ROX PAY S.R.L.
POLITICA DI PREVENZIONE E CONTRASTO DEL RICICLAGGIO E DEL FINANZIAMENTO DEL TERRORISMO

1 - PANORAMICA

1.1 – PRINCIPALI NORMATIVE E ORIENTAMENTI

Il presente documento definisce la Policy di Rox Pay S.r.l. in materia di contrasto al riciclaggio, al finanziamento del terrorismo e alla violazione delle misure restrittive[1]e si applica a Rox Pay S.r.l. e le sue operazioni.

Le norme sono da considerarsi complementari ed applicabili in quanto non in conflitto con le disposizioni emanate dalle Autorità locali.

1.2 – DESTINATARI E MODALITÀ DI ATTUAZIONE

La Policy si applica a Rox Pay S.r.l.

2 – PRINCIPI GENERALI

2.1 QUADRO NORMATIVO AML-CFT

Il riciclaggio dei proventi di attività illecite e criminali costituisce una delle forme di criminalità più gravi sui mercati finanziari e costituisce un ambito di specifico interesse per le attività della criminalità organizzata.

Il riciclaggio di denaro ha un impatto negativo significativo sull'intera economia: il reinvestimento dei proventi illeciti in attività legali e la collusione tra individui o istituzioni finanziarie e organizzazioni criminali incidono profondamente sui meccanismi di mercato, minano l'efficienza e l'equità delle attività finanziarie e hanno un effetto indebolente sull'economia. Il finanziamento di attività terroristiche può comportare l'utilizzo di proventi derivanti dalla legge e/o da proventi derivanti dalla criminalità.

La mutevole natura del riciclaggio e del finanziamento del terrorismo, facilitata anche dalla continua evoluzione della tecnologia, richiede un costante adeguamento delle misure di prevenzione e contrasto.

Il quadro normativo antiriciclaggio (AML) e contrasto al finanziamento del terrorismo (CFT) si basa su un insieme completo di fonti normative nazionali, comunitarie e internazionali.

A livello internazionale, un contributo fondamentale all'armonizzazione normativa è venuto dal Financial Action Task Force (FATF), il principale organismo internazionale attivo nella lotta al riciclaggio di denaro, al finanziamento del terrorismo e alla proliferazione delle armi di distruzione di massa.

1 Come definito negli Orientamenti dell'ABE (EBA/GL/2024/14): "Le misure restrittive dell'Unione di cui all'articolo 2, punto (1) della Direttiva (UE) 2024/1226 e le misure restrittive nazionali adottate dagli Stati membri in conformità con il loro ordinamento giuridico nazionale (nella misura in cui si applicano agli istituti finanziari).

Nell'adempimento delle proprie responsabilità, il GAFI ha stabilito una serie di standard internazionali, le "40 raccomandazioni", a cui si sono aggiunte nel 2001 altre 9 raccomandazioni speciali per combattere il finanziamento del terrorismo internazionale. La materia è stata integralmente rivista nel febbraio 2012 con l'adozione degli Standard Internazionali sulla Lotta al Riciclaggio di Denaro e al Finanziamento del Terrorismo e della Proliferazione, poi riassunti nelle citate "40 Raccomandazioni".

Nell'ambito della lotta contro la proliferazione delle armi di distruzione di massa, le Nazioni Unite hanno preparato una serie di misure per contrastare il finanziamento dei programmi di proliferazione, compreso il divieto di assistere o finanziare qualsiasi persona coinvolta in tali attività.

L'Unione Europea, in attuazione delle Risoluzioni adottate nell'ambito delle Nazioni Unite, ha emanato una serie di disposizioni al fine di attuare misure restrittive quali il congelamento dei fondi e delle risorse economiche di persone o entità coinvolte nello sviluppo di attività sensibili alla proliferazione delle armi di distruzione di massa.

Il GAFI ha sviluppato linee guida per attuare le sanzioni finanziarie adottate dalle Nazioni Unite.

Misure specifiche per affrontare la proliferazione delle armi di distruzione di massa sono state recentemente incluse nelle Raccomandazioni, in conformità con le risoluzioni del Consiglio di Sicurezza delle Nazioni Unite.

Le linee guida UE sulla prevenzione dell'uso del sistema finanziario per il riciclaggio di denaro e il finanziamento del terrorismo sono contenute nella Direttiva UE 2015/849[2]del Parlamento Europeo e del Consiglio del 20 maggio 2015 (Quarta Direttiva Antiriciclaggio), come modificata dalla Direttiva UE 2018/843 (Quinta Direttiva Antiriciclaggio) nonché nei Regolamenti e nelle Linee Guida di volta in volta emanate rispettivamente dalla UE – Unione Europea e dall'EBA – Autorità Bancaria Europea.

A livello nazionale, la prevenzione e il contrasto al riciclaggio e al finanziamento del terrorismo è regolata dalle seguenti leggi primarie:

- **Il decreto legislativo italiano n. 109 del 22 giugno 2007 e successive modifiche e integrazioni recante "Disposizioni per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività di Paesi che minacciano la pace e la sicurezza internazionale", in attuazione della Direttiva 2015/849 come modificata dalla Direttiva UE 2018/843;**
- **Il decreto legislativo italiano n. 231 del 21 novembre 2007, e successive modifiche e integrazioni, in attuazione della Direttiva 2015/849/UE, che modifica le Direttive 2009/138/CE e 2013/36/UE, modificata dalla Direttiva 2018/843/UE sulla prevenzione dell'uso del sistema finanziario a fini di riciclaggio e di finanziamento del terrorismo (di seguito, anche Decreto).**

2 La Direttiva UE 2024/1640 del Parlamento Europeo e del Consiglio del 31/05/2024 sulle procedure che devono essere poste in essere dagli Stati membri per prevenire l'uso del sistema finanziario a fini di riciclaggio di denaro o di finanziamento del terrorismo, da recepire entro il 10 luglio 2027, modifica la Direttiva UE 2019/1937 e abroga la Direttiva UE 2015/849.

Esiste infine anche una normativa secondaria a livello nazionale emanata dalla Banca d'Italia e dell'Unità di Informazione Finanziaria ("UIF"), ed è contenuta nelle seguenti fonti normative:

- **Provvedimento del 26 marzo 2019 recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo di intermediari finanziari e di altri soggetti a fini di riciclaggio e di finanziamento del terrorismo, come modificato dal Provvedimento Banca d'Italia del 1° agosto 2023;**
- **Provvedimento del 28 marzo 2019 recante istruzioni in materia di comunicazioni oggettive;**
- **Provvedimento del 30 luglio 2019 recante disposizioni attuative in materia di adeguata verifica della clientela, come modificato dal Provvedimento di Banca d'Italia del 13 giugno 2023;**
- **Provvedimento del 24 marzo 2020 recante disposizioni attuative per la conservazione e la disponibilità di documenti, dati e informazioni in materia di antiriciclaggio e di finanziamento del terrorismo;**
- **Provvedimento del 25 agosto 2020 recante disposizioni per la presentazione di segnalazioni antiriciclaggio aggregate;**
- **Provvedimento del 12 maggio 2023 sugli indicatori di anomalia destinati agli intermediari per agevolare l'identificazione delle operazioni sospette, in vigore dal 1° gennaio 2024.**

RoxPay S.r.l. (di seguito "la Società") recepisce la normativa sopra richiamata nei propri documenti normativi interni.

A livello generale, la Società ha adottato la presente "Politica in materia di contrasto al riciclaggio e al finanziamento del terrorismo" (di seguito la "Politica") quale espressione del proprio impegno nel contrasto dei predetti fenomeni criminali su base internazionale, ponendo particolare attenzione al contrasto, nella consapevolezza che il perseguimento della redditività e dell'efficienza deve coniugarsi con il continuo ed efficace monitoraggio dell'integrità delle strutture aziendali.

La Politica applicata all'interno della Società descrive la politica adottata da Rox Pay S.r.l. in conformità alle regole e ai principi dettati dalle disposizioni normative nazionali e comunitarie, nel rispetto degli standard internazionali in materia ed è attuato congiuntamente alle procedure interne in materia di Antiriciclaggio e Antiterrorismo, al Codice Etico e alle procedure interne che danno attuazione alla normativa locale primaria e secondaria vigente specificando processi, ruoli e responsabilità.

La presente Politica è stata approvata dal Consiglio di Amministrazione della Società.

