Procedura operativa del Processo di adeguata verifica, SOS e gestione conto

Procedura emessa il 13/06/2022
Owner della procedura: Perspective Happiness & Services

1 OBIETTIVI DEL DOCUMENTO

Obiettivo del presente documento è illustrare l'origine e le caratteristiche del processo di adeguata verifica della clientela. In particolare, la procedura descrive:

- le attività operative e la sequenza logica con cui sono eseguite;
- il ruolo e la responsabilità degli attori coinvolti a vario titolo nel processo;
- i dettagli dei controlli effettuati;
- gli strumenti a supporto dell'operatività.

Facendo riferimento alla tassonomia dei processi aziendali, i processi in esame sono classificati:

Adeguata verifica

1.00 Processi Direzionali

1.09 Antiriciclaggio e FCM

1.09.3 Definizione linee guida adeguata verifica e profilatura del rischio antiriciclaggio

SOS

1.00 Processi Direzionali

1.09 Antiriciclaggio e FCM

1.09.8 Segnalazione di operazioni sospette

Gestione conto

3.00 Processi di Operations

3.01 Conti di pagamento

3.01.01 Gestione conto

1.1 Ambito di applicazione

La presente procedura si applica a Flowe S.p.A. Società Benefit.

1.2 Aggiornamento del documento

L'aggiornamento e la revisione del presente documento sono di responsabilità della *Perspective Happiness & Services*.

2 DEFINIZIONI

Si riportano di seguito alcune definizioni e concetti di base utilizzati all'interno della procedura operativa:

- **AML (*Anti Money Laundering*)**: dicitura inglese (in italiano Antiriciclaggio) con cui si intende l'azione preventiva e la lotta al riciclaggio di beni, denaro o altre utilità in genere. L'attività di riciclaggio in sé e per sé consiste nell'investire capitali provenienti da reato all'interno di attività lecite, così da rendere difficoltosa la loro identificazione. Attraverso questo meccanismo, ogni bene frutto di attività illecita (traffico di stupefacenti, evasione fiscale, rapina, sequestro o qualsivoglia reato non colposo) viene "ripulito" dal suo alone di illiceità e reintrodotto nel circolo economico attraverso sbocchi perfettamente legali.
- **AUI**: Archivio Unico Informatico, sistema di registrazione e conservazione dati adottato dalla società
- **KYC (*Know Your Customer*)**: insieme di procedure che, conformemente al D.Lgs. 231/2007, devono essere attuate anche dagli IMEL, per acquisire dati certi e informazioni sull'identità della clientela. La Società è quindi tenuta a verificare l'identità del cliente e ad acquisire su di lui informazioni che aiutino a valutare il rischio di riciclaggio di denaro o finanziamento alla criminalità. La procedura non comprende la sola verifica dell'identità ma anche l'acquisizione di tutte quelle informazioni che dovrebbero consentire di valutare l'esposizione ad eventuali rischi di riciclaggio e finanziamento al terrorismo, su cui la Società dovrà effettuare un controllo costante.
- **Non US Person**: cliente non soggetto al Fisco Statunitense in base alla normativa FATCA (*Foreign Account Tax Compliance Act*) ovvero non avente nessuno dei 7 indizi (US Indicia)[1].
- **Persona Politicamente Esposta - PEP**: qualsiasi persona che occupi (o abbia occupato) una posizione pubblica preminente/importante, o che sia strettamente collegata o in rapporto di parentela diretto con una persona in tale posizione. La Società identifica come PEP le persone fisiche che occupano, o che hanno cessato di occupare da meno di un anno, le cariche pubbliche indicate previste da decreto antiriciclaggio, nonché i loro familiari e coloro che con i predetti intrattengono

[1] Indizi che devono essere verificati ed eventualmente giustificati dal cliente nel caso fossero in contrasto con lo *status* dichiarato: 1. Cittadinanza o residenza statunitense 2. Luogo di nascita negli Stati Uniti 3. Indirizzo corrente postale e di residenza statunitense 4. Ordini di bonifico permanente a favore di un conto intrattenuto negli Stati Uniti 5. Numeri telefonici statunitensi o non statunitensi 6. Procura o potestà di firma attualmente valida conferita a un soggetto con indirizzo statunitense 7. Indirizzo "c/o" o di fermo posta che rappresenta l'unico recapito del titolare del conto.

notoriamente stretti legami ai sensi delle previsioni dell'art. 1, comma 2, lett. dd) del D.Lgs. 231/2007 tempo per tempo vigente.

- **Politici Italiani Locali - PIL**: qualsiasi persona che occupi (o abbia occupato) una carica politica in Italia a livello regionale, provinciale, comunale e delle città metropolitane.
- **Lista Appalti**: si intende quell'elenco di soggetti aventi ruolo pubblico di assegnatari (RUP) nelle gare di appalti.
- **Lista Indesiderati**: si intende quell'insieme di liste che la Società utilizza come fonte allo scopo di identificare eventuali profili indesiderati di *prospect* e/o clienti a livello di Gruppo.
- **Perspective**: Unità organizzativa di Flowe.
- **Adeguata verifica rafforzata (di seguito anche AVR):** le misure rafforzate di adeguata verifica (ai sensi del D.Lgs. 231/2007) si applicano quando sussiste un elevato rischio di riciclaggio e di finanziamento del terrorismo, per effetto di specifiche previsioni normative o di una autonoma valutazione dell'intermediario. Le misure rafforzate di adeguata verifica della clientela vengono attuate: approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto; acquisendo informazioni aggiuntive sul cliente; intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale.
- **Piattaforma IQP**: Strumento a supporto del processo di KYC, dell'*outsourcer* InfoCert.
- **Piattaforma SGR**: Piattaforma utilizzata al fine di verificare la presenza di notizie di reato e/o altre notizie afferenti al *prospect*/cliente (es: assessore comunale; dirigente dell'agenzia del demanio ecc.)
- **Transaction Alert manager-Gateway SIC**: sezione FCM dedicata agli *alert* di *onboarding* (es. liste pep, pil).
- **Input**: profilo base dell'operatore FCM. Attualmente assegnato al *Team Operations Flowe* di Banca Mediolanum.
- **Chief Service Senior:** profilo da supervisore assegnato al *Team AML* della *Perspective Happiness & Services*.
- **Head of Chief Service:** profilo del Responsabile della *Perspective Happiness & Services*.
- **Soggetto collegato:** cliente Flowe collegato per operatività al cliente Flowe principale oggetto di analisi.
- **Prospect**: è una persona che ha iniziato il processo di *onboarding* per l'apertura del conto.
- **CIF Alert manager**: "*alert*" che scattano successivamente all'*onboarding* e consentono di valutare se rispetto al primo *check* c'è stato un cambiamento sulla posizione del cliente.
- **Batch Alert manager**: sezione FCM dedicata agli *alert profile* che scattano se le transazioni effettuate dal cliente sul proprio conto di pagamento superano soglie/parametri stabiliti dal Delegato della Funzione Antiriciclaggio.
- **Case Investigations**: sezione FCM mediante la quale è possibile inserire sulla posizione del cliente un apposito "*case*" sia in seguito a richieste provenienti dall'Autorità Giudiziaria sia qualora si renda necessario monitorare il cliente

(operazione eseguita in via occasionale, se richiesto dalla *Funzione Antiriciclaggio* ecc).

- **Pregiudizievoli:** sono atti che colpiscono i beni limitandone l'uso e/o la proprietà. Sono rilevate quotidianamente dalle Conservatorie dei registri immobiliari. Rientrano nelle pregiudizievoli: decreti ingiuntivi, sequestri conservativi, ipoteche, pignoramenti.
- **Protesto**: è l'atto attraverso il quale un Pubblico Ufficiale autorizzato, constata la mancata accettazione di una cambiale tratta o il mancato pagamento di una cambiale, di un vaglia cambiario, di un assegno bancario o postale. Gli ufficiali levatori, alla fine di ogni mese, devono trasmettere alla Camera di Commercio competente per territorio l'elenco dei protesti verbalizzati e i dati del debitore contro il quale ogni protesto è levato in modo da poter essere identificato.
- **Posting Restriction**: tipologia di blocco che può essere apposto sul conto nel *CoreBanking* (T24).
- **SOS**: Segnalazione Operazioni Sospette.
- **WorkFlow**: Gestionale utilizzato da Banca Mediolanum per il caricamento di dossier SOS alla UIF.

3 STRUMENTI A SUPPORTO DEL PROCESSO

L'infrastruttura tecnologica di cui si è dotata Flowe per supportare il processo in oggetto include gli strumenti informatici di seguito descritti.

3.1 Piattaforma IQP

Durante il processo di adeguata verifica Flowe si avvale della piattaforma applicativa IQP "Strumento a supporto del processo di KYC" dell'*outsourcer* InfoCert, la quale fornisce supporto per la gestione di alcuni steps del processo di onboarding ed apertura conto di pagamento, con riferimento alla verifica dell'identità del prospect.
Nello specifico, attraverso questo strumento la *Perspective Happiness & Services – Team AML* - anche mediante gli operatori del *Team Operations Flowe* di Banca Mediolanum, valuta l'esito del processo di KYC, effettua controlli manuali, accetta o respinge la richiesta di *onboarding* del soggetto. Inoltre, la *Perspective Happiness & Services - Team AML* - approfondisce laddove 6 necessario inviando "adeguata verifica rafforzata".

3.2 Legal Doc

Soluzione tecnologica per l'archiviazione sostitutiva e la consultazione di tutte le pratiche di *onboarding* che risultano essere state finalizzate e di tutte le evidenze raccolte anche in caso di fallimento del processo.

3.3 Temenos - FCM

Il modulo *Financial Crime Mitigation* (FCM) dell'*outsourcer* Temenos, di seguito denominato anche Gestionale Antiriciclaggio, permette lo svolgimento di una serie di attività e controlli ai fini AML supportando la Società dalla fase di acquisizione del cliente e per tutta la durata del rapporto.

