizzativa coinvolta che l'attività è vietata. Tale decisione sarà da considerarsi definitiva e vincolante. 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 della Funzione Antiriciclaggio locale, il Responsabile della Funzione Antiriciclaggio e Antiterrorismo locale può effettuare l'escalation all'Alto Dirigente Locale di grado superiore.

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.

9. Conservazione della documentazione delle informazioni e delle operazioni e messa a disposizione di dati e informazioni alle autorità

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

- copia o riferimenti ai documenti utilizzati per l'adeguata verifica del cliente;
- 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) con riferimento ai rapporti continuativi: il punto operativo di instaurazione del rapporto, la data di instaurazione e la data di chiusura del rapporto;
- b) con riferimento alle operazioni occasionali da sottoporre ad adeguata verifica e alle operazioni a valere sui rapporti continuativi: la data di effettuazione; l'importo; il segno monetario; la causale dell'operazione e il mezzo di pagamento utilizzato.
- c) con riferimento alle operazioni occasionali per le quali l'adeguata verifica non è dovuta, i destinatari conservano, oltre a quanto previsto dalla lettera b), i dati e le informazioni idonei a identificare in modo univoco il cliente e l'esecutore, nonché, ove noti, il settore di attività economica e i dati e le informazioni idonei a identificare in modo univoco il titolare effettivo
- d) i dati identificativi ivi compresi, ove disponibili, i dati ottenuti mediante i mezzi di identificazione elettronica e i pertinenti servizi fiduciari di cui al regolamento UE n. 910/2014 o mediante procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale del cliente, del titolare effettivo e dell'esecutore e le informazioni sullo scopo e la natura del rapporto o della prestazione;
- e) la consultazione, ove effettuata, dei registri sulla titolarità effettiva di persone giuridiche.

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, ove richiesto dalla normativa locale di riferimento, devono garantire che le informazioni vengano archiviate nelle rispettive procedure contabili informatizzate e che la documentazione venga conservata in sistemi di conservazione informatizzati che assicurino:

- a) l'accessibilità completa e tempestiva ai documenti, ai dati e alle informazioni da parte delle autorità competenti;
- b) l'acquisizione tempestiva, da parte dei destinatari, dei documenti, dei dati e delle informazioni, con indicazione della relativa data;

- c) l'integrità dei documenti, dei dati e delle informazioni e la non alterabilità dei medesimi successivamente alla loro acquisizione;
- d) l'adozione di idonee misure finalizzate a prevenire qualsiasi perdita dei documenti, dei dati e delle informazioni;
- e) la trasparenza, la completezza e la chiarezza dei documenti, dei dati e delle informazioni nonché il mantenimento della storicità dei medesimi.

Le Società del Gruppo adempiono agli obblighi predetti in relazione ai rapporti continuativi²⁸ e alle operazioni che rientrano nella rispettiva attività istituzionale²⁹, salvo che tali rapporti e operazioni siano inclusi nella lista delle esenzioni, descritta in seguito nel par. 9.2 (per la Capogruppo). L'acquisizione dei documenti, dei dati e delle informazioni nei sistemi automatizzati deve essere completata con tempestività e, in ogni caso, non oltre il trentesimo giorno dall'instaurazione del rapporto continuativo, dall'esecuzione dell'operazione, dalla variazione e dalla chiusura del rapporto continuativo.

9.1. Capogruppo - Messa a disposizione dei dati: il Nuovo Archivio Unico Informatico

Al fine di rendere disponibili alla Banca d'Italia e alla UIF dati e informazioni secondo gli standard definiti nelle Disposizioni per la Conservazione e la Messa a Disposizione dei Documenti, dei Dati e delle Informazioni per il Contrasto del Riciclaggio e del Finanziamento del Terrorismo ("Provvedimento di Banca d'Italia" del 24 marzo 2020), la Capogruppo utilizza archivi standardizzati conformi con gli standard di cui all'Allegato 2 del Provvedimento di Banca d'Italia. Tale scelta permette alla Capogruppo di continuare a mantenere l'Archivio Unico Informatico (AUI), le procedure di alimentazione e i presidi in essere, aggiornati, ove necessario, per assicurarne la conformità con i requisiti normativi del Provvedimento.