Le linee guida AML e CFT sono applicate da Rox Pay S.r.l. in coerenza con le leggi vigenti.

La Società si impegna a rispettare tale quadro normativo nonché le eventuali disposizioni attuative emanate dalla Banca d'Italia in materia di adeguata verifica della clientela, conservazione dei dati e delle informazioni, organizzazione, procedure, controlli e controlli rafforzati contro il finanziamento di programmi finalizzati alla proliferazione di armi di distruzione di massa.

La Società è fortemente impegnata a garantire che l'organizzazione operativa ed il sistema di controllo siano completi, adeguati, funzionali ed affidabili per la supervisione strategica, a tutelare la Società da tolleranze o commistioni di forme di illegalità che possano danneggiarne la reputazione e pregiudicarne la stabilità.

Per questi motivi Rox Pay S.r.l. ha adottato regole organizzative e comportamentali e sistemi di monitoraggio e controllo volti a garantire il rispetto della normativa vigente da parte degli organi amministrativi e di controllo, del personale, dei collaboratori e dei consulenti della Società. Tali controlli sono coerenti anche con le regole e le procedure previste dal Codice in materia di protezione dei dati personali.

La Società si avvale inoltre di indicatori di anomalie e modelli di comportamenti irregolari nell'ambiente economico e finanziario, emessi nel tempo dall'Unità di Informazione Finanziaria (UIF) in merito a potenziali attività di riciclaggio e di finanziamento del terrorismo.

2.2 - IL QUADRO NORMATIVO IN MATERIA DI MISURE RESTRITTIVE ED EMBARGO

Tutte le misure restrittive poste per contrastare il finanziamento del terrorismo e tutte le attività illecite o sospette che minacciano la pace e la sicurezza internazionale possono essere sia commerciali, come restrizioni all'importazione/esportazione da/verso un Paese, sia finanziarie, come il blocco parziale o totale dei trasferimenti di fondi ma anche limitazioni operative e il congelamento dei fondi.

Tra le misure restrittive rientrano le sanzioni finanziarie internazionali, denominate anche embarghi, attuate dallo Stato italiano, da enti esteri (es. OFAC, UKSL) e da organizzazioni sovranazionali (ONU, UE) attraverso una serie di obblighi a cui la Società è tenuta a conformarsi. Il Consiglio impone a tutti gli Stati membri dell'ONU alcune misure restrittive (sanzioni) per attuare le risoluzioni adottate dal Consiglio di sicurezza dell'ONU ai sensi del capitolo VII della Carta delle Nazioni Unite. Inoltre, le sanzioni possono essere adottate, o decise autonomamente, dall'Unione Europea attraverso regolamenti del Consiglio, immediatamente esecutivi in ciascuno Stato membro per garantirne la tempestiva e simultanea applicazione.

A livello internazionale, esistono normative che stabiliscono specifici divieti o restrizioni agli investimenti in determinati settori industriali o all'importazione/esportazione da/verso "Paesi ad alto o significativo rischio". Si tratta, in particolare, delle risoluzioni del Consiglio di Sicurezza dell'ONU (SC) ai sensi dell'articolo 41 del Capitolo VII della Carta delle Nazioni Unite, attraverso le quali vengono imposte misure restrittive nei confronti di persone e/o Paesi.

Per quanto riguarda la normativa comunitaria, le principali disposizioni sono:

- il Regolamento 2021/821 del Parlamento Europeo e del Consiglio del 20 maggio 2021[3] **e successive modifiche, con le quali viene istituito un regime comunitario per il controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito di beni a duplice uso;**

3 che ha sostituito il Regolamento 428/2009/CE del Consiglio del 5 maggio 2009

- il Regolamento (UE) 2023/1113 del Parlamento Europeo e del Consiglio del 31 maggio 2023 relativo alle informazioni che accompagnano i trasferimenti di fondi e determinate cripto-attività e che modifica la Direttiva (UE) 2015/849 (rifusione);
- il Regolamento (UE) 2024/886 del Parlamento Europeo e del Consiglio del 13 marzo 2024 che modifica i Regolamenti (UE) n. 260/2012 e (UE) 2021/1230 e le Direttive 98/26/CE e (UE) 2015/2366 per quanto riguarda i bonifici istantanei in euro;
- la Direttiva (UE) 2024/1226 del Parlamento Europeo e del Consiglio del 24 aprile 2024 sulla definizione dei reati e delle sanzioni per la violazione delle misure restrittive dell'Unione e che modifica la direttiva (UE) 2018/1673 recepita nell'ordinamento italiano dal decreto legislativo 211/2025.
- **Orientamenti dell'Autorità bancaria europea su politiche, procedure e controlli interni per garantire l'attuazione di misure restrittive nazionali e dell'Unione (EBA/GL/2024/14)**[4];
- **Orientamenti dell'Autorità bancaria europea su politiche, procedure e controlli interni per garantire l'attuazione di misure restrittive nazionali e dell'Unione, in conformità al regolamento (UE) 2023/1113 (EBA/GL/2024/15) sulle informazioni che accompagnano i trasferimenti di fondi e determinate cripto-attività e che modifica la direttiva (UE) 2015/849**[5].

Infine, a livello nazionale, gli embarghi sono regolati come segue:

- **Legislazione primaria:**
  - **Il Decreto Legislativo n. 221/2017, che ha modificato e semplificato le procedure di autorizzazione all'esportazione di beni e tecnologie a duplice uso e le sanzioni sugli embarghi commerciali nonché su ogni tipologia di operazione di esportazione di materiali proliferanti.**
- **Legislazione secondaria:**
  - **Provvedimento Banca d'Italia del 12 maggio 2023 recante indicatori di anomalia per gli intermediari al fine di agevolare l'identificazione delle operazioni sospette.**

Infine, tutte le norme emanate dalle Autorità statunitensi hanno rilevanza per l'attività della Società in considerazione degli aspetti reputazionali e del riferimento a tali norme negli impegni contrattuali che comportano la potenziale applicazione di sanzioni con effetto extraterritoriale (cd "secondary sanctions" statunitensi). Tali disposizioni normative sono contenute nello USA Patriot Act6 e nei provvedimenti relativi alle sanzioni economiche e commerciali emanati dal Governo statunitense attraverso l'Office of Foreign Assets Control (OFAC) del Dipartimento del Tesoro.[6]

4 al quale Banca d'Italia ha dichiarato di volersi conformare con la Nota n. 48 dell'8 aprile 2025 e applicabile dal 30 dicembre 2025.

5 al quale Banca d'Italia ha dichiarato di voler conformarsi con la Nota n. 52 del 19 maggio 2025 e applicabile dal 30 dicembre 2025.

6 Legge federale statunitense del 26 ottobre 2001, intitolata ufficialmente "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001".

3 – MODELLI E METODOLOGIE DI GRUPPO

3.1 – ASPETTI GENERALI

Il consolidato quadro normativo nazionale in materia di azione preventiva contro il riciclaggio, il finanziamento del terrorismo e le violazioni delle Misure Restrittive si fonda su una serie di obblighi

che i destinatari sono tenuti a rispettare:

- obbligo di adottare strutture organizzative, procedure e misure di controllo interno adeguate;
- obbligo di adottare procedure coerenti e coerenti per l'analisi e la valutazione dei rischi legati al riciclaggio di denaro, al finanziamento del terrorismo e alla violazione delle Misure restrittive nonché di stabilire la supervisione, i controlli e le procedure necessarie per mitigare e gestire tali rischi;
- obbligo di adeguata verifica della clientela, attraverso il quale la Società acquisisce e verifica informazioni riguardanti l'identità del cliente e dell'eventuale titolare effettivo, nonché lo scopo e la natura prevista del rapporto o dell'operazione, garantendo nel contempo il costante monitoraggio di tutte le operazioni effettuate dal cliente;
- un approccio basato sul rischio, in base al quale gli obblighi di adeguata verifica della clientela sono suddivisi in diversi gradi di due diligence commisurati al profilo di rischio del cliente;
- obbligo di conservare documenti, dati e informazioni in modo da consentirne la tempestiva acquisizione, la trasparenza, la completezza, l'inalterabilità e l'integrità, nonché una complessiva e tempestiva accessibilità;
- obbligo di segnalazione delle operazioni sospette;
- obbligo di astenersi dall'instaurare nuovi rapporti con i clienti, dall'effettuare transazioni occasionali o dal mantenere un rapporto con i clienti esistenti laddove non sia stata condotta la dovuta diligenza o si sospetti che possa esserci un collegamento con il riciclaggio di denaro o il finanziamento del terrorismo;
- obbligo di denuncia al Ministero dell'Economia e delle Finanze delle violazioni di cui agli articoli 49 e 50 del D.Lgs. 231/07, nonché di rispetto delle limitazioni all'utilizzo del contante e dei titoli al portatore;
- monitorare tutte le transazioni con persone fisiche e giuridiche e/o con Paesi inclusi nelle European Union Council Lists (UE), nell'Office of Foreign Assets Control List (OFAC), nella UK Sanctions List (UKSL)[7], nella Consolidated Sanctions List (ONU) del Consiglio di Sicurezza delle Nazioni Unite, nei Provvedimenti emanati dalle Autorità Nazionali contenenti specifiche misure restrittive per il contrasto al terrorismo;
- monitorare le operazioni effettuate con paesi considerati non cooperativi in materia di vigilanza fiscale, finanziaria e antiriciclaggio, generalmente denominati "paradisi fiscali" o "centri finanziari offshore";
- adottare adeguati programmi di formazione del personale per garantire l'attuazione e la corretta applicazione di leggi e regolamenti;
- obbligo di fornire all'UIF "comunicazioni oggettive" secondo le specifiche istruzioni relative alle modalità e alla frequenza delle comunicazioni;

7 La lista OFSI (Office of Financial Sanctions Implementation HMT) è stata chiusa il 28 gennaio 2026; da tale data, la UK Sancti ons List è l'unica fonte ufficiale per tutte le designazioni delle sanzioni del Regno Unito.

- obbligo di comunicazione di eventuali violazioni o violazioni di cui venga a conoscenza da parte degli Organi di Controllo nello svolgimento dei propri compiti;
- obbligo di adottare procedure per la gestione delle segnalazioni interne di violazioni presentate dai dipendenti (Whistleblowing).

Per quanto riguarda l'attività di contrasto al finanziamento del terrorismo, la normativa italiana impone ai soggetti obbligati di:

- congelamento dei fondi e delle risorse economiche di alcune persone incluse nelle liste UE;
- informare l'Unità di Informazione Finanziaria (UIF) delle misure applicate per il congelamento dei fondi, ovvero il Nucleo Speciale di Polizia Valutaria della Guardia di Finanza in caso di risorse economiche;
- informare la UIF di operazioni, rapporti d'affari sospetti e di ogni altra informazione disponibile riguardante soggetti inseriti nelle liste nere pubblicate dalla UIF stessa;
- segnalare operazioni sospette che, sulla base delle informazioni disponibili, siano direttamente o indirettamente collegate ad attività di finanziamento del terrorismo.

Per quanto riguarda le sanzioni internazionali (i cosiddetti Embarghi) e l'esposizione a misure restrittive, la legislazione richiede l'adozione di alcune misure, tra cui ma non limitate a:

- dati personali e controlli transazionali sulle operazioni connesse alle importazioni e/o esportazioni effettuate dai clienti, volti a bloccare le importazioni/esportazioni da o verso un Paese, e relative normative. Il divieto può essere generale, interessando tutte le tipologie di merci salvo specifica autorizzazione, oppure limitato a determinate tipologie di merci, ad es. armamenti (fare riferimento al codice doganale);
- restrizioni totali o parziali sui trasferimenti finanziari da/verso un Paese;
- obbligo di autorizzazione preventiva per effettuare trasferimenti;
- obbligo di comunicazione dei trasferimenti (in uscita o in entrata);
- divieto di finanziare, fornire assistenza finanziaria o mettere a disposizione del Governo prestiti agevolati (direttamente o in alcuni casi indirettamente tramite società affiliate o partecipazione a istituzioni finanziarie internazionali);
- divieto di finanziare clienti che operano con paesi sanzionati;
- attuazione di misure restrittive nei confronti di soggetti russi e bielorussi;
- la tracciabilità dei controlli effettuati su operazioni provenienti da o dirette verso paesi, persone ed entità soggette a restrizioni.

3.2 - ADEGUATA VERIFICA DELLA CLIENTELA

3.2.1 – Aspetti generali

La Società adotta tutte le misure di adeguata verifica della clientela quando:

- instaurazione di rapporti commerciali;
- eseguire operazioni occasionali, disposte dalla clientela, quali bonifici o altre operazioni pari o superiori alla soglia designata applicabile, indipendentemente dal fatto che l'operazione sia effettuata in un'unica operazione o in più operazioni collegate o che consista in un trasferimento di fondi, eccedente i limiti di legge;

- vi è il sospetto di riciclaggio di denaro o finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia designata che possa applicarsi;
- sussistano dubbi sulla completezza, affidabilità e veridicità delle informazioni o della documentazione precedentemente acquisita ai fini dell'identificazione di un Cliente.

Obblighi di dovuta diligenza:

- sono soddisfatte:
  - nei confronti di nuovi clienti prima dell'instaurazione di un rapporto continuativo o del compimento di un'operazione occasionale;
  - nei confronti dei clienti esistenti, ogniqualvolta la due diligence sia opportuna alla luce di un cambiamento nel livello di rischio di riciclaggio o di finanziamento del terrorismo associato al cliente o laddove vi siano sospetti o dubbi circa l'accuratezza o l'adeguatezza delle informazioni precedentemente ottenute dal cliente;

- e consistono nelle seguenti attività:
  - identificare il Cliente, il titolare effettivo e l'esecutore testamentario e verificarne l'identità sulla base di documenti, dati o informazioni ottenuti da fonte attendibile e indipendente;
  - ottenere e valutare informazioni sullo scopo e sulla natura prevista del rapporto commerciale;
  - effettuare un monitoraggio continuo durante tutta la durata del rapporto con il cliente.

A tal fine, la Società - attraverso i propri dipendenti e/o tramite agenti/consulenti finanziari abilitati all'offerta fuori sede e che entrano in contatto diretto con il Cliente - ottiene le informazioni richieste dalla normativa e raccoglie ogni altra documentazione rilevante come specificato nella presente Politica e nei documenti procedurali della Società.

La Società applica misure di adeguata verifica della clientela ordinarie, semplificate o rafforzate secondo l'approccio basato sul rischio applicato ai clienti.

3.2.2 - Onboarding remoto del cliente

Nei casi in cui la Società utilizzi modalità di identificazione a distanza consentite dal D.Lgs. n. 231/07, articolo 19, comma 1, lettera a), commi 2 e 5, adotta particolari procedure per l'adempimento degli obblighi di adeguata verifica, anche in considerazione del rischio di frode connesso al furto di identità. In questo caso l'identificazione si basa sull'acquisizione del certificato di firma elettronica qualificata, che viene generato a seguito di un processo di identificazione effettuato attraverso:

- l'utilizzo del Sistema Pubblico di Identità Digitale (SPID) o della Carta d'Identità Elettronica;
- mediante tecniche e procedure di identificazione elettronica sicure e regolamentate, autorizzate o riconosciute dall'Agenzia per l'Italia Digitale.

In tutti i casi, il processo di identificazione a distanza prevede la raccolta dei dati identificativi del cliente e dell'eventuale esecutore in formato elettronico, nonché l'effettuazione di verifiche e controlli sull'autenticità dei dati, oltre a quelli previsti per l'identificazione di persona,

secondo un approccio basato sul rischio, anche tramite contatto telefonico su numero certificato (welcome call) o bonifico effettuato dal cliente tramite un intermediario bancario e finanziario con sede in Italia.

Al fine di limitare l'esposizione a potenziali rischi di riciclaggio e/o frode, non è consentito instaurare rapporti bancari a distanza con persone giuridiche o persone fisiche che agiscono per conto di una persona giuridica, a meno che non siano state identificate di persona (faccia a faccia).

Non è consentita l'instaurazione di rapporti bancari a distanza con clientela non residente in Italia.

3.2.3 – Valutazione Pre-Implementazione e monitoraggio nel continuo dei processi di apertura di rapporti a distanza.