Nello specifico, nel processo di *onboarding*, il modulo:

- registra al suo interno per ogni cliente Flowe una posizione anagrafica contenente le informazioni fornite in app Flowe dallo stesso cliente;
- con le informazioni acquisite e grazie ad uno *screening* del potenziale cliente con liste terze certificate gestisce il processo di calcolo del profilo di rischio, sulla base delle regole definite dalla Società;
- permette la sospensione del processo di *onboarding* per i potenziali clienti sui quali sono rilevate possibili corrispondenze con i soggetti presenti nelle liste, ponendo degli "*alert*" sulle posizioni che l'operatore della *Perspective Happiness & Services* può consultare e gestire al fine di accertare il livello di rischio del profilo, applicare ove necessarie misure di adeguata verifica rafforzata e accettare o respingere la richiesta di *onboarding* del soggetto.

Nello specifico, nel *continuum*, il modulo:

- registra gli aggiornamenti al suo interno per ogni cliente Flowe laddove vengano modificate le informazioni fornite in App Flowe dallo stesso cliente;
- con le informazioni acquisite e grazie ad uno *screening* del potenziale cliente con liste terze certificate gestisce il processo di aggiornamento del calcolo del rischio, sulla base delle regole definite dalla Società;
- permette la rivalutazione sulla posizione dei clienti sui quali sono rilevate possibili corrispondenze con i soggetti presenti nelle liste, ponendo degli "*alert- CIF*" sulle posizioni che gli operatori del *Team Operations Flowe* di Banca Mediolanum quale primo livello di controllo interno e gli operatori del *Team AML* della *Perspective Happiness & Services* in qualità di secondo livello di controllo interno, possono consultare e gestire al fine di accertare il livello di rischio del profilo, applicare ove necessarie misure di adeguata verifica rafforzata, bloccare e/o recedere dal rapporto.

3.4 P0 (Pzero)

P0 è la Piattaforma della Società (*full cloud* - Microsoft Azure) sulla quale è implementata la logica applicativa. Mediante la piattaforma è possibile integrare sistemi esterni.
P0 supporta il processo di *onboarding* effettuando dei controlli sia sui dati acquisiti tramite app sia comunicando con le piattaforme messe a disposizione da InfoCert oltre a controlli *quali ID document manager* e *face manager* utilizzando la tecnologia di intelligenza artificiale fornita da Microsoft.

3.5 Fan Base

Piattaforma applicativa sviluppata internamente alla Società basata su tecnologia *cloud* Microsoft Power Platform. Tale soluzione mette a disposizione degli operatori di *front e back office* funzionalità volte al supporto diretto e indiretto del cliente finale (*Customer Relationship Management*).
Fan Base è la *Power App* che supporta la *Perspective Happiness & Services – Team AML*- nello svolgimento delle attività di adeguata verifica legate al processo di *onboarding* ed apertura del conto di pagamento. A partire dal secondo trimestre 2022 la Power App consente, attraverso un compositore automatico nella sezione "*Activity - AML*", l'invio dell'adeguata verifica e tutte le comunicazioni necessarie alla gestione del rapporto con il cliente (es. *onboarding* PEP, *onboarding* notizie di reato, recesso a 60 giorni, ecc), nonché la tracciatura di tutte le attività effettuate sulla posizione del cliente consentendo un aggiornamento costante a tutta la *Perspective Happiness & Services*. Infine, tramite Fan Base è possibile appore blocchi all'utilizzo dell'App da parte del cliente in caso di soggetti potenzialmente sospetti e/o in caso di mancato riscontro ad adeguata verifica rafforzata.

3.6 GUI-NEXI

Flowe si avvale della piattaforma di gestione pagamenti e carte di pagamento SIA Crystal Gate (GUI) messa a disposizione dal fornitore NEXI. La piattaforma permette di impostare eventuali blocchi temporanei (ad esempio quando richiesto dagli Organi Investigativi e/o dall'Autorità Giudiziaria in caso di pignoramento, sequestro, richieste A.G., per soggetti considerati potenzialmente sospetti o in caso di mancato riscontro ad adeguata verifica rafforzata), e fornisce tutti i dettagli delle operazioni con carta (di debito e prepagata).

3.7 Gestionale Segnalazioni AUI – Easybox

Flowe si avvale dell'applicativo Easybox dell'*outsourcer* NEXI per la gestione dell'Archivio Unico Informatico (c.d. AUI) ai fini antiriciclaggio, all'interno del quale sono registrate tutte le prescritte operazioni derivanti dal processo di *onboarding* e le successive variazioni (comprese le cancellazioni per chiusura rapporti) ai fini delle successive segnalazioni alle Autorità di Vigilanza. Il *Team AML* della *Perspective Happiness & Services*, con cadenza mensile, si occupa della produzione e dell'invio in modalità telematica mediante il portale Infostat - UIF delle segnalazioni antiriciclaggio aggregate (S.AR.A.). Inoltre, attraverso l'Archivio Unico Informatico, gli operatori della *Perspective Happiness & Services – Team AML* - effettuano su richiesta dell'Autorità Giudiziaria la ricerca massiva AUI per rapporto (per operazioni di importo maggiore o uguale a 5.000 euro).

3.8 App Flowe

L'App Flowe è il canale con cui operano i clienti della Società, in versione *IOS* e *Android*, per la gestione del conto di pagamento e della carta di debito ad esso associata. Tramite l'App Flowe il cliente:

- inizia il processo di *onboarding* fornendo tutti i dati anagrafici e le informazioni necessarie al fine dell'apertura del conto Flowe e dell'adeguata verifica (ad esempio: professione, reddito ecc);
- usufruisce di un sistema *chatbot* al fine di ricevere supporto istantaneo anche durante le varie fasi del processo di *onboarding*;
- usufruisce di un sistema di notifiche in app che gli consente di essere informato sull'esito dell'onboarding;
- compila il modulo di adeguata verifica rafforzata in caso di profilo di rischio medio o alto.

3.9 Top

Orchestratore a supporto del processo di KYC che fornisce supporto per la gestione di alcune fasi del processo di *onboarding* del cliente, con riferimento alla verifica dell'identità del *prospect*. Nello specifico, attraverso questo strumento è possibile effettuare la firma digitale del contratto ed effettuare l'archiviazione sostitutiva su Legal Doc.

3.10 Experian

Piattaforma interfacciata dagli applicativi InfoCert ed utilizzata per lo svolgimento di ulteriori controlli sulla verifica dell'identità del potenziale cliente tramite consultazione della banca dati Experian (servizio Detect).

4 ATTORI, RUOLI E RESPONSABILITÀ

Gli attori, ovvero le unità organizzative aziendali coinvolte a vario titolo nei processi in ambito del presente documento sono di seguito richiamati, con evidenza esclusivamente del ruolo specificatamente attribuito nel processo medesimo.

4.1 Consiglio di Amministrazione

Approva un sistema di controlli interni funzionale alla rilevazione della gestione del rischio di riciclaggio e di finanziamento del terrorismo, assicurando che i compiti e le

responsabilità in materia antiriciclaggio e di contrasto al finanziamento del terrorismo siano allocati in modo chiaro e appropriato, garantendo che le funzioni medesime siano fornite di risorse qualitativamente e quantitativamente adeguate. Esamina annualmente la relazione del Responsabile della Funzione Antiriciclaggio sulle attività di verifica svolte, sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere, nonché sull'attività formativa del personale.

4.2 Amministratore Delegato

Assicura che i processi e le procedure interne consentano sia la corretta identificazione anagrafica del cliente e l'aggiornamento di tutte le informazioni funzionali all'adeguata verifica sia la costante verifica dell'attività svolta dai dipendenti e dai collaboratori al fine di rilevare eventuali anomalie.

4.3 Collegio Sindacale

Valuta l'idoneità delle procedure in essere per l'adeguata verifica della clientela, stimola l'azione di approfondimento di carenze, anomalie e irregolarità riscontrate e promuove l'adozione di eventuali misure correttive.

4.4 Organismo di vigilanza di cui al D.Lgs. 231/2001

Contribuisce in via preventiva a definire modelli idonei a prevenire la commissione di reati di riciclaggio, di autoriciclaggio, di finanziamento del terrorismo monitorando nel continuo il rispetto delle procedure ivi previste. Vigila sull'osservanza delle norme contenute nel D. Lgs. 231/2001 comunicando senza ritardo, agli organi di vertice, qualunque atto o fatto che possa costituire una violazione delle disposizioni in materia.

4.5 Funzione Internal Audit

Verifica il grado di adeguatezza dell'assetto organizzativo aziendale e la sua conformità rispetto alla disciplina di riferimento. In particolare, controlla il costante rispetto dell'obbligo di adeguata verifica, l'effettiva acquisizione e l'ordinata conservazione dei dati e documenti prescritti dalla normativa e l'effettivo grado di coinvolgimento del personale dipendente e dei collaboratori nonché dei responsabili delle strutture centrali e periferiche, al fine di dare attuazione all'obbligo della "collaborazione attiva". La Funzione svolge interventi di *follow-up* al fine di assicurarsi dell'avvenuta adozione degli interventi correttivi.

4.6 Funzione Antiriciclaggio

La Funzione Antiriciclaggio di Banca Mediolanum (funzione esternalizzata in virtù di apposito accordo di servizio), nell'ambito del presente processo, fornisce, qualora necessario, le linee guida e/o consulenza alla *Perspective Happiness & Services - Team AML* - nelle varie fasi del processo di acquisizione dei nuovi clienti.
Identifica le norme applicabili individuando procedure e controlli al fine di contrastare rischi di riciclaggio e di finanziamento del terrorismo; predispone annualmente una Relazione sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale, da sottoporre al Collegio Sindacale, all'Amministratore Delegato ed al Consiglio di Amministrazione della Società; valida e aggiorna la normativa interna, le policy ed i regolamenti in materia di antiriciclaggio e antiterrorismo.