9.2 Capogruppo - Esenzioni

Ai sensi delle disposizioni normative sopracitate, la Capogruppo si avvale della facoltà di disapplicare le norme relative alla messa a disposizione dei dati e delle operazioni alle Autorità, in relazione ai rapporti continuativi o alle operazioni poste in essere con:

1. intermediari bancari e finanziari aventi sede in Italia o in altro stato membro;
2. istituti di moneta elettronica;
3. gli istituti di pagamento;
4. società di intermediazione;
5. società di gestione del risparmio;
6. società di investimento a capitale variabile;
7. società di investimento a capitale fisso, mobiliare e immobiliare;
8. altri intermediari iscritti nell'albo previsto dall'articolo 106 TUB;
9. Cassa depositi e prestiti;
10. imprese di assicurazione, che operano nei rami di cui all'articolo 2, comma 1, CAP;
11. soggetti eroganti micro-credito;
12. confidi e gli altri soggetti di cui all'articolo 112 TUB;
13. fondi comuni monetari e non monetari di paesi UE;
14. autorità bancarie centrali dei paesi UE, incluso Banca d'Italia;

¹⁹ Per la Capogruppo: rapporti di conto corrente, deposito titoli, mutui, prestiti personali, carte di credito, Fidejussione.

²⁰ L'attività per la quale la Banca ha ottenuto l'iscrizione ovvero l'autorizzazione da parte dell'autorità pubblica.

15. altre istituzioni finanziarie monetarie dei paesi UE.³⁰

9.3 Capogruppo - Le Comunicazioni Oggettive, le Segnalazioni Antiriciclaggio Aggregate (S.A.R.A.), flussi DEPRU e TRU

La Funzione Antiriciclaggio cura l'inoltro alla UIF delle Comunicazioni Oggettive, delle Segnalazioni SARA, dei flussi DEPRU e TRU ed ogni altro reporting tempo per tempo richiesto, secondo le disposizioni operative definite dalla UIF stessa, ai sensi della normativa tempo per tempo applicabile alla Capogruppo.

10 Segnalazione di operazioni sospette e segnalazione di violazioni

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.

10.1. Individuazione e segnalazione delle operazioni sospette

Le Società del Gruppo collaborano 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, le Società del Gruppo implementano 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);
- la tempestiva risposta alle richieste di informazioni che pervengono dalle Autorità e dagli Organi Investigativi.

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

- 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;
- contengono precise disposizioni in ordine alle modalità per assicurare tempestività e segretezza nel processo segnalativo, sia all'interno delle Società del Gruppo 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;

³⁰ Come definite dall'art. 1, comma 2, lettera h-bis e h-sexies del TUB e dall'art. 1, comma 1, lettera e), o), i), i-bis) del TUF.

- 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;
- prevedono l'obbligo di istituire appositi archivi nel quale devono essere conservate le evidenze relative alle segnalazioni, incluso le 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;
- garantiscono la riservatezza sull'identità del segnalante.

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

Le Società del Gruppo si avvalgono di metodologie e strumenti in grado di individuare eventuali comportamenti anomali, facendo anche riferimento ad indicatori di anomalia o red flags emanati tempo per tempo dalle Autorità di Vigilanza operanti nei paesi in cui hanno sedi le Società del Gruppo.

10.2. Segnalazione di violazioni

Le Società del Gruppo e la Capogruppo in particolare assicura che le procedure di segnalazione interna delle violazioni di cui all'art. 48 del D. Lgs. n. 231/2007 e successive modifiche (violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo) siano portate a conoscenza di tutto il personale. Questo compito è attribuito dalla normativa interna pertinente al Responsabile del sistema interno di segnalazione delle violazioni. Inoltre, è previsto che il responsabile della gestione del canale (il responsabile Compliance della Capogruppo) informi tempestivamente se del caso/a seconda dell'argomento trattato il responsabile della Funzione Antiriciclaggio della Società del Gruppo interessata³¹.

11. Obblighi di formazione

La Capogruppo, nell'ambito del piano formativo, cura in via continuativa, e per i neoassunti 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 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.