I processi di identificazione e onboarding del cliente da remoto sono formalizzati e dettagliati nella normativa interna. Il modello per presidiare tali processi prevede:

I. la valutazione preliminare della soluzione di onboarding da remoto (c.d. Pre-Implementation Assessment[8]) mirato a:
   (i) valutare l'adeguatezza della soluzione in termini di completezza e accuratezza dei dati e dei documenti da raccogliere, nonché l'affidabilità e l'indipendenza delle fonti informative utilizzate;
   (ii) valutare l'impatto dell'utilizzo della soluzione sui rischi aziendali inclusi i rischi operativi, reputazionali e legali attraverso il coinvolgimento delle competenti funzioni tecniche e specialistiche;
   (iii) identificare misure di mitigazione e azioni correttive per ciascun rischio individuato;
   (iv) definire test ex ante per valutare i rischi ICT e frode e test end-to-and sul funzionamento della soluzione.

II. monitoraggio continuo della soluzione di onboarding adottata attraverso controlli periodici ed event-driven per garantirne il corretto funzionamento nel tempo (cd. Ongoing Monitoring).

III. la revisione della valutazione preliminare nella soluzione di remote onboarding (c.d. Pre-Implementation Assessment) quando si verificano cambiamenti strutturali nella soluzione adottata o si verificano determinati eventi quali:
   (i) cambiamenti nell'esposizione ai rischi in materia di antiriciclaggio e contrasto al finanziamento del terrorismo, nonché degli embarghi;
   ii) carenze rilevate affinché la nostra soluzione funzioni;
   iii) un aumento dei tentativi di frode;
   (iv) modifiche normative.

3.2.4 – Obblighi di due diligence semplificati

In generale, la Società utilizza un approccio basato sul rischio per identificare le tipologie di clienti a cui possono essere applicate misure semplificate di due diligence. Rientrano in tale ambito i casi in cui siano presenti "indicatori di basso rischio", come indicati nell'Allegato 1 del Provvedimento della Banca d'Italia in materia di adeguata verifica della clientela del 30 luglio 2019 (di seguito "Il Provvedimento").

8 Nota n. 32 del 13 giugno 2023 con la quale Banca d'Italia ha dichiarato l'intenzione di conformarsi agli Orientamenti EBA (EBA/GL/2022/15) sull'utilizzo di soluzioni di onboarding remoto della clientela.

Gli "indicatori di basso rischio" rilevanti ai fini dell'applicazione di una procedura di due diligence semplificata si basano sulla tipologia del cliente, esecutore o titolare effettivo, sull'area geografica di residenza o in cui è stabilita la sede centrale, sullo specifico prodotto, servizio o canale distributivo.

Nel dettaglio, tra le tipologie di clientela considerate a basso rischio di riciclaggio, a cui può applicarsi l'adeguata verifica semplificata, rientrano:

- Pubbliche Amministrazioni, Istituzioni o Enti che svolgono funzioni pubbliche, ai sensi del diritto dell'Unione Europea;
- Società quotate su un mercato regolamentato e soggette a obblighi di informativa, inclusa la garanzia di un'adeguata trasparenza sulla titolarità effettiva finale;
- gli enti creditizi e finanziari della Comunità Europea elencati nell'articolo 3, comma 2, del decreto antiriciclaggio – esclusi quelli di cui alle lettere i), o), s), v)[9]— e gli enti creditizi e finanziari residenti in Stati membri o paesi terzi dotati di efficaci sistemi di riciclaggio e di finanziamento del terrorismo;
- Clienti, esecutori o titolari effettivi residenti o stabiliti in aree geografiche a basso rischio di riciclaggio.

La Società non applica misure semplificate di adeguata verifica della clientela quando:

- emergano dubbi, incertezze o incongruenze circa i dati identificativi e le informazioni raccolte in sede di identificazione del cliente, esecutore o titolare effettivo;
- non sussistono più le condizioni per un'adeguata verifica semplificata della clientela sulla base degli indicatori di rischio previsti dal decreto antiriciclaggio e dalla normativa secondaria in materia;
- il monitoraggio dell'operatività complessiva effettuata dal cliente e le informazioni raccolte nel corso del rapporto escludono una tipologia di rischio basso;
- sussiste ancora il sospetto di riciclaggio di denaro o di finanziamento del terrorismo.

La Funzione Antiriciclaggio ha competenza esclusiva in merito alla valutazione e autorizzazione delle misure semplificate di adeguata verifica della clientela, effettuate seguendo tutti gli adempimenti previsti dall'ordinario processo di adeguata verifica della clientela - compreso l'obbligo di identificare e verificare l'identità del cliente, dell'esecutore e dell'intestatario effettivo, nonché di acquisire tutti i dati e i documenti necessari alla loro completa registrazione (es. denominazione, forma giuridica, sede legale e, ove applicabile, codice fiscale) - pur riducendone il livello di approfondimento, portata e frequenza.

3.2.5 – Obblighi di due diligence rafforzati

La Società applica misure rafforzate di adeguata verifica della clientela in presenza di clienti o di situazioni a maggior rischio di riciclaggio o di finanziamento del terrorismo e in tutti i casi di cui all'articolo 24 del Decreto. Tali misure rafforzate prevedono, tra l'altro, il coinvolgimento di ruoli di responsabilità commisurati al livello di rischio individuato nei confronti del cliente.

9 i) gli agenti di cambio di cui all'articolo 201 del TUF; o) intermediari assicurativi di cui all'articolo 109, comma 2, lettere a), b) ed), del CAP, operanti nei rami di attività di cui all'articolo 2, comma 1, del CAP; s) le società fiduciarie iscritte nell'albo istituito ai sensi dell'articolo 106 del TUB; v) consulenti finanziari di cui all'articolo 18-bis del TUF e società di consulenza finanziaria di cui all'articolo 18-ter del TUF.

Per quanto riguarda i clienti private banking, la Società valuta i fattori di rischio specifici inerenti alla natura della loro attività e applica misure rafforzate di due diligence sulla base delle informazioni complessive disponibili e delle valutazioni effettuate.

Il coinvolgimento della Funzione Antiriciclaggio è richiesto nei seguenti casi:

- le persone fisiche e giuridiche inserite negli elenchi delle persone o degli enti sottoposti a provvedimenti di congelamento ai sensi di regolamenti o decreti europei ai sensi del D.Lgs. 109/07, nonché le persone ad esse strettamente legate;
- un rapporto di corrispondenza transfrontaliero instaurato con una banca o un istituto situato in un Paese terzo, sulla base di fattori geografici ad alto rischio (come riportato nell'Allegato 2 delle disposizioni della Banca d'Italia in materia di adeguata verifica della clientela);
- rapporti o transazioni in cui il cliente o il titolare effettivo finale è una persona politicamente esposta[10];
- situazioni che comportano elementi di rischio che richiedono l'applicazione di specifiche misure di riservatezza;
- situazione con un rischio più elevato di riciclaggio di denaro o finanziamento del terrorismo a causa di contingenze oggettive, ambientali o soggettive;
- clientela classificata "Trust", servizi di Money Transfer e Cambi Valuta Virtuale;
- Società fiduciarie, salvo quanto previsto al paragrafo 3.4;

Inoltre, prima di iniziare, proseguire o mantenere un rapporto continuativo con Persone Politicamente Esposte o Enti Corrispondenti di Paesi terzi, è necessario acquisire l'apposita autorizzazione da parte del Direttore Generale o del suo delegato, previo parere della Funzione Antiriciclaggio. Nel caso dei delegati ex art. 25 del D.Lgs. 231/07 appartenenti alla Funzione Antiriciclaggio, tale autorizzazione è inserita nel processo di adeguata verifica rafforzata.

In tutti gli altri casi, l'applicazione delle misure rafforzate è commisurata al livello di rischio attribuito al cliente. Se il rischio è considerato medio/alto, o se sono presenti alcuni fattori di rischio indipendentemente dal punteggio assegnato, è richiesto il coinvolgimento del Responsabile della business unit responsabile della gestione commerciale del cliente.