4.7 Responsabile Antiriciclaggio

Al Responsabile Antiriciclaggio di Flowe competono funzioni complesse, sia in termini di verifica della funzionalità di procedure, strutture e sistemi, sia di supporto e consulenza agli Organi e alle Funzioni aziendali interessate. Il Responsabile Antiriciclaggio ha la responsabilità di supervisionare le attività svolte in materia di antiriciclaggio e di contrasto al terrorismo e rientra a tutti gli effetti nel novero dei responsabili delle Funzioni aziendali di controllo.

4.8 Delegato alle segnalazioni delle operazioni sospette

Valuta le segnalazioni di operazioni sospette ricevute, autorizza la trasmissione delle segnalazioni ritenute fondate alla UIF e risponde tempestivamente ad eventuali richieste di approfondimento; comunica con le modalità operative ritenute più appropriate, l'esito della propria valutazione alla struttura della Funzione Antiriciclaggio (in *outsourc*ing presso la Banca Capogruppo) che gestisce, in virtù di apposito accordo di servizio, le operazioni sospette.

4.9 Funzione Compliance

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

4.10 Perspective Happiness & Services

La *Perspective Happiness & Services - Team AML -*, nell'ambito del presente processo, è responsabile di:

- indirizzare verso i corretti canali di supporto - *Chatbot* o mail del *Team Caring* - il potenziale cliente (di seguito anche *prospect*) durante l'intera durata del rapporto;
- valutare per i casi in cui il processo di *onboarding* risulti sospeso (c.d. semaforo giallo), le possibili cause che hanno inibito l'apertura immediata del rapporto. Il *Team AML* della *Perspective Happiness & Services* si attiva, caso per caso, verificando la correttezza e la completezza dei dati inseriti a sistema provvedendo a richiedere modifiche/integrazioni al *prospect* laddove ritenuto necessario al fine del perfezionamento dell'*onboarding*;
- eseguire le attività di adeguata verifica rafforzata nei casi in cui, anche durante l'*onboarding*, si evidenzi la necessità di svolgere ulteriori accertamenti sul soggetto richiedendo eventualmente al *prospect* informazioni aggiuntive e, se necessario, richiedendo consulenza alla *Funzione Antiriciclaggio* al fine dell'adeguata valutazione del profilo di rischio del soggetto;
- autorizzare o inibire il completamento dell'*onboarding* e, quindi, acconsentire o meno all'apertura del conto di pagamento sulla base delle verifiche rafforzate svolte;
- presidiare il corretto funzionamento nonché l'adeguatezza e l'efficacia del sistema di identificazione a distanza della clientela;
- verificare la corretta attribuzione del profilo di rischio dalle procedure informatiche adottate e provvedere ad aggiornare i parametri utilizzati a fronte della rilevazione di nuovi elementi di rischio/evoluzioni del contesto normativo e operativo di riferimento;
- effettuare gli approfondimenti sulle operazioni "potenzialmente sospette" rilevate dagli strumenti di monitoraggio della clientela (FCM -Batch Alert manager);
- raccogliere i dati e le informazioni da inoltrare alla *Funzione Antiriciclaggio* per l'avvio del processo di valutazione di Segnalazione Operazioni Sospette (di seguito chiamate SOS);
- avviare il processo di estinzione del rapporto, previa autorizzazione del Responsabile della *Perspective Happiness & Services*, inviando relativa comunicazione al cliente.

La *Perspective Happiness & Services*, inoltre, viene coinvolta nel presente processo anche tramite:

- il *Team Monitoraggio Segnalazioni* che procede, in caso di anomalie massive riscontrate dal *Team Operations Flowe* di Banca Mediolanum sui dati confluiti su Easybox (anagrafiche soggetti, anagrafiche rapporti, estinzioni, movimenti) a risolverle coinvolgendo direttamente i fornitori impattati;
- Il *Team account monitoring* che si occupa di ricevere e verificare le segnalazioni di operazioni di sospetta frode; laddove necessario raccogliere i dati e le informazioni da inoltrare per l'avvio del processo di Segnalazione delle Operazioni Sospette; laddove necessario raccogliere l'autorizzazione alla chiusura del rapporto;

- Il *Team Customer interaction* che in seguito al contatto con il cliente, evidenzia al *Team AML* o *Account Monitoring* della *Perspective Happiness & Services* eventuali anomalie circa l'identificazione, le dichiarazioni in *onboarding* o l'operatività.

4.11 Outsourcers

4.11.1 Banca Mediolanum- Team Operations Flowe

Nell'ambito del presente processo il *Team Operations Flowe* del *Settore Product Operations* di Banca Mediolanum, nell'ottica di fornire supporto al *Team AML* della *Perspective Happiness & Services*, si occupa di:

- monitorare e gestire gli eventuali disallineamenti nella piattaforma EasyBox delle anagrafiche rispetto a T24. Laddove, si verifichino discrepanze massive/frequenti il *team* le segnala alla *Perspective Happiness & Services – Team Monitoraggio Segnalazioni*;
- effettuare le attività di quadratura giornaliera dell'alimentazione delle posizioni (aperte ed estinte) e dei movimenti sopra soglia di 5.000 euro nell'Archivio Unico Informatico, che viene periodicamente sottoposta al controllo della *Funzione Antiriciclaggio*;
- effettuare un primo controllo delle posizioni presenti sulla piattaforma IQP e su FCM e, laddove necessario, richiedere i dovuti approfondimenti al *Team AML* della *Perspective Happiness & Services*, che valuta se procedere con invio AVR;
- effettuare una prima analisi a supporto del *Team AML* della *Perspective Happiness & Services* in merito alle evidenze dei *match* tra i *prospect* e i soggetti inclusi nelle liste utilizzate dal Gestionale Antiriciclaggio (quali ad esempio *black-list*, liste PEP, liste PIL, liste appalti) al fine di escludere eventuali casi di omonimia attraverso l'utilizzo della piattaforma SGR;
- supportare il Team AML della *Perspective Happiness & Services*, nell'ambito dell'adeguata verifica (*Batch Alert Manager – CIF Alert Manager*) al fine di procedere alla verifica delle regole scattate in FCM (Input) passando le posizioni da dover approfondire in valutazione al *Team AML* della *Perspective Happiness & Services* (*Chief Service Senior*).

4.11.2 Banca Mediolanum - Ufficio Atti Giudiziari

L'Ufficio Atti Giudiziari della Direzione Affari Societari, Legale e Contenzioso
di Banca Mediolanum come *outsourcer* svolge, anche in collaborazione con le strutture operative, attività di riscontro e gestione delle richieste e dei provvedimenti da parte degli Organi Investigativi e dell'Autorità Giudiziaria.
La *Perspective Happiness & Services - Team AML* - inoltra tutte le comunicazioni ricevute a mezzo PEC, distinguendo in ragione della richiesta pervenuta, al *Team* di riferimento dell'Ufficio Atti Giudiziari. Inoltre, il *Team AML* della *Perspective*

Happiness & Services fornisce tutta la documentazione richiesta dagli Organi Investigativi e dall'Autorità Giudiziaria, e procede con l'apposizione di eventuali blocchi o preclusioni previste.
Infine, il *Team AML* della *Perspective Happiness & Services* si occupa del censimento nel gestionale di riferimento (FCM) del dato aggiuntivo per la profilatura di rischio della clientela e del caricamento, laddove necessario, di apposita segnalazione nel Sistema gestionale (WorkFlow) affinché, la *Funzione Antiriciclaggio* possa effettuare gli approfondimenti di competenza e sottoporre al Delegato le segnalazioni da valutare ai fini dell'eventuale inoltro alla UIF.

4.11.3 Temenos

Flowe si avvale dell'*outosourcer* Temenos - applicativo di *Core Banking* T24 – attraverso il quale apre la posizione anagrafica del cliente e il conto di pagamento a fronte dell'esito positivo di tutti i controlli di *onboarding*. T24 permette inoltre di gestire i processi "*core*" della Società per la gestione delle operazioni di pagamento. L'outsourcer fornisce anche il modulo *Financial Crime Mitigation* (FCM) per lo svolgimento di una serie di attività e controlli ai fini AML supportando la Società dalla fase di acquisizione del cliente e per tutta la durata del rapporto.

4.11.4 NEXI

Flowe si avvale dell'*outosourcer* NEXI per la consultazione delle informazioni della carta associata al cliente – tipologia di carta (fisica o virtuale), dettagli dell'intestatario della carta (luogo di spedizione, dati anagrafici e residenza). La piattaforma SIA Crystal Gate (GUI) permette inoltre, di impostare eventuali blocchi temporanei nonché di avere evidenza di tutti i dettagli delle operazioni della carta (di debito e prepagata).

4.11.5 Infocert

Nell'ambito del presente processo Inforcert supporta Flowe in alcune attività di "*Know Your Customer*" (di seguito anche KYC). L'*outsourcer* riceve ed elabora, in collaborazione con Experian, le informazioni del potenziale cliente raccolte tramite apposita sezione dedicata all'interno dell'App in fase di *onboarding* e necessarie ai fini dell'adempimento dei relativi obblighi normativi. Effettua, inoltre, alcuni controlli sulla correttezza delle informazioni di identità fornite dal *prospect* in fase di *onboarding* tramite App. Nello specifico mediante questo strumento gli operatori della *Perspective Happiness & Services* possono consultare l'esito del processo di KYC e visualizzare le regole applicate che non hanno consentito di proseguire nel processo di *onboarding*.
InfoCert supporta e gestisce il processo di archiviazione sostitutiva del *dossier* del cliente, conformemente alla normativa vigente (anche in caso di future eventuali variazioni della stessa).