L'addestramento e la formazione assicurano una specifica preparazione del Personale a più diretto contatto con la clientela o comunque coinvolto nel processo di segnalazione di operazioni sospette nonché di quello addetto alla Funzione Antiriciclaggio. A questi membri del Personale è richiesto un continuo aggiornamento sull'evoluzione dei rischi di riciclaggio e sugli schemi tipici delle operazioni finanziarie criminali. Nel caso di ricorso a un fornitore esterno, il Responsabile della Funzione Antiriciclaggio locale accerta che i soggetti cui sia

³¹ Cfr. Global Policy Whistleblowing FB 026_2023.

affidato lo svolgimento dell'attività formativa possiedano le conoscenze in materia di antiriciclaggio richieste per garantire la qualità della formazione e che il contenuto di questa sia adeguato alle specificità della Società del Gruppo.

Le Società del Gruppo prevedono programmi di preparazione e formazione periodica tesi ad assicurare la sensibilizzazione e l'aggiornamento delle conseguenze del personale in merito al funzionamento delle soluzioni di onboarding a distanza del cliente, ai rischi associati e alle politiche e procedure di onboarding a distanza del cliente volte a mitigare tali rischi. La formazione include un test finalizzato a valutare che il Personale 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.

La Funzione AML della Capogruppo supervisiona il piano annuale di formazione del personale a livello di Gruppo.

12. 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.

13. 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 5.000 euro (si intende superata la soglia anche quando il trasferimento è effettuato con più pagamenti, inferiori alla soglia, che appaiono artificialmente frazionati);
- il trasferimento superiore al limite dei 5.000 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'imposta di bollo di 1,50 euro.
- È ammessa esclusivamente l'emissione di libretti di deposito, bancari o postali, nominativi;
- È 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.
- È 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.
- È 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.

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

La Capogruppo 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.

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 simili, 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.

14. Esternalizzazione

Lo svolgimento dei compiti attribuiti alla Funzione Antiriciclaggio può essere affidato a soggetti esterni nel rispetto del principio di proporzionalità. La responsabilità per la corretta gestione dei rischi di riciclaggio resta, in ogni caso, in capo alla Società del Gruppo, la quale è tenuta a presidiare i rischi derivanti dalle scelte effettuate e mantenere le competenze tecniche e gestionali necessarie per monitorare nel continuo le attività affidate a soggetti esterni. La decisione di ricorrere all'esternalizzazione non deve pregiudicare la qualità del sistema dei controlli.

Nelle situazioni in cui gli obblighi di adeguata verifica delle Società del Gruppo siano assolti da terzi ("Soggetti Delegati"), è necessario che:

- a) la Società del Gruppo abbia definito in un apposito accordo contrattuale i rispettivi diritti ed obblighi che devono essere assolti, le modalità e i tempi di assolvimento. In particolare: i livelli di servizio attesi, espressi in termini oggettivi e misurabili, nonché le informazioni necessarie per la verifica del loro rispetto; gli eventuali conflitti di interesse e le opportune cautele per prevenirli o, se non possibile, attenuarli; la durata dell'accordo e le modalità di rinnovo nonché gli impegni reciproci connessi con l'interruzione del rapporto;
- b) la frequenza minima dei flussi informativi nei confronti del responsabile interno e degli organi aziendali e delle funzioni di controllo, fermo restando l'obbligo di corrispondere tempestivamente a qualsiasi richiesta di informazioni e di consulenza;
- c) gli obblighi di riservatezza delle informazioni acquisite nell'esercizio della funzione;
- d) la possibilità di rivedere le condizioni del servizio al verificarsi di modifiche normative o nell'operatività e nell'organizzazione del destinatario;
- e) la possibilità di accedere alle informazioni utili e ai locali in cui opera il fornitore di servizi per l'attività di monitoraggio, supervisione e controllo
- f) la Società del Gruppo abbia ottenuto un'idonea attestazione da parte del Soggetto Delegato che lo stesso abbia provveduto ad adempiere agli obblighi di adeguata verifica in conformità alla normativa applicabile alla Società del Gruppo;
- g) l'attestazione di cui al punto precedente sia univocamente riconducibile al Soggetto Delegato e trasmessa alla Società del Gruppo che se ne avvale. Nella medesima attestazione è necessario che sia espressamente confermato il corretto adempimento degli obblighi da parte del Soggetto Delegato in relazione alle attività di verifica effettuate nonché la coincidenza tra il cliente verificato dal Soggetto Delegato e i clienti della Società del Gruppo cui l'attestazione si riferisce;
- h) il Soggetto Delegato metta a disposizione della Società del Gruppo le informazioni richieste in occasione dell'adempimento degli obblighi di identificazione e di raccolta delle informazioni di adeguata verifica;
- i) le copie dei documenti acquisiti dai Soggetti Delegati siano trasmesse senza ritardo alle Società del Gruppo che ne facciano richiesta.