Esempi di tali casi sono:

- clienti persone giuridiche con un esecutore identificato come PEP o PEP indiretto, indipendentemente dal profilo di rischio;
- servizi offerti attraverso reti di agenti finanziari, consulenti finanziari, appaltatori e agenti;
- clienti classificati come Fondazioni/Enti no profit;
- clienti persone giuridiche in fase di onboarding;
- clienti con notizie negative in fase di onboarding ("Notizie avverse");

10 Persone Politicamente Esposte (PEP): come elencate dall'art. 1, comma 2, lettera dd) D.Lgs 231/07.

- clienti residenti o con sede in Paesi terzi ad alto rischio ovvero in caso di rapporti continuativi, prestazioni professionali ed operazioni che coinvolgono Paesi ad alto rischio;
- le società che hanno emesso azioni al portatore o che hanno una società che emette azioni al portatore nella loro struttura di catena di controllo;
- rapporti o operazioni in cui il cliente e il titolare effettivo ricoprono una carica pubblica diversi da quelli elencati per le persone politicamente esposte[11];
- società partecipate da Trust, Società fiduciarie, Fondazioni, società di capitali attraverso più livelli di partecipazione o partecipazioni incrociate;
- clienti impegnati in una tipologia di attività economica particolarmente esposta al rischio di riciclaggio o in settori di attività "controversi"[12] ovvero attività commerciali ad alta intensità di contante, quali cash-for-gold, cambio valuta, gioco d'azzardo/scommesse anche on-line, industria degli armamenti, estrazione mineraria, raccolta e smaltimento rifiuti, produzione di energia rinnovabile, aziende operanti nel settore dei cripto-asset, edilizia, approvvigionamento di strumenti farmaceutici;
- clienti che partecipano ad appalti pubblici o ricevono finanziamenti pubblici (sanità, edilizia, raccolta e smaltimento rifiuti, produzione di energia rinnovabile, estrazione mineraria, fornitura di strumenti farmaceutici);
- nei casi di clienti che hanno acquisito la cittadinanza di uno Stato membro o hanno ottenuto il diritto di soggiorno in uno Stato membro (UE) attraverso un programma di cittadinanza per investimento o un programma di residenza per investimento;
- nei casi di persone giuridiche clienti residenti in un Paese dell'Unione Europea, dove i diritti di proprietà della società sono detenuti - direttamente o indirettamente - per più del 40% da una persona giuridica, organizzazione o organismo con sede in Russia, o da una persona fisica con residenza o cittadinanza russa.

Il coinvolgimento del Responsabile della business unit preposta alla gestione commerciale del cliente è richiesto anche nel caso in cui si verifichino eventuali errori informatici che possano impedire il calcolo in tempo reale del rischio di riciclaggio del cliente.

Le misure rafforzate di adeguata verifica comprendono l'acquisizione di informazioni aggiuntive sul cliente, sull'esecutore e sul titolare effettivo, l'approfondimento dello scopo e della natura del rapporto e l'incremento della frequenza delle procedure volte a garantire un monitoraggio continuo nel corso del rapporto in corso.

Nel pieno rispetto della normativa vigente e di quanto previsto dalle procedure interne in materia di Antiriciclaggio e Finanziamento del terrorismo ed in linea con il Codice Etico della Società, la Società non supporta operazioni con clienti operanti in settori controversi che (i) non sono conformi alla normativa nazionale vigente e (ii) non sono, ove applicabile, preventivamente autorizzati dalle competenti autorità nazionali italiane, in particolare:

- la produzione, il transito e/o la commercializzazione di materiali di armamento;
- produzione e vendita di marijuana light, locali di intrattenimento per adulti;

11 Incarichi pubblici diversi da quelli ricoperti dalle Persone Politicamente Esposte (PEP) di cui alla nota 1), applicabile a tutti i soggetti che ricoprono incarichi negli enti pubblici, nei consorzi, nelle associazioni a carattere pubblico di cui alla sezione A 8) dell'Allegato 2 del Provvedimento.
12 un settore economico è "controverso" se i beni/servizi fabbricati/offerti e/o le modalità con cui sono prodotti/offerti sono in contrasto con i valori ampiamente condivisi di etica e sostenibilità, anche quando servizi o attività sono leciti e quindi non in contrasto con obblighi di legge.

- attività commerciali ad alta intensità di contante diverse da quelle sopra elencate, come enti di beneficenza e ONG non regolamentate, produzione di metalli e pietre preziose, rimesse di denaro.

Inoltre, la Società presta particolare attenzione al rispetto delle misure restrittive poste in essere dallo Stato italiano, da enti esteri (es. OFAC, UKSL) e/o da organismi sovranazionali (ONU, UE). Tali misure possono essere di natura commerciale (es. blocco delle importazioni/esportazioni) o di natura finanziaria, come il blocco parziale/totale dei trasferimenti di denaro da o verso uno specifico Paese o limitazioni alle operazioni e/o congelamento dei fondi detenuti presso intermediari finanziari.

Al fine di ottemperare agli obblighi previsti dal D.Lgs. 109/07 - volti a prevenire e contrastare il finanziamento del terrorismo e alle attività di Paesi che minacciano la pace e la sicurezza internazionale, mediante l'applicazione di misure restrittive di "congelamento" di fondi e risorse economiche detenuti da persone fisiche e giuridiche, gruppi ed enti appositamente individuati dalle Nazioni Unite e dall'Unione Europea ("soggetti designati") - e agli obblighi di rafforzata adeguata verifica previsti dal D.Lgs. 231/07, la Società ha adottato procedure automatiche di controllo. Tali procedure sono in grado di verificare la coerenza tra i dati identificativi del cliente ottenuti attraverso il processo di due diligence e quelli contenuti negli elenchi prodotti dalla UE e da altre istituzioni e organismi internazionali, quali:

- le persone investite di una carica pubblica di rilievo o che abbiano cessato dalla carica da meno di un anno (PEP), i loro familiari e coloro che con essi hanno stretti legami secondo la definizione dell'art. 1 c. 2 lettera dd del D.Lgs. 231/07 (PEP residenti e non residenti);
- soggetti residenti in Italia che ricoprono cariche pubbliche, che non rientrano nella definizione di PEP, ma sono comunque esposti ad un significativo rischio di corruzione e riciclaggio;
- le persone fisiche e giuridiche operanti, anche parzialmente, in Stati che non impongono misure e regolamenti equivalenti, secondo gli indirizzi della Banca d'Italia o di altre istituzioni nazionali o sovranazionali preposte alla prevenzione dei reati;
- persone fisiche e giuridiche soggette a misure di embargo o congelamento di fondi/risorse economiche e beni finanziari (Sanction Lists UN, EU, UKSL, OFAC).

3.3 - PROFILAZIONE CLIENTE

La Società adotta idonee procedure volte a definire il profilo di rischio di riciclaggio e di finanziamento del terrorismo (RP) attribuibile a ciascun cliente, sulla base delle informazioni acquisite e delle analisi effettuate, con riferimento sia agli elementi di valutazione indicati nel Provvedimento, sia ad ulteriori elementi che potranno essere adottati nel tempo dalla Società stessa (c.d. profilazione).

Sulla base della profilazione della clientela, effettuata anche con cadenza periodica, la Società applica misure standard o rafforzate, che prevedono il coinvolgimento di ruoli di responsabilità commisurati al livello di rischio individuato dal cliente. È richiesto il parere preventivo della Funzione Antiriciclaggio secondo le competenze previste nel documento interno "Procedure interne antiriciclaggio e contrasto al finanziamento del terrorismo".

La classificazione della clientela per l'adeguata verifica semplificata è autorizzata dalla Funzione

Antiriciclaggio, su richiesta del Responsabile della Business Unit Operativa.

In tal caso l'ambito e la frequenza degli adempimenti vengono ridotti, con una scadenza della verifica dopo 8 anni indipendentemente dal punteggio di rischio, a meno che non siano più soddisfatte le condizioni per l'applicazione della due diligence semplificata.

Inoltre, la Società si è dotata di una procedura informatica per valutare il profilo di rischio del cliente e per definire in modo coerente un orizzonte temporale di rivalutazione adeguato al livello di rischio calcolato; la frequenza di rivalutazione dipende dal processo individuato nell'ultima valutazione effettuata o, in assenza di un questionario KYC, dal profilo di rischio del cliente, come di seguito specificato:

Classe di rischio (RP)	Punteggio	Processo di due diligence	Ruolo di convalida	Frequenza di rivalutazione
Clienti classificati come soggetti a due diligence semplificata	NA	Semplificato	Accettazione automatica/Responsabile Business Unit (*)	8 anni
Immateriale	<=5	Norma	Accettazione automatica	8 anni
Basso	>=6 e <=12			6 anni
Medio	>=13 e <=24	Migliorato	Responsabile Unità Aziendale (**)	2 anni
Alto	>=25			1 anno
In caso di elementi di rischio specifici (***)		Migliorato	Funzione di convalida AML	1 anno

(*) fornito qualora il punteggio di rischio calcolato o risultante dal KYC effettuato sia almeno medio. (**) forniti anche in presenza di elementi di rischio definiti che mantengono il profilo di rischio inferiore alla media.
(***) forniti anche in presenza di Persone Giuridiche con RP >39, se svolgono attività commerciali relative all'acquisto di oro, giochi e scommesse e raccolta e smaltimento rifiuti (codici ATECO ad alto rischio) e/o se sono sottoposti a controlli/indagini.