5 ORIGINE DELLA PROCEDURA OPERATIVA SULL'ADEGUATA VERIFICA E SULL'ADEGUATA VERIFICA RAFFORZATA

Alla *Perspective Happiness & Services – Team AML* – compete il processo di identificazione e di adeguata verifica della clientela assegnata, quale primo livello di controllo, assicurando un monitoraggio continuo nel corso del rapporto.
La *Perspective Happiness & Services – Team AML* -, procede con l'adeguata verifica (di seguito anche ADV) o adeguata verifica rafforzata (di seguito anche AVR) sia nell'instaurazione del rapporto sia nel *continuum*.
Ad essa compete lo svolgimento del processo di adeguata verifica rafforzata nei casi previsti dalla normativa e, laddove richiesto dalla *Funzione Antiriciclaggio*, nonché l'onere di segnalare tempestivamente eventuali operazioni sospette, secondo le procedure e le modalità definite internamente, allorché si sappia, sospetti o ci siano ragionevoli motivi di sospettare che sia stata compiuta, sia in corso o sia tentata un'operazione di riciclaggio o finanziamento del terrorismo. Nel dettaglio, realizza l'istruttoria delle attività di adeguata verifica e di adeguata verifica rafforzata in tutti i casi in cui sia necessaria, integrando le informazioni ricevute dal cliente con quelle relative al profilo di rischio, all'operatività realizzata e alla conoscenza del cliente, derivante da eventuali precedenti istruttorie. Infine, monitora e aggiorna la profilatura di rischio della clientela della Società, in base alle informazioni emerse dalle istruttorie.

5.1 Identificazione e caratteristiche dell'adeguata verifica e dell'adeguata verifica rafforzata della clientela

Al fine di graduare la profondità e l'estensione degli obblighi di adeguata verifica, Flowe si avvale di uno specifico Gestionale - Temenos FCM - per la profilazione di rischio della clientela attraverso il quale sono attribuiti quotidianamente appositi punteggi a ciascun cliente (mediante il calcolo notturno), in funzione delle informazioni anagrafiche, dell'operatività e dei dati di relazione con la Società.

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

- relativi al cliente persona fisica (titolare effettivo ed esecutore);
- relativi a prodotti, servizi, operazioni o canali di distribuzione;
- relativi a fattori geografici.

I presidi informatici adottati permettono di determinare, sulla base dell'elaborazione dei dati e delle informazioni a disposizione della Società ed acquisite in sede di instaurazione di rapporti continuativi e di monitoraggio dell'operatività posta in essere, un "punteggio" rappresentativo del livello di rischio di riciclaggio o di finanziamento del terrorismo e di classificare i clienti in modo da poter eseguire, nei

loro confronti, verifiche più o meno incisive e commisurate ad una delle quattro tipologie di profilo di rischio.

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

RIF.	CLASSE DI RISCHIO	FREQUENZA AGGIORNAMENTO
I	Irrilevante	Ogni 48 mesi
B	Basso	Ogni 36 mesi
M	Medio	Ogni 24 mesi
A	Alto	Annuale (ogni 12 mesi)

In presenza di profilo di rischio Medio e/o Alto la Società approfondisce la conoscenza della clientela mediante l'adozione di presidi rafforzati di adeguata verifica.

FCM effettua automaticamente l'aggiornamento del profilo di rischio. Pertanto, allo scattare di detti indicatori ed al superamento della soglia di rischiosità prevista (Medio - Alto), la *Perspective Happiness & Services - Team AML* - effettuerà gli opportuni approfondimenti di adeguata verifica rafforzata. Ad esempio, quando:

- i fondi impiegati nel rapporto continuativo sono stati prodotti in un paese terzo, assume particolare rilievo il tasso di criminalità del paese stesso e l'efficacia del suo sistema investigativo e giudiziario;
- i fondi sono ricevuti da o inviati a paesi terzi associati ad attività terroristiche, i destinatari valutano eventuali elementi di sospetto, anche alla luce dello scopo e della natura del rapporto.

Indipendentemente dalle scadenze sopra indicate in tabella, l'aggiornamento dei dati e delle informazioni raccolte in sede di profilatura della clientela è richiesto alla scadenza del documento di identità nonché ogniqualvolta il *Team AML* a seguito di approfondimento sul cliente rilevi che non sono più attuali le informazioni precedentemente acquisite (es. se il cliente ha fatto scattare un *Alert* in FCM- *Batch Alert Manager* per reddito pari a 0 euro e status disoccupato ma dall'operatività si evince l'accredito di emolumenti, il *Team AML* richiede l'aggiornamento dell'anagrafica).

Il cliente può effettuare l'aggiornamento delle informazioni autonomamente, mediante accesso all'area riservata dell'App, aggiornando o confermando i dati ed effettuando l'importazione (*upload*) del documento; la convalida del documento e l'aggiornamento dei dati deve essere confermata dal cliente mediante SCA (*Strong Customer Authentication*). In caso di aggiornamento dei dati, FCM procede con il ricalcolo del profilo di rischio assumendo, quale data di scadenza, quella

corrispondente al nuovo profilo attribuito. Con particolare riferimento ai clienti con livello di rischio medio e alto, alla data di scadenza del profilo di rischio sarà il sistema automatico che chiederà al cliente di aggiornare il modulo di adeguata verifica rafforzata.

In ogni caso, la *Perspective Happiness & Services - Team AML* - ha l'obbligo di procedere con adeguata verifica rafforzata della clientela almeno nei seguenti momenti:

- in occasione della instaurazione di un rapporto continuativo;
- quando viene eseguita un'operazione occasionale disposta dal cliente che appaia sospetta (es. in quanto non conforme con il reddito dichiarato);
- quando vi è sospetto di riciclaggio o di finanziamento del terrorismo;
- quando sorgono dubbi sulla completezza, attendibilità o veridicità delle informazioni dichiarate dal cliente.

In caso di impossibilità oggettiva di svolgere l'adeguata verifica della clientela, così come previsto dall'art. 42 del Decreto Antiriciclaggio, Flowe si astiene dall'instaurare, proseguire il rapporto, a dar corso alle operazioni e a valutare se effettuare una segnalazione di operazione sospetta alla *Funzione di Antiriciclaggio* che procederà con segnalare alla UIF (Cfr. par. 12.2.2).

6 Adeguata verifica

Si riportano di seguito le attività di adeguata verifica svolte sia in fase di *onboarding* sia nel *continuum*.

6.1 Adeguata verifica in onboarding

In fase di *onboarding*, il *Team Operations Flowe* di Banca Mediolanum si occupa di effettuare un primo vaglio delle posizioni presenti sulla piattaforma IQP e su FCM, laddove necessario, richiede i dovuti approfondimenti al *Team AML* della *Perspective Happiness & Services*, che valuterà se procedere con invio AVR (Cfr. Cap. 7).

In particolare, in FCM i prospect in *onboarding* vengono sottoposti al controllo delle seguenti liste, ai sensi del D. Lgs. n. 231/07:

- **Lista Persone Esposte Politicamente** (di seguito PEP) sono considerate a più alto rischio di riciclaggio in quanto maggiormente esposte a potenziali fenomeni di corruzione.
  L'art. 1, c.2, lett. dd) – D. Lgs. n. 231/07 (c.d. Decreto Antiriciclaggio) prevede l'applicazione di misure rafforzate di adeguata verifica dei clienti che assumono la qualifica di PEP (cfr. Regolamento del Processo di adeguata verifica). In base a quanto previsto dalla normativa vigente, i soggetti originariamente individuati

come PEP perdono tale qualifica decorso un anno dalla cessazione delle cariche pubbliche ricoperte. Al termine dell'istruttoria, il *Team AML* della *Perspective Happiness & Services* sottopone, tramite *Alert* in ambiente FCM Temenos, la pratica al Responsabile della *Perspective Happiness & Services* stessa al fine di valutare se autorizzare l'instaurazione, il mantenimento e/o l'interruzione del rapporto con il *prospect*/cliente qualificato come PEP. Nel momento in cui il *Team AML* della *Perspective Happiness & Services* "certifica" il cliente come PEP, a questi viene automaticamente associato un attributo in FCM (c.d. dato aggiuntivo), che comporta un incremento del punteggio di rischio nel sistema di profilatura di + 25 punti, portando lo stesso in automatico nella fascia di rischio Alta. Nella lista dei PEP, abbiamo anche gli RCA (*Relative and Close Associate*), che sono coloro che presentano legami di parentela (ad es. fratello, figlio, nipote, moglie, marito) o professionali (ad es. *partner*, socio) con il PEP. Anche per gli RCA si applica l'adeguata verifica rafforzata, poiché rientrano nella lista delle persone politicamente esposte.