In caso di esecuzione degli obblighi di adeguata verifica da parte di soggetti terzi, le Società del Gruppo, responsabili finali dell'adeguata verifica della clientela, valutano se gli elementi raccolti e le verifiche effettuate dai Soggetti Delegati siano idonei e sufficienti ai fini dell'assolvimento degli obblighi previsti dalla normativa antiriciclaggio e antiterrorismo applicabile e verificano, nei limiti della diligenza professionale, la veridicità dei documenti ricevuti. In caso di dubbi sull'identità del cliente, dell'esecutore e del titolare effettivo, le Società del Gruppo provvedono, in proprio a compierne l'identificazione e ad adempiere, in via diretta, agli obblighi di adeguata verifica.

È fatto divieto alle Società del Gruppo di avvalersi di Soggetti Delegati aventi sede in Paesi Terzi ad Alto Rischio.

15. 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 in quanto in quest'ultimo caso, 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, le società del Gruppo non devono instaurare rapporti con persone fisiche o giuridiche presenti nelle liste dell'UE, ONU OFAC ed in quelle dei paesi in cui le società del gruppo esercitano la loro attività. Questo divieto deve essere osservato anche in caso di operatività in paesi fuori della UE. UK e degli USA, poiché la mancata osservanza di tale divieto può comportare un rischio reputazionale e compromettere i rapporti d'affari del Gruppo

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 suesposte Liste, se previsto o richiesto dalla legge;
- 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.

16. 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.

Il Regolamento UE n. 847 del 20 maggio 2015³², 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.

16.1. 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:

- la carta, lo strumento o il dispositivo siano utilizzati esclusivamente per il pagamento di beni o servizi;
- 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.

16.2. 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

³² Si segnala il Regolamento (UE) 2023/1113 del Parlamento europeo e del Consiglio, del 31 maggio 2023, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività efficace dal 20 giugno 2023 e applicabile da dicembre 2024 che modifica la direttiva (UE) 2015/849 e le disposizioni sulle informazioni che accompagnano i trasferimenti dei fondi.

16.2.1. 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:

- d) il nome del beneficiario;
- e) 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.

16.2.2. 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.

16.2.3. 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.

16.2.4. 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.

16.2.5. 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.

17. Monitoraggio dei controlli

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

18. Sanzioni

L'inosservanza degli adempimenti previsti dalla normativa AML, espone il Gruppo a rischi sanzionatori e reputazionali. A tal riguardo si precisa che laddove una Società del Gruppo sia ritenuta responsabile, in via esclusiva o concorrente, di violazioni gravi, ripetute o sistematiche ovvero plurime delle disposizioni in materia di:

- obblighi di adeguata verifica della clientela e di astensione;
- obblighi di conservazione dei dati; e
- obblighi di segnalazione di operazioni sospette

ovvero in materia di organizzazione, procedure e controlli interni, nonché delle relative disposizioni attuative adottate dalle Autorità di vigilanza si applicheranno sanzioni amministrative come specificato dalla normativa locale applicabile alla Società del Gruppo (es. per la Capogruppo la sanzione amministrativa e pecuniaria da 30.000 euro a 5.000.000 di euro ovvero pari al dieci per cento del fatturato complessivo annuo, quando tale importo percentuale è superiore a 5.000.000 di euro e il fatturato è disponibile e determinabile).

Fermo quanto disposto dal precedente punto, le sanzioni amministrative si applicheranno anche nei confronti di soggetti che svolgono funzioni di amministrazione, direzione e controllo che, non assolvendo in tutto o in parte ai compiti direttamente o indirettamente correlati alla funzione o all'incarico, hanno agevolato, facilitato o comunque reso possibili le violazioni di cui al precedente punto, ovvero hanno inciso in modo rilevante sull'esposizione della Società del Gruppo al rischio di riciclaggio o di finanziamento del terrorismo.

L'impianto sanzionatorio su esposto, limitatamente alla Capogruppo e alle società del Gruppo operanti in Italia è completato dalle norme penali in tema di riciclaggio (art. 648-bis, 648-ter e 648-ter 1 del codice penale) che fanno rientrare nelle fattispecie di reato presupposto al riciclaggio qualsiasi delitto.