3.4 - STRUMENTI A SUPPORTO DELLA DUE DILIGENCE

La Società ha implementato strumenti tecnologicamente avanzati a supporto dei processi antiriciclaggio, accanto alle tradizionali applicazioni già in uso:

- Robotic Process Automation (RPA) applicata alle attività di raccolta dati negli ambiti di adeguata verifica della clientela e segnalazione di operazioni sospette;
- Motore di Intelligenza Artificiale, basato su componenti statistiche e indicatori predittivi (Predict Index AML, Reputational Index e Criminal Infiltration Index) costruito con tecniche di Data Analytics, applicato al regolare processo di revisione dei clienti;
- Piattaforma di intelligence Cogito, applicazione utilizzata per la raccolta di notizie, documenti e informazioni testuali per la ricerca di notizie negative riguardanti i clienti sottoposti a due diligence;
- Rozes, uno strumento di data intelligence che, analizzando i bilanci in tempo reale, consente di identificare aziende i cui indicatori patrimoniali e finanziari sono simili a quelli riscontrati nelle aziende soggette a infiltrazioni criminali.

Inoltre, nell'ambito degli strumenti avanzati sopra citati, sono stati individuati alcuni "trigger events", volti ad intercettare eventi riguardanti il cliente e/o i rapporti ad esso correlati, determinando una variazione della data di scadenza del "Customer Evaluation – KYC", ad esempio:

- in caso di modifica dei dati anagrafici del titolare effettivo e del legale rappresentante;
- in caso di variazione del Profilo di Rischio dovuta alla presenza di alcuni fattori ad alto rischio tra quelli previsti dal Provvedimento;
- in caso di assunzione del ruolo di PEP da parte di un titolare effettivo, ovvero di registrazione di un nuovo titolare effettivo PEP;
- in caso di delega ad un rapporto di clientela persona fisica conferito ad un soggetto qualificabile come PEP;
- in caso di discordanza tra il titolare effettivo iscritto nel registro e quanto risulta dagli estratti della Camera di Commercio;
- in caso di controlli di secondo livello da parte della Funzione AML.

La responsabilità del processo di due diligence di un cliente spetta all'unità di gestione delle relazioni con il cliente, che in genere gestisce l'instaurazione di nuovi rapporti continuativi, esegue eventuali transazioni occasionali, rivaluta periodicamente i clienti esistenti e garantisce il monitoraggio continuo della relazione con il cliente.

3.5 - OBBLIGHI DI ASTENIMENTO

La Società si astiene dall'instaurare, eseguire o proseguire il rapporto, le operazioni e le prestazioni professionali (c.d. obbligo di astensione) in caso di oggettiva impossibilità a svolgere l'adeguata verifica della clientela, valutando se segnalare alla UIF un'operazione sospetta.

Nei casi in cui l'astensione non è possibile, poiché sussiste un obbligo legale di eseguire l'operazione non rinviabile o qualora rifiutarla potrebbe ostacolare le indagini, la Società è comunque tenuta a segnalare immediatamente l'operazione sospetta.

Inoltre, qualora a seguito di un'ulteriore valutazione o a valle del processo di due diligence rafforzata emergano elementi di elevato rischio che possano incidere sul profilo legale e/o reputazionale della Società, la Società si riserva il diritto di limitare o risolvere il rapporto commerciale con il cliente. Tali limitazioni possono riguardare, ad esempio, l'accesso del cliente a determinate tipologie di prodotti o comportare l'interruzione dei servizi offerti dalla Società in relazione all'account/rapporto.

Le misure di adeguata verifica della clientela adottate dalla Società non precludono/negano, tuttavia, l'accesso ai servizi finanziari a clienti o intere categorie di clienti ad alto rischio che ne avrebbero diritto ai sensi della normativa vigente, salvi i casi espressamente previsti dal D.Lgs. 231/07, in merito al divieto di intrattenere rapporti con determinate tipologie di soggetti.

La Società non intrattiene rapporti di corrispondenza con una banca di comodo e si astiene dall'intrattenere rapporti con soggetti che consentano l'accesso a rapporti di corrispondenza con una banca di comodo. Non deve entrare in rapporti d'affari con soggetti il cui assetto proprietario (societario, fiscale e finanziario) sia caratterizzato da un elevato grado di opacità che impedisca la chiara identificazione del titolare effettivo ovvero la natura e lo scopo della struttura.

A tal fine la Società adotta tutte le misure affinché non collabori deliberatamente e consapevolmente con istituti finanziari che a loro volta operano con banche di comodo.

Inoltre, la Società si astiene dall'instaurare o proseguire rapporti d'affari con soggetti particolarmente esposti al rischio di riciclaggio/finanziamento del terrorismo, quali:

- Società fiduciarie che hanno sede legale in un Paese indicato dal GAFI come a maggior rischio di riciclaggio o che non adottano misure coerenti con gli obblighi imposti dal D.Lgs. 231/07 o dalle Direttive europee;
- Trust per i quali non sono disponibili informazioni adeguate, accurate e aggiornate sulla titolarità effettiva del trust, sulla sua natura e sul suo scopo;
- Società di scommesse, anche on-line, casinò e operatori di Bingo per le quali non siano state rilasciate e/o verificate autorizzazioni e/o licenze previste dalla normativa italiana ed internazionale;
- Soggetti affiliati e mandatari dei prestatori di servizi di pagamento (di cui alla definizione dell'art.1 c.2 lettera nn) e degli istituti di moneta elettronica che non rispettano le disposizioni del capo V del D.Lgs. 231/07 agli articoli 43 e ss.;
- Società a responsabilità limitata o controllate tramite azioni al portatore, con sede in Paesi ad alto rischio;
- Clienti che operano nella produzione e vendita di marijuana light o in locali di intrattenimento per adulti, qualora non sia in grado di verificare le autorizzazioni previste dalla legge.

La Società utilizza tutte le informazioni acquisite durante il processo di due diligence sui propri clienti e sulle loro transazioni per determinare se una transazione o un rapporto commerciale è, direttamente o indirettamente, collegato a persone o entità coinvolte nel riciclaggio di denaro, nel finanziamento del terrorismo o nello sviluppo di armi di distruzione di massa, e non supporta in alcun modo transazioni che coinvolgono armi controverse e/o vietate dai trattati internazionali,
ad es. armi nucleari, biologiche e chimiche, bombe a grappolo, armi contenenti uranio impoverito, mine antiuomo.

Relativamente alla produzione, transito e/o commercializzazione di materiali di armamento diversi da quelli sopra menzionati, la Società può sostenere operazioni debitamente autorizzate dalle autorità competenti e conformi alla normativa applicabile e vigente.

3.6 – SEGNALAZIONE DI OPERAZIONI SOSPETTE

Ogni volta che la Società sospetta o ha ragionevoli motivi per sospettare che sia stata o sia condotta o tentata un'operazione di riciclaggio di denaro o di finanziamento del terrorismo:

- presenta una segnalazione di operazione sospetta all'Unità di Informazione Finanziaria

(UIF), se l'operazione ha sede in Italia;

- se l'operazione ha sede in un altro Paese, si attiene a quanto previsto dalla normativa locale e, ove questa preveda l'applicazione di misure equivalenti a quelle previste dalla normativa comunitaria, informa tempestivamente il Responsabile Antiriciclaggio, adottando tutte le cautele necessarie a tutelare l'identità dei segnalanti dell'operazione sospetta.

La Società ha posto in essere procedure e processi per monitorare, identificare e segnalare attività sospette in conformità con i tempi e le modalità richieste dalla Legge applicabile.