- **Lista Politici Italiani Locali** (di seguito PIL) sono coloro che occupano una carica politica in Italia a livello regionale, provinciale, comunale.
- **Lista Indesiderati** è una lista che contiene i nominativi dei clienti indesiderati della Capogruppo Banca Mediolanum, la quale viene periodicamente importata (cadenza mensile/bimestrale). Inoltre, la stessa *Funzione Antiriciclaggio* può indicare nuovi nominativi da aggiungere a questa lista.
- **Lista Appalti** è una lista che contiene un elenco dei soggetti aventi ruolo pubblico di assegnatari (RUP) gare di appalti.
- **Lista Nominativi**: un *alert* che scatta qualora un soggetto risulti positivo ad una notizia di reato pubblica.
- **Sanction List** è una lista di soggetti sottoposti a sanzione per ONU, EU, SDN, OFAC.
- **Embargo** è una lista di paesi soggetti a limitazioni.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica paese di nascita del *prospect* se incluso in: Grey List→ l'*onboarding* si ferma per valutazione da parte di un operatore del *Team Operations Flowe* di Banca Mediolanum attraverso la Piattaforma IQP. Il *Team AML* della *Perspective Happiness & Services* procede con l'invio di AVR al *prospect*	Automatico + Manuale	Continuativo	Power Apps; Piattaforma IQP
Blocco del processo qualora il *prospect* rientri nelle: • Sanction list (ONU, EU, SDN, OFAC...)	Automatico	Continuativo	App Flowe; P0; Piattaforma FCM

• Embargo (Lista di paesi soggetti a limitazioni)			
Verifica liste AML I dati fondamentali del *prospect* (Nome, Cognome, CF, Data e Luogo di Nascita, ecc.) sono utilizzati per verificare la presenza di una potenziale HIT nelle seguenti liste: • Lista PEP • Lista PIL • Lista Indesiderati • Lista Appalti • Lista Nominativi (Lista fornita periodicamente dal fornitore SGR Consulting che riporta il nome di tutti i soggetti coinvolti in diversi reati, ad es. truffa, spaccio, mafia, etc.). Questa lista viene stilata basandosi su fonti pubbliche certificate, come ad esempio gli articoli di note testate giornalistiche.	Automatico + Manuale	Continuativo	App Flowe; P0; Piattaforma FCM; Power Apps

6.1.1 Gestione posizioni in "stand by" per alert nel Gestionale Antiriciclaggio in onboarding

Il *Team AML* della *Perspective Happiness & Services* giornalmente, sulla base anche delle rilevazioni effettuate dal *Team Operations Flowe* di Banca Mediolanum, analizza su FCM la presenza di posizioni che in fase di *onboarding* hanno evidenziato degli *alert* che richiedono una verifica (ad esempio per l'eventuale presenza del *prospect* nelle liste di riferimento come liste PEP, PIL, ecc).
Laddove sia generato un potenziale *match* con tali liste, il *Team Operations Flowe* di Banca Mediolanum e successivamente, come secondo livello di controllo interno, il *Team AML* della *Perspective Happiness & Services,* prende in carico le posizioni e le analizza al fine di confermare o meno che il *prospect* sia effettivamente presente nelle liste di FCM, anche attraverso l'utilizzo della piattaforma SGR e del WEB (banche dati e le fonti aperte indipendenti e attendibili certificate); se necessario durante le verifiche viene coinvolta, per supporto, l'*Head of Chief Service* e la *Funzione Antiriciclaggio* di Banca Mediolanum.

Le evidenze delle verifiche svolte vengono conservate su FCM. Inoltre, in caso di approfondimenti svolti (per *alert* "true HIT") questi vengono conservati in un *case* aperto

ad hoc (ad es. *check* PIL, *check* PEP) sulla piattaforma FCM alla sezione "*Manager Customer*".

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Controllo di primo livello da parte del *Team Operations Flowe* di Banca Mediolanum sugli *alert* delle liste appalti e nominativi. In caso di *False HIT*, possono essere chiuse al livello input.	Automatico + Manuale	Continuativo	Piattaforma FCM; SGR; Power Apps
Verifica soggetto PEP Per la gestione del *prospect* che si dichiari PEP nel questionario AML in fase di *onboarding* si rimanda alla "Procedura Operativa di onboarding e apertura conto di pagamento". Per quanto riguarda il controllo delle liste, il *Team AML* verifica che le informazioni che hanno generato la potenziale HIT (nome, cognome, data di nascita, residenza, professione dichiarata) corrispondano alle stesse del *prospect* che ha effettuato l'*onboarding*. In caso di *match*, viene attivata da parte dell'operatore della *Perspective Happiness & Services – Team AML*: • la ricerca di informazioni su internet (banche dati e le fonti aperte indipendenti e attendibili certificate). Qualora da fonti aperte indipendenti si riescano a recuperare i dati economico/patrimoniali del soggetto PEP, potrebbe non essere necessario l'approfondimento; • la richiesta di adeguata verifica rafforzata con	Automatico + Manuale	Continuativo	Piattaforma FCM; SGR; Power Apps

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
documentazione aggiuntiva a supporto (e.g. invio dell'ultima dichiarazione dei redditi) In seguito al riscontro del *prospect*, che invia i moduli compilati e la dichiarazione dei redditi entro i termini richiesti, l'apertura del rapporto è oggetto di approvazione da parte del Responsabile della *Perspective Happiness & Services* che procede alla chiusura dell'*alert* come *True HIT*. Il *Team AML*, a seguito di approvazione procede con apertura del *case* in FCM.			
Lista PIL Il *Team AML* della *Perspective Happiness & Service*s verifica che i dati presenti nelle liste che hanno generato la potenziale HIT (nome, cognome, data di nascita, codice fiscale, residenza) corrispondano a quelli del *prospect* che ha effettuato l'*onboarding*.	Automatico + Manuale	Continuativo	Piattaforma FCM; SGR
Lista Appalti Il *Team AML* della *Perspective Happiness & Services* verifica che i dati presenti nelle liste che hanno generato la potenziale HIT (nome, cognome, data di nascita, codice fiscale, residenza) corrispondano a quelli del *prospect* che ha effettuato l'*onboarding*.	Automatico + Manuale	Continuativo	Piattaforma FCM

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Lista Nominativi Il *Team AML* verifica se i dati presenti nelle notizie che hanno fatto scattare l'*alert* (nome, cognome, data di nascita, residenza), corrispondano a quelli del *prospect* che ha effettuato l'*onboarding* (effettuando, se necessario, anche un confronto fotografico). In caso di *match*, l'operatore valuta a seconda della notizia di reato se procedere con il rifiuto della posizione oppure chiedere al *prospect* informazioni aggiuntive tramite adeguata verificata rafforzata.	Automatico + Manuale	Continuativo	Piattaforma FCM; SGR; Power Apps
Lista Indesiderati Il *Team AML* effettua delle verifiche con l'ausilio sia di Internet sia della piattaforma SGR per verificare una eventuale corrispondenza di dati tra l'*alert* emerso e i dati del *prospect*. Qualora il *Team AML* avesse dubbi sull'esatta corrispondenza, chiederà supporto alla *Funzione Antiriciclaggio* di Banca Mediolanum.	Automatico + Manuale	Continuativo	Piattaforma FCM; SGR

6.1.2 Rilevazione posizione anagrafica nel Gestionale Antiriciclaggio (FCM) in onboarding

Laddove sia stata identificata una vera rispondenza del *prospect* con un soggetto presente all'interno delle liste considerate ad alto profilo di rischio, FCM rileva la posizione anagrafica indicando la categoria a cui il *prospect* appartiene e individua profilo di rischio ad esso associato (alto). Il *Team AML* della *Perspective Happiness & Services* procede manualmente all'apertura di un apposito *case* in cui conserva la documentazione del cliente.
Si rappresenta che la posizione anagrafica del cliente viene automaticamente censita (a T+1) in FCM.

6.2 Adeguata verifica nel continuum

Nel *continuum* del rapporto la *Perspective Happiness & Services - Team AML* -, svolge controlli tramite FCM (sezione "Screen- CIF Alert Manager") sulle seguenti liste:

- Lista PEP
- Lista PIL
- Lista Nominativi
- Lista Appalti
- Lista Indesiderati

PEP

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
FCM effettua un controllo automatico giornaliero, su tutta la clientela, al fine di intercettare l'eventuale presenza di clienti in liste c.d. PEP	Automatico	Giornaliero	FCM
Il *Team AML* della *Perspective Happiness & Services* riceve un "*Alert*" (c.d. CIF) quando il sistema identifica un *match*, richiedendo maggiori informazioni al cliente con AVR. In seguito al riscontro del cliente, che invia i moduli compilati e la dichiarazione dei redditi entro i termini richiesti, il mantenimento del rapporto è oggetto di approvazione da parte del Responsabile della *Perspective Happiness & Services*.	Manuale	Ad Evento	FCM; SGR; Power Apps

Il *Team AML*, a seguito di approvazione procede con apertura del case in FCM.			

PIL

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
FCM effettua un controllo automatico giornaliero, su tutta la clientela, al fine di intercettare l'eventuale presenza di clienti in liste c.d. PIL	Automatico	Giornaliero	FCM
Il *Team AML* della *Perspective Happiness & Services* riceve un "*Alert*" (c.d. CIF) quando il sistema identifica un *match*	Automatico	Ad Evento	FCM; SGR

Lista Nominativi

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
FCM effettua un controllo automatico giornaliero, su tutta la clientela, al fine di intercettare l'eventuale presenza di clienti in liste c.d. Nominativi	Automatico	Giornaliero	FCM
Il *Team AML* della *Perspective Happiness & Services* riceve un "*Alert*" (c.d. CIF) quando il	Manuale	Ad Evento	FCM; SGR; Power Apps

sistema identifica un *match*, richiedendo maggiori informazioni al cliente con AVR			

Liste Appalti

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
FCM effettua un controllo automatico giornaliero, su tutta la clientela, al fine di intercettare l'eventuale presenza di clienti in liste c.d. Appalti	Automatico	Giornaliero	FCM
Il *Team AML* della *Perspective Happiness & Services* riceve un "Alert" (c.d. CIF) quando il sistema identifica un match	Automatico	Ad Evento	FCM

Lista Indesiderati

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
FCM effettua un controllo automatico giornaliero, su tutta la clientela, al fine di intercettare l'eventuale presenza di clienti in liste c.d. Indesiderati	Automatico	Giornaliero	FCM
Il *Team AML* della *Perspective Happiness & Services* riceve un "*Alert*" (c.d. CIF) quando il sistema identifica un	Manuale	Ad Evento	FCM; SGR

match richiedendo eventualmente maggiori informazioni alla *Funzione Antiriciclaggio*			

6.2.1 Aggiornamento posizione anagrafica nel Gestionale Antiriciclaggio (FCM) nel continuum

Laddove sia stata identificata una vera rispondenza del cliente con un soggetto presente all'interno delle liste considerate ad alto profilo di rischio, FCM aggiorna la posizione anagrafica indicando la categoria a cui il cliente appartiene e il profilo di rischio ad esso associato. Il *Team AML* della *Perspective Happiness & Services* procede manualmente all'apertura di un apposito *case* in FCM in cui conserva la documentazione del cliente.
Si rappresenta che la posizione anagrafica del cliente viene automaticamente aggiornata (a T+1) in FCM.

7 Adeguata verifica rafforzata

Si riportano di seguito le attività di adeguata verifica rafforzata svolte sia in fase di *onboarding* sia nel *continuum*.

7.1 Destinatari dell'Adeguata Verifica Rafforzata

La Normativa Antiriciclaggio identifica quali destinatari dell'adeguata verifica rafforzata sia Flowe - *Perspective Happiness & Services* - sia il cliente.

La Società adempie agli obblighi di adeguata verifica rafforzata nei confronti dei nuovi clienti nonché in relazione ai clienti già acquisiti.

Per il *prospect*, qualora non risponda alla e-mail di AVR entro i tempi richiesti dalla Società (5 giorni lavorativi), il processo di *onboarding* termina con il rifiuto della posizione.

Qualora, invece, la risposta del *prospect* sia incompleta o sospetta, il *Team AML* della *Perspective Happiness & Services*, con il supporto dell'*Head of Chief Service*, effettua degli approfondimenti sulla posizione e decide se aprire o meno il conto al *prospect*. In caso di esito positivo, il *prospect* viene informato via e-mail e tramite notifica in App, dell'apertura del conto. Se dal confronto dovesse conseguire esito negativo, il *prospect* viene informato tramite gli stessi applicativi su menzionati circa l'impossibilità di aprire il conto e quindi il processo termina.

Nel caso di AVR inviate al presunto PEP, qualora il *prospect* dovesse rispondere dichiarando di essere il soggetto identificato come PEP – fugando, pertanto, ogni dubbio e allegando l'intera documentazione richiesta -, l'approvazione dello stesso dovrà necessariamente passare per *l'Head of Chief Service*.

In relazione ai clienti già acquisiti, i destinatari svolgono l'adeguata verifica rafforzata quando opportuno, in ragione dell'innalzamento del livello di rischio di riciclaggio e di finanziamento del terrorismo associato al cliente.
La *Perspective Happiness & Services* applica le misure rafforzate di adeguata verifica della clientela, quando sussista un elevato rischio di riciclaggio e di finanziamento del terrorismo, risultante da specifiche previsioni normative oppure da una loro autonoma valutazione (cfr. cap 8 - 9) o qualora attraverso FCM - sezione *Batch Alert manager* - scattino degli *alert profile* – sulla base di transazioni effettuate dal cliente sul proprio conto di pagamento. In base al principio dell'approccio basato sul rischio, l'intensità e l'estensione degli obblighi di adeguata verifica della clientela sono modulati secondo il grado di rischio di riciclaggio e di finanziamento del terrorismo del singolo cliente.

Nel *continuum*, se un soggetto minore ha fatto scattare un *alert profile,* si procede con l'invio dell'AVR al soggetto maggiorenne che ha approvato il conto del minore. In tal caso, il *Team AML* della *Perspective Happiness & Services* oltre a verificare l'operatività presente sul conto del minore procede al controllo del legame tra maggiorenne e minore dichiarato al momento della sottoscrizione del contratto di quest'ultimo. In primo luogo, la verifica viene effettuata sul documento di identità del minore stesso, accertando i nominativi dei rispettivi genitori. Qualora si riscontrino anomalie, il *Team AML* della *Perspective Happiness & Services* procederà altresì a richiedere al maggiorenne collegato il rapporto di genitorialità (es. richiesta dell'atto di nascita/ stato di famiglia).

Resta comunque ferma la possibilità, da parte della *Funzione Antiriciclaggio*, di chiedere alla *Perspective Happiness & Services - Team AML* - di svolgere il processo di adeguata verifica rafforzata in tutti i casi in cui appaia particolarmente elevato il rischio di riciclaggio o finanziamento del terrorismo.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Prospect incluso in *Grey List*: l'*onboarding* si ferma per valutazione da parte di un operatore del *Team Operations Flowe* di Banca Mediolanum attraverso la Piattaforma IQP. Il *Team AML* della *Perspective Happiness & Services* procede con l'invio di AVR al *prospect*	Automatico + Manuale	Continuativo	Piattaforma IQP; Power Apps;
Prospect/Clienti che rientrano nella qualifica di PEP (*onboarding*/CIF): scatta un alert in automatico in FCM e il *Team AML* procede con invio AVR	Automatico + Manuale	Ad Evento	FCM;PowerApps; T24; GUI

Prospect/Clienti che rientrano nella Lista Nominatavi (*onboarding*/CIF): scatta un alert in automatico in FCM e il *Team AML* procede con invio AVR	Automatico + Manuale	Ad Evento	FCM; Power Apps; T24; GUI
Clienti oggetto di richieste/provvedimenti degli Organi Investigativi e/o dall'Autorità Giudiziaria	Automatico + Manuale	Ad Evento	FCM; Power Apps; T24; GUI
Clienti oggetto di decreti di sequestro, misure cautelari reali e di prevenzione adottate dall'Autorità Giudiziaria	Automatico + Manuale	Ad Evento	FCM; Power Apps; T24; GUI
Clienti che hanno "fatto scattare" un *alert profile* in FCM	Automatico + Manuale	Ad Evento	FCM; Power Apps; T24; GUI
Clienti oggetto di precedente segnalazione alla UIF	Automatico + Manuale	Ad Evento	FCM; Power Apps; T24; GUI
Clienti classificati a rischio alto, in base al sistema di profilatura della clientela adottato internamente o su richiesta del Delegato della *Funzione Antiriciclaggio*	Automatico + Manuale	Ad Evento	FCM; Power Apps; T24; GUI
Qualunque altro cliente, nel caso cui si ravvisa un più elevato rischio di riciclaggio o finanziamento del terrorismo (es. la riluttanza a fornire le informazioni richieste)	Automatico + Manuale	Ad Evento	FCM; Power Apps; T24; GUI

7.2 Modalità e esecuzione dell'adeguata verifica rafforzata

La Società si è adoperata affinché il cliente sia in grado di svolgere in App l'adeguata verifica rafforzata. In particolare, alla data di scadenza del profilo di rischio medio e alto, sarà il sistema automatico che chiederà al cliente di aggiornare il modulo di adeguata verifica rafforzata e solo in seguito i dati saranno acquisiti a sistema (FCM).

Inoltre, qualora risulti necessario approfondire con adeguata verifica, il *Team AML* della *Perspective Happiness & Services* si avvale di uno specifico applicativo Power Apps - Fan Base, che consente la tracciatura, la conservazione e l'invio dell'AVR tramite casella

Antiriciclaggio@flowe.com , nonché la possibilità di allegare i moduli di adeguata verifica rafforzata e di operatività, che dovranno essere compilati dal cliente oggetto di verifica.

CONTROLLO	DEADLINE RISCONTRO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
In caso di scadenza di profilo di rischio alto o medio	3 mesi dal giorno della scadenza	Automatico	A scadenza	App Flowe; P0; Power Apps; FCM
In presenza di uno dei casi in cui vi è obbligo di procedere con AVR: il *Team AML* della *Perspective Happiness & Services* invia prima mail	5 giorni lavorativi	Manuale	Ad Evento	Power Apps; FCM
Il *Team AML* della *Perspective Happiness & Services* procede con invio mail di sollecito, nel caso in cui il cliente non fornisca riscontro alla prima mail di AVR nei termini stabiliti	Ulteriori 5 giorni lavorativi	Manuale	Ad Evento	Power Apps; FCM
Il *Team AML* della *Perspective Happiness & Services* procede con invio mail di blocco + sms, nel caso in cui il cliente non fornisca riscontro alla mail di sollecito nei termini stabiliti	Ulteriori 5 giorni lavorativi	Manuale	Ad Evento	Power Apps; T24; GUI; FCM

Il *Team AML* valuta la necessità del caricamento del dossier SOS sul gestionale Mediolanum (WorkFlow)	/	Manuale	Ad Evento	WorkFlow; FCM

In seguito all'invio della prima mail di adeguata verifica rafforzata, la *Perspective Happiness & Services- Team AML* - verifica costantemente che il cliente fornisca riscontro entro le tempistiche sopraindicate. L'operatore è tenuto a valutare attentamente le informazioni fornite dal cliente, al fine di verificare che il riscontro fornito sia completo, corretto, esaustivo e coerente con le informazioni fornite in *onboarding*.
Tutte le attività svolte dal *Team AML* della *Perspective Happiness & Services* per eseguire la verifica rafforzata e i relativi esiti, sono tracciate all'interno del gestionale FCM mediante la creazione di appositi "*Case Investigations*", nonché all'interno del gestionale Power Apps - Fan Base nelle "*Activity-AML*".