I dipendenti segnalano tempestivamente qualsiasi conoscenza o sospetto di riciclaggio di denaro, finanziamento del terrorismo o di altre attività criminali, o proventi di attività criminali, indipendentemente dalla loro dimensione, in conformità con il modello organizzativo aggiornato e le modalità operative previste dalla normativa interna di riferimento. Fino al completamento del processo di segnalazione, la Società si astiene dal porre in essere l'operazione, salvo che ciò sia impossibile in quanto sussista un obbligo legale di accettare l'atto o l'esecuzione dell'operazione non sia rinviabile a causa del normale svolgimento degli affari o laddove possa ostacolare le indagini. In questi casi la segnalazione viene inviata immediatamente dopo l'esecuzione dell'operazione.

Costituiscono motivo di sospetto le caratteristiche, l'entità e la natura dell'operazione, il tentativo di frazionamento dell'operazione e ogni altra circostanza di cui i dipendenti siano venuti a conoscenza in ragione delle loro mansioni, tenuto conto anche della portata finanziaria e della natura dell'attività svolta dall'oggetto dell'operazione sospetta, sulla base degli elementi acquisiti ai sensi della normativa antiriciclaggio (ad esempio in sede di due diligence).

Per limitare il rischio di coinvolgimento della Società – anche involontario – nelle attività illecite sopra menzionate, viene attivato un processo di due diligence rafforzato nelle operazioni di trasferimento di fondi laddove gli attori coinvolti in questo tipo di operazioni (ordinante, beneficiario, le banche coinvolte nel trasferimento di fondi) possono indurre a sospettare di riciclaggio di denaro, finanziamento del terrorismo o violazioni delle restrizioni internazionali applicabili su determinati beni, persone o entità.

A valle del processo di segnalazione, la Società potrà limitare e/o interrompere il rapporto commerciale con i clienti, in particolare laddove tale rapporto possa costituire un significativo rischio legale o reputazionale per Rox Pay S.r.l.

3.7 – CONSERVAZIONE DEI DATI

La Società conserva tutti i documenti e registra tutti i dati ottenuti attraverso il processo di adeguata verifica della clientela, garantendo la tracciabilità delle transazioni della clientela per agevolare le funzioni di controllo, comprese le ispezioni, della Banca d'Italia e della UIF.

A tal fine Rox Pay S.r.l., in qualità di intermediario finanziario con sede in Italia, ha istituito un Archivio Unico Informatico (Archivio Unico Informatico o AUI) che le consente di fornire informazioni alla Banca d'Italia e alla UIF secondo le norme tecniche specificate nell'Allegato 2 delle Disposizioni in materia di conservazione dei dati. Questo archivio memorizza elettronicamente tutti i dati identificativi e altre informazioni relative ai rapporti commerciali in corso e alle transazioni con i clienti come richiesto dalla legge applicabile.

Al riguardo, in risposta ai recenti aggiornamenti introdotti dalle "Disposizioni in materia di conservazione dei dati e di accesso a documenti, dati e informazioni" e dalle "Disposizioni in

materia di trasmissione dei dati aggregati", la Società ha deciso di adottare alcuni principi di esenzione dagli obblighi di registrazione come espressamente previsti. In particolare, i dati e le informazioni riguardanti le operazioni effettuate dagli intermediari bancari e finanziari, che rientrano nelle fattispecie indicate dall'art

8 delle Disposizioni sulla Conservazione dei dati e l'articolo 3 delle Disposizioni sui dati aggregati non sono registrati nell'Archivio Unico Informatico.

Per quanto riguarda gli obblighi di adeguata verifica della clientela, la Società conserva copie o registrazioni di tutti i documenti richiesti per un periodo di dieci anni dalla cessazione del rapporto commerciale.

Per quanto riguarda le transazioni e i rapporti commerciali in corso, tutti i documenti giustificativi e le registrazioni, ad esempio documenti originali o copie ammissibili in giudizio, vengono conservati per un periodo di dieci anni dopo l'esecuzione dell'operazione o dopo la cessazione del rapporto commerciale.

3.8 – LA PREVENZIONE RIGUARDA MISURE RESTRITTIVE

Considerata la natura, le dimensioni e la complessità della propria attività, nonché la gamma e la tipologia dei servizi forniti, la Società è esposta al rischio di violazione delle misure restrittive.

Al fine di mantenere un sistema organizzativo e procedurale volto a garantire il rispetto delle misure restrittive internazionali, comunitarie e nazionali, il rischio di violazione delle misure restrittive è valutato dalla Funzione Antiriciclaggio sulla base di fattori geografici, di clientela, di prodotti/servizi e di canale distributivo, assicurando un costante monitoraggio dell'efficacia del sistema, garantito anche attraverso la periodica conduzione di un esercizio di self-assessment, che consenta l'identificazione di eventuali azioni correttive in risposta alla rilevazione di criticità esistenti e/o l'adozione di idonee misure di prevenzione e mitigazione del rischio.

La Società ha stabilito procedure e processi per monitorare, identificare e segnalare le attività che violano le misure restrittive, con tempi e modalità coerenti con i requisiti di legge.

I controlli esistenti su persone/enti e transazioni vengono effettuati attraverso un processo di screening automatizzato, effettuato sia quotidianamente che durante la fase di onboarding, utilizzando specifici elenchi – aggiornati due volte al giorno – riguardanti clienti, controparti, paesi e transazioni.

Sono in atto processi per monitorare i flussi in entrata o in uscita verso paesi e/o enti soggetti a sanzioni finanziarie internazionali, con responsabilità definite tra le funzioni competenti.

Si garantisce che il personale sia adeguatamente formato e informato sulle politiche, procedure e controlli al fine di rispettare le misure restrittive.

4 – ELENCO DEI PROCESSI CHIAVE

4.1 – GESTIONE DEL RISCHIO DI RICICLAGGIO E FINANZIAMENTO DEL TERRORISMO

Il processo di "Gestione del rischio di riciclaggio e finanziamento del terrorismo" è il processo attraverso il quale all'interno della Società vengono svolte le seguenti attività al fine di mitigare il rischio di mancato rispetto dei requisiti in materia di antiriciclaggio e finanziamento del terrorismo:

- Identificazione del rischio di non conformità ai requisiti AML-CFT attraverso la

supervisione continua delle modifiche legislative e la valutazione degli impatti sui processi e sulle procedure aziendali, nonché identificazione e valutazione del rischio AML-CFT utilizzando un approccio basato sul rischio;

- Gestione e mitigazione del rischio di riciclaggio e di finanziamento del terrorismo attraverso l'implementazione e il monitoraggio delle azioni di mitigazione del rischio di non conformità previste nel Piano annuale (Piano AML) o individuate dalla Governance della Società come applicate da tutte le funzioni aziendali interessate nell'implementazione delle procedure (norme interne, applicazioni informatiche, processi operativi, controlli);
- Controlli di conformità (ex-ante ed ex-post) negli ambiti normativi assegnati dalla proprietà attraverso la definizione e il monitoraggio degli indicatori di rischio e della loro evoluzione nel tempo. Lo scopo è quello di individuare eventuali situazioni di non conformità nonché di svolgere attività di controllo ex-ante ed ex-post;
- Fornire consulenza e supporto su tematiche AML/CFT, partecipando a gruppi di lavoro interfunzionali e fornendo supporto alle strutture aziendali o agli Organi di Alta Gestione nelle questioni e nei processi aziendali in cui il rischio di riciclaggio e finanziamento del terrorismo è rilevante, espletando gli adempimenti previsti dalla normativa di vigilanza ed effettuando una valutazione preliminare di conformità in tale ambito in sede di offerta di nuovi prodotti/servizi;
- Monitoraggio e controllo del rischio AML/CFT attraverso l'analisi dei flussi informativi ricevuti dalle funzioni di I livello e dalle altre funzioni di controllo relativi agli adempimenti operativi antiriciclaggio e mediante l'implementazione dei controlli di monitoraggio del rischio e verificandone costantemente l'adeguatezza;
- Condurre l'autovalutazione antiriciclaggio mediante lo svolgimento delle attività preliminari necessarie alla compilazione dei Questionari c.d. "Sistema" e "Operativo" nonché alla determinazione del rischio residuo;
- Reporting verso gli Organi Sociali apicali e le Autorità di Vigilanza, in particolare predisponendosi a riferire annualmente agli Organi Sociali e al Consiglio di Sorveglianza nonché predisponendosi a riferire periodicamente sull'attività svolta e sulle eventuali specifiche richieste provenienti dalle Autorità di Vigilanza;
- Erogare specifici corsi di formazione AML/CFT organizzando un adeguato piano formativo insieme alle altre funzioni aziendali preposte alla formazione. L'obiettivo è quello di realizzare una formazione continua dei dipendenti e dei collaboratori.

Le regole e le responsabilità specifiche della Società in merito a questo processo sono dettagliate nel documento interno
documento "Procedure interne antiriciclaggio e finanziamento del terrorismo".

4.2 – GESTIONE DEI RAPPORTI CON LE AUTORITÀ DI VIGILANZA PER IL CONTRASTO AL RICICLAGGIO E AL FINANZIAMENTO DEL TERRORISMO

Il processo AML/CFT Regulatory Relationship Management è il processo attraverso il quale all'interno della Società vengono svolte attività per gestire, analizzare, indirizzare e monitorare tutte le comunicazioni con le autorità di regolamentazione su questioni relative all'antiriciclaggio e al contrasto al finanziamento del terrorismo. L'obiettivo è quello di presidiare queste attività, compresa l'archiviazione dei documenti in un unico repository.

Nell'ambito di questo processo vengono svolte le seguenti attività:

- Gestione dei rapporti con le Autorità di Vigilanza (Antiriciclaggio), gestendo, analizzando ed indirizzando le comunicazioni e le richieste delle Autorità di Vigilanza in merito alla conformità in materia;
- Gestione delle Segnalazioni di Vigilanza Antiriciclaggio, attraverso la predisposizione

del flusso e l'invio delle Segnalazioni di Vigilanza Antiriciclaggio;

- Cura dei procedimenti amministrativi in materia di antiriciclaggio attraverso l'esame delle domande riconvenzionali relative a procedimenti amministrativi notificati alla Società dalle autorità competenti (GdF e UIF) nonché rappresentanza della Società avanti al MEF, essendo responsabile del censimento dei procedimenti nella relativa istanza e dell'accantonamento al Fondo Rischi ed Oneri e dell'eventuale pagamento di sanzioni, in coordinamento con la Funzione Budget.

Le specifiche regole e responsabilità della Società in merito a tale processo sono dettagliate nel documento interno "Procedure interne antiriciclaggio e contrasto al finanziamento del terrorismo".

4.3 – GESTIONE DELLE ESIGENZE OPERATIVE PER IL CONTRASTO AL RICICLAGGIO E AL FINANZIAMENTO DEL TERRORISMO

Il processo di Gestione dei Requisiti Operativi AML/CFT è il processo attraverso il quale vengono svolte all'interno della Società le seguenti attività al fine di conformarsi ai requisiti normativi:

- limitare l'utilizzo del contante e dei titoli al portatore, dando attuazione agli obblighi normativi in materia di limitazioni all'utilizzo del contante e dei titoli/titoli al portatore;
- gestire adeguati obblighi di adeguata verifica della clientela, eseguendo attività di adeguata verifica della clientela (o di adeguata verifica rafforzata) nei casi previsti dalla Legge italiana (D.Lgs. 231/07 e successive modifiche) in funzione del profilo di rischio del cliente, supportando la Rete della Società nell'adempimento degli obblighi previsti dalle leggi e dai regolamenti vigenti, e fornendo supporto alle strutture della Società che gestiscono i rapporti con la clientela e con le controparti bancarie e finanziarie al fine di consentire l'instaurazione ed il mantenimento dei rapporti;
- gestire gli obblighi di segnalazione delle operazioni sospette, svolgendo le attività di segnalazione di operazioni sospette in esecuzione delle deleghe del Consiglio di Amministrazione (ex art. 36 D.Lgs. 231/07) e monitorando le richieste pervenute dalla UIF;
- gestire gli adempimenti in materia di contrasto al finanziamento del terrorismo, definendo la metodologia di screening volta ad assicurare l'attuazione delle misure restrittive comunitarie e nazionali, verificando il recepimento degli aggiornamenti della Sanction List nonché segnalando alle competenti Autorità (nazionali e di vigilanza) i provvedimenti restrittivi (UIF, MAECI e MEF) sui provvedimenti di congelamento dei capitali (ex D.Lgs. 109/07) ed espletando i necessari adempimenti operativi;
- gestire gli obblighi di conservazione dei dati, verificando l'affidabilità del Sistema Informativo mediante l'aggiornamento dell'Archivio Unico Informatico (AUI), apportando eventuali revisioni, inviando periodicamente i dati aggregati alla UIF e trasmettendo alla UIF e alla Banca d'Italia le comunicazioni previste dalla normativa;
- monitorare la corretta attuazione delle sanzioni finanziarie internazionali (embarghi finanziari);
- monitoraggio continuo della clientela a maggior rischio di riciclaggio e finanziamento del terrorismo, monitoraggio delle richieste di approfondimento dei clienti che potenzialmente espongono la Società ad elevati rischi di riciclaggio, attivando, ove necessario, il processo di valutazione delle operazioni sospette e il processo di screening dei clienti che potenzialmente espongono la Società ad elevati rischi di riciclaggio.

Le regole e le responsabilità specifiche della Società in merito a questo processo sono dettagliate

nel documento interno
documento “Procedure interne antiriciclaggio e finanziamento del terrorismo”.

5 - QUADRI ORGANIZZATIVI E ORGANI DI CONTROLLO

Per gestire efficacemente il rischio di riciclaggio e di finanziamento del terrorismo, nonché di violazione delle Misure Restrittive, la Società ha individuato funzioni organizzative, risorse e procedure coerenti e proporzionate alla tipologia e dimensione dell'attività svolta, alla complessità organizzativa nonché alle caratteristiche operative.

Il monitoraggio dei rischi relativi al riciclaggio e al finanziamento del terrorismo è assicurato:

- dalla Funzione Antiriciclaggio di Rox Pay S.r.l., la cui responsabilità è affidata al Responsabile della Funzione AML che riporta direttamente all'Amministratore Delegato.
- Dal Membro dell'organo amministrativo responsabile dell'Antiriciclaggio, con delega all'Amministratore Delegato, che costituisce il principale punto di contatto tra il Responsabile della Funzione Antiriciclaggio e il Consiglio di Amministrazione e garantisce a quest'ultimo le informazioni necessarie per comprendere appieno la rilevanza dei rischi di riciclaggio a cui Rox Pay S.r.l. è esposto.

Il monitoraggio dei rischi connessi alla violazione delle Misure Restrittive:

- è assicurata dal Responsabile delle Misure Restrittive, la cui responsabilità è affidata al Responsabile della Funzione AML, che vigila sull'adeguatezza e sull'efficacia delle politiche, delle procedure interne e dei controlli relativi alla gestione delle Misure Restrittive, delle sanzioni e degli embarghi. Il Responsabile propone, in collaborazione con le competenti funzioni aziendali, le modifiche organizzative e procedurali necessarie e/o opportune per garantire un adeguato presidio del rischio di violazione di misure restrittive, sanzioni ed embarghi.

La Società, nel rispetto della normativa vigente, ha impostato la propria struttura organizzativa e di governo societario in modo da tutelare gli interessi della Società assicurando, al tempo stesso, una sana e prudente gestione ed evitando il rischio, anche involontario,
- di qualsiasi coinvolgimento diretto in atti di riciclaggio e/o finanziamento del terrorismo.

A tal fine, in conformità al Sistema di Controllo Interno adottato dalla Società, il Consiglio di Amministrazione e il Collegio Sindacale sono coinvolti nella mitigazione dei rischi sopra indicati attraverso compiti e responsabilità chiaramente definiti.

Inoltre, la Società ha istituito un'unità centralizzata per la gestione del sistema interno di segnalazione delle violazioni, con la responsabilità di supervisionare le attività di ricezione, analisi e valutazione delle segnalazioni inoltrate dai dipendenti attraverso la procedura Whistleblowing.

6 – REVISIONE E AGGIORNAMENTO DELLA POLICY

La Funzione Antiriciclaggio riesamina la policy con cadenza almeno annuale, la aggiorna se e dove necessario e predispone il testo per l'approvazione da parte del Consiglio di Amministrazione su proposta dell'Amministratore Delegato.

Eventuali modifiche alla Politica approvate dal Consiglio di Amministrazione di Rox Pay S.r.l. vengono successivamente implementati in tutta la Società con delibera del vertice aziendale, allineando responsabilità, processi e regole interne.