7.3 Obblighi rafforzati

La *Perspective Happiness & Services - Team AML* - ha l'obbligo, in sede di adeguata verifica rafforzata, di:

- acquisire maggiori informazioni sul cliente;
- acquisire/aggiornare e valutare informazioni sulla reputazione del cliente ivi comprese eventuali pregiudizievoli;
- valutare attentamente le informazioni fornite dal cliente sullo scopo e sulla natura del rapporto, mettendole in relazione con le altre informazioni conosciute all'atto di apertura del conto (es. reddito) o, nel caso di clienti che hanno un rapporto già in essere con la Società, con l'operatività effettivamente rilevata sullo stesso;
- svolgere approfondite verifiche sull'origine del patrimonio e dei fondi impiegati nel rapporto continuativo, attraverso un processo articolato che prenda in considerazione, diversi fattori tra cui l'attendibilità delle informazioni a disposizione della Società, tenuto conto della eventuale disponibilità di informazioni economico – patrimoniali prodotte direttamente dal cliente o rilevabili dalla movimentazione del rapporto (es. accredito emolumenti) o reperibili tramite fonti aperte o banche dati pubbliche (es. dichiarazioni dei redditi, atti notarili, dichiarazioni di successione, dichiarazioni/documenti provenienti dal datore di lavoro o da altri intermediari); a tal riguardo, assumono specifica valenza aspetti, quali il grado di conoscenza del cliente e/o l'anzianità della relazione, la coerenza tra il profilo del cliente e la sua situazione economico-patrimoniale;
- condurre in modo frequente la verifica e l'aggiornamento delle informazioni anagrafiche.

Il *Team AML* ha altresì l'obbligo di assicurare il monitoraggio costante e rafforzato della clientela nel corso del rapporto continuativo, secondo le procedure e le modalità definite internamente ed in linea con la normativa antiriciclaggio.

In particolare, tale obbligo sussiste in tutti i casi in cui vi è la necessità di monitorare l'operatività del cliente nel tempo nonché laddove vi siano dubbi sulla movimentazione e/o sul comportamento del cliente, anche in seguito all'invio di AVR. Il monitoraggio sul cliente può essere disposto anche in seguito ad una segnalazione proveniente dalla *Funzione Antiriciclaggio* e/o da altro organismo esterno (Cfr. cap. 8 – 9).

Il *Team AML* procede al monitoraggio mediante FCM- *Case Investigations*, la cui frequenza, di seguito riportata, è stabilita dal *Team AML* a seconda del singolo caso e/o in base alle indicazioni della *Funzione Antiriciclaggio*.

SCADENZA MONITORAGGIO
3 mesi
6 mesi
12 mesi

7.4 Processo di Countdown

Il processo di *countdown* è un processo automatizzato che consiste nell'avvio di una serie di iniziative propedeutiche all'aggiornamento e/o conferma dei dati contenuti nella sezione dei dati personali dell'App alla scadenza del profilo di rischio del cliente e/o del documento identificativo.

In particolare, per il profilo di rischio sono previste:

- invio di notifiche in App e via mail a 30, 14, 7 giorni precedenti alla scadenza e il giorno in cui scade il profilo di rischio. Le notifiche successive non vengono inviate se il cliente compila l'ADV o AVR in App;
- dal giorno della scadenza al 89-esimo giorno l'operatività è limitata;
- invio di notifiche al 30-esimo giorno ed al 60-esimo giorno per avvisare il cliente del blocco totale dell'operatività al 90-esimo giorno;
- Dal 90-esimo giorno il cliente potrà accedere all'App solo per aggiornare le informazioni di ADV o AVR.

Qualora il cliente non aggiorni il documento identificativo, la Società provvede:

- invio di notifiche in App e via mail a 3, 2, 1 mese precedente alla scadenza e 14 giorni antecedenti la scadenza del documento identificativo. Le notifiche successive non vengono inviate se il cliente carica documento in corso di validità in App;
- dal giorno della scadenza al 89-esimo giorno l'operatività è limitata;
- invio di notifiche al 30-esimo giorno ed al 60-esimo giorno per avvisare il cliente del blocco totale dell'operatività al 90-esimo giorno;

- Dal 90-esimo giorno il cliente potrà accedere all'App solo per caricare documento in corso di validità.

Non è comunque possibile procedere alla instaurazione di nuovi rapporti continuativi con la Società da parte di clienti con "Documenti identificativi" o "Profilo di Rischio" scaduti.
È compito dell'operatore a cui è affidata, nel concreto, la gestione e l'amministrazione dei rapporti con la clientela valutare eventuali elementi di sospetto nel comportamento del cliente, effettuando, ove presenti, una segnalazione di operazione sospetta alla *Funzione Antiriciclaggio* (Cfr. cap. 12).
Qualora la Società si trovi nella impossibilità oggettiva di effettuare l'adeguata verifica della clientela, si astiene dall'instaurare, eseguire o proseguire il rapporto, procedendo quindi all'estinzione del rapporto continuativo già in essere e valutando se effettuare una segnalazione di operazione sospetta alla *Funzione Antiriciclaggio*.

7.5 Soglie di riferimento e tipo di richieste in AVR con particolare riferimento alla valutazione del rischio

Se necessario, l'operatore della *Perspective Happiness & Services - Team AML* - procede a contattare via mail il cliente laddove si rilevino operazioni potenzialmente sospette, richiedendo le informazioni e/o documenti necessari in base alla casistica.

In particolare, le aree oggetto di controllo sono:

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica della situazione reddituale e patrimoniale	Manuale	Ad Evento	Power Apps; FCM
Verifica corrispondenza tra reddito dichiarato e operatività	Manuale	Ad Evento	Power Apps; FCM
Verifica origine della provvista	Manuale	Ad Evento	Power Apps; FCM
Verifica profilo di rischio attribuito dal sistema	Manuale	Ad Evento	Power Apps; FCM
Verifica dello scopo e natura del rapporto rispetto alla/e operazione/i oggetto di analisi	Manuale	Ad Evento	Power Apps; FCM
Verifica della presenza delle c.d. bad notice da fonti pubbliche e/o da banche dati specialistiche	Manuale	Ad Evento	Power Apps; FCM; SGR; Web; Cerved

La *Perspective Happiness & Services - Team AML* - svolge altresì un controllo periodico nel corso del rapporto continuativo per mantenere aggiornato il profilo di rischio del cliente ed individuare elementi di incongruenza che possono costituire anomalie rilevanti ai fini di specifici adempimenti.
Il controllo costante si esercita attraverso l'esame della complessiva operatività del cliente, mediante l'acquisizione di informazioni in sede di verifica o aggiornamento delle informazioni fornite.

Il controllo costante è effettuato con una periodicità che dipende dal profilo di rischio associato al cliente. In particolare, per i clienti in fascia di rischio:

- IRRILEVANTE, è effettuato ogni 48 mesi;
- BASSO, è effettuato ogni 36 mesi;
- MEDIO, è effettuato ogni 24 mesi;
- ALTO, è effettuato ogni 12 mesi.

Il processo di aggiornamento della profilatura è gestito informaticamente attraverso FCM. Lo strumento informatico utilizzato consente di calcolare la data di scadenza del profilo, sulla base della data dell'ultimo aggiornamento anagrafico e del relativo livello di rischio di riciclaggio a seconda della fascia di rischio e di effettuare il ricalcolo automatico della data di scadenza del profilo di rischio, a seguito della variazione del relativo livello, assumendo come riferimento la data dell'avvenuta variazione e del tempo trascorso dall'ultimo aggiornamento.
Indipendentemente dalle scadenze sopra indicate, l'aggiornamento dei dati e delle informazioni raccolte in sede di profilatura della clientela è richiesto alla scadenza del documento di identità o alla scadenza del profilo di rischio, nonché ogniqualvolta l'operatore incaricato rilevi che non sono più attuali le informazioni precedentemente acquisite.

7.6 Gestione soggetti collegati

La *Perspective Happiness & Services - Team AML* - nell'ottica di rafforzare e irrobustire i controlli sulla clientela, ha previsto di svolgere dei controlli oltre che sul cliente principale oggetto di analisi anche sul/i soggetto/i collegato/i cliente/i di Flowe. In particolare, le aree oggetto di controllo sono le medesime descritte al paragrafo precedente (cfr. par. 7.5).

A tal proposito, sono stati stabiliti dei parametri necessari al fine di comprendere quando risulta necessario procedere con l'invio di AVR anche per il soggetto collegato.

Per il/i soggetto/i collegato/i si procede con invio di AVR, comunque, nel caso in cui quest'ultimo abbia fatto scattare in FCM un *alert profile*, in quanto le transazioni effettuate sul proprio conto di pagamento superano soglie/parametri stabiliti, e/o sia pervenuto un *alert* esogeno (es. richieste A.G.). In caso il/i soggetto/i collegato/i non abbia fatto scattare alcun *alert* si procede ad AVR solo nei seguenti casi:

REDDITO DICHIARATO	OPERATIVITÀ	INVIO AVR	FREQUENZA CONTROLLO	APPLICATIVO
0	Se l'operatività cumulata in 12 mesi è > 1.000 €	Si procede con invio AVR anche per il soggetto collegato	Ad Evento	PowerApps; FCM
Fino a 15K	Se l'operatività cumulata in 12 mesi è > 5.000 €	Si procede con invio AVR anche per il soggetto collegato	Ad Evento	PowerApps; FCM
Da 15K a 30K	Se l'operatività cumulata in 12 mesi è > 10.000 €	Si procede con invio AVR anche per il soggetto collegato	Ad Evento	PowerApps; FCM
Da 30K a 45K	Se l'operatività cumulata in 12 mesi è > 20.000 €	Si procede con invio AVR anche per il soggetto collegato	Ad Evento	PowerApps; FCM
Da 45K a 70K	Se l'operatività cumulata in 12 mesi è > 30.000 €	Si procede con invio AVR anche per il soggetto collegato	Ad Evento	PowerApps; FCM
Oltre 70K	Se l'operatività cumulata in 12 mesi è > 40.000 €	Si procede con invio AVR anche per il soggetto collegato	Ad Evento	PowerApps; FCM

8 Gestione delle richieste provenienti da altre Strutture

Si riportano di seguito le modalità di gestione del *Team AML* della *Perspective Happiness & Services* delle richieste provenienti da altre Strutture di Banca Mediolanum e di Flowe.

8.1 Richieste provenienti dalla Funzione Antiriciclaggio e/o dal Responsabile Antiriciclaggio

La *Perspective Happiness & Services - Team AML* - su richiesta della *Funzione Antiriciclaggio* e/o dal Responsabile Antiriciclaggio procede allo svolgimento di approfondimenti nonché di AVR su clienti indicati. Dopo essere stato attivato, il *Team*

AML della *Perspective Happiness & Services* procede alla fase di istruzione della pratica propedeutica alla raccolta di tutte le informazioni utili a qualificare il cliente o il comportamento anomalo dello stesso.
In tale ambito, l'operatore procede, in particolare, all'acquisizione ed all'approfondimento dei dati anagrafici del cliente e di quelli forniti dal medesimo in sede di adeguata verifica, controllando, allo stesso tempo, la presenza di analisi e/o segnalazioni pregresse sul medesimo, il relativo profilo di rischio di riciclaggio, la presenza di notizie o pregiudizievoli sulle banche dati in uso e su fonti aperte, nonché eventuali richieste di informazioni o provvedimenti censiti nel *database* Atti Giudiziari. L'operatore provvede, altresì, ad analizzare la movimentazione effettuata sul rapporto di conto corrente e gli eventuali legami con altri soggetti nonché ad approfondire le caratteristiche, l'entità e la natura della/e operazione/i in esame, interfacciandosi anche con il *Team Account Monitoring* della *Perspective Happiness & Services*.

8.2 Segnalazioni provenienti da altre strutture di Flowe

La *Perspective Happiness & Services - Team AML* - può avviare l'attività di approfondimento del cliente anche in seguito ad una segnalazione di altre strutture operative di Flowe che gestiscono nel concreto i rapporti con la clientela, nello specifico a titolo esemplificativo:

- *Il Team Customer Interaction* della *Perspective Happiness & Services*, che in seguito al contatto con il cliente percepisce una qualsiasi anomalia in ordine all'identificazione, alle dichiarazioni di *onboarding*, sull'operatività ecc.
- Il *Team Reclami* della *Perspective Happiness & Services*, che procede a segnalare al *Team AML* della *Perspective Happiness & Services* i casi di reclamo, per valutare eventuali soggetti coinvolti in richieste dell'Autorità o in attività di controllo AML.

Per tutti i casi in cui il *Team Account Monitoring* della *Perspective Happiness & Services* rileva o viene coinvolto per presunte e/o sospette frodi (cfr. "Procedura Operativa di monitoraggio e gestione conto ai fini antifrode").

9 Gestione degli Atti Giudiziari

La *Perspective Happiness & Services - Team AML* - attraverso il supporto dell'Ufficio Atti Giudiziari, fornisce assistenza nella gestione di Atti Giudiziari a seguito di formali richieste pervenute dagli Organi Investigativi e/o dall'Autorità Giudiziaria (di seguito A.G.), al fine di effettuare le necessarie verifiche e predisporre le opportune risposte, nel rispetto della riservatezza prevista dagli artt. 45 e 46 del D.Lgs. 231/2007. Qualora emergessero elementi di sospetto dalle richieste pervenute, il *Team AML* della *Perspective Happiness & Services* effettua senza indugio AVR e di conseguenza laddove persiste il sospetto, una segnalazione alla *Funzione Antiriciclaggio*, per le opportune valutazioni di competenza.

In particolare, le richieste provenienti dagli Organi Investigativi e/o dall'Autorità Giudiziaria sono:

- Richieste generiche di indagine dell'A.G.
- Pignoramenti
- Pignoramenti massivi (ex art. 72 bis. dpr 602/73)
- Sequestri
- Accertamenti Fiscali
- Fallimenti

ATTIVITÀ	TIPO ATTIVITÀ	FREQUENZA ATTIVITÀ	APPLICATIVO
Richieste generiche di indagine dell'A.G. • trasmettere per il/i cliente/i indicato/i nella richiesta la documentazione richiesta (documenti di identità, lista movimenti, estratto conto ecc.) • verificare l'operatività presente sul conto dall'apertura alla data della richiesta • procedere con invio AVR laddove si dovessero riscontrare operazioni sospette • procedere se necessario con segnalazione alla *Funzione Antiriciclaggio* • procedere ad aprire un *case investigations* • apporre il dato aggiuntivo in FCM per il ricalcolo del profilo di rischio	Manuale	Ad Evento	Legal Doc; PowerApps; T24; GUI; FCM
Pignoramenti • procedere con apposizione di blocchi temporanei per i soli addebiti sul conto, e blocco totale dell'accesso in App e dell'utilizzo della carta, fino ad indicazioni diverse dell'Autorità • verificare se vi siano accrediti riconducibili ad emolumenti • controllare ed apporre blocco preventivo a eventuali carte prepagate del minore legate al conto • procedere ad aprire un *case investigations*	Manuale	Ad Evento	Power Apps; T24; GUI; FCM

• apporre il dato aggiuntivo in FCM per il ricalcolo del profilo di rischio			
Pignoramenti massivi • procedere con apposizione di blocchi temporanei per i soli addebiti sul conto, e blocco totale dell'accesso in App e dell''utilizzo della carta, fino ad indicazioni diverse dell'Autorità • verificare se vi siano accrediti riconducibili ad emolumenti • controllare ed apporre blocco preventivo a eventuali carte prepagate del minore legate al conto • procedere ad aprire un case investigations • apporre il dato aggiuntivo in FCM per il ricalcolo del profilo di rischio Se non vi sono dati sufficienti ad identificare il soggetto, il *Team AML* della *Perspective Happiness & Service*s, provvederà in autonomia a scrivere una pec al soggetto notificante dando atto di tale carenza ai fini dell'evasione della richiesta	Manuale	Ad Evento	Power Apps; T24; GUI; FCM
Sequestri • procedere con apposizione di blocchi temporanei per accrediti e addebiti sul conto, e blocco totale dell'accesso in App e dell''utilizzo della carta, fino ad indicazioni diverse dell'Autorità • procedere altresì con blocco di eventuali automatismi/domiciliazioni/RID • procedere al blocco delle eventuali carte prepagate relative ad eventuali minori	Manuale	Ad Evento	Power Apps; T24; GUI; FCM

associati al soggetto oggetto di sequestro • procedere ad aprire un *case investigations* • apporre il dato aggiuntivo in FCM per il ricalcolo del profilo di rischio • SOLO in caso di devoluzione al FUG, sarà attivato il *Team BO* per processare in T24 la richiesta			
Accertamenti Fiscali • trasmettere per il/i cliente/i indicato/i nell'atto la documentazione richiesta dall'A.G. (dati anagrafici, Modulo di Apertura Rapporto, lista movimentazione conto ecc.) • compilare e trasmettere file CSV per l'applicativo COMMAWEB • procedere ad aprire un *case investigations* • apporre il dato aggiuntivo in FCM per il ricalcolo del profilo di rischio	Manuale	Ad Evento	Power Apps; T24; GUI; FCM
Fallimento • procedere con apposizione di blocchi temporanei per accrediti e addebiti sul conto, e blocco totale dell'accesso ie dell'utilizzo della carta, fino ad indicazioni diverse dell'Autorità • procedere altresì con blocco di eventuali automatismi/domiciliazioni/RID • procedere ad aprire un *case investigations* • apporre il dato aggiuntivo in FCM per il ricalcolo del profilo di rischio	Manuale	Ad Evento	Power Apps; T24; GUI; FCM

10 Aggiornamento posizione anagrafica - AUI

Una volta confermata l'apertura del conto di pagamento la posizione anagrafica del cliente viene automaticamente censita (a T+1) nel Gestionale a supporto delle segnalazioni di Vigilanza.

10.1. Monitoraggio e gestione scarti/disallineamenti posizioni anagrafiche (post apertura conto)

La *Perspective Happiness & Services* per il tramite dell'*outsourcer*, *Team Operations Flowe* di Banca Mediolanum, giornalmente accede alla piattaforma Easybox e verifica la presenza di posizioni per le quali in automatico la piattaforma ha rilevato anomalie/incongruenze relativamente ai dati/informazioni fornite in App dal cliente in fase di *onboarding* o successivamente e poi confluite, con *batch*, appunto in Easybox ai fini delle differenti tipologie di segnalazioni che la Società è tenuta a predisporre in conformità alla normativa di vigilanza di riferimento.
Per agevolare questa attività, Easybox mette a disposizione dell'operatore un cruscotto che riassume le anomalie/incongruenze sulle quali è necessario intervenire. L'operatore procede alla lavorazione di ogni singola posizione/NDG entrando nella relativa "anagrafica" e interviene sulle sezioni "anomale" evidenziate. Se necessario, verifica i documenti del cliente oppure interroga l'anagrafica cliente in T24.
L'operatore può sanare eventualmente l'errore tramite una disamina dei documenti usati dal cliente nella fase di *onboarding* o successivamente. Questi documenti sono archiviati nel *Repository* documentale dell'*outsourcer* InfoCert, denominato Legal Doc. L'operatore del *Team Operations Flowe* di Banca Mediolanum, pertanto, accede a questo *Repository* tramite il codice fiscale del cliente, recupera i documenti e procede a una disamina degli stessi per acquisire le informazioni corrette e/o mancanti nella Piattaforma, necessarie per sistemare l'anomalia riscontrata da Easybox.
Per la correzione delle posizioni anomale, l'operatore può effettuare l'inserimento *ex novo* o la correzione dei dati errati/mancanti.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica presenza anomalie su cruscotto anagrafiche / rapporti	Manuale	Giornaliero	Piattaforma Easybox; T24; Legal Doc
Sulle anomalie segnalate, verifica documenti identità del cliente per sistemazione dati mancanti / errati (a titolo esemplificativo e non esaustivo):	Manuale	Giornaliero	Piattaforma Easybox; T24; Legal Doc

• verifica correttezza / completezza CAP e CAB; • verifica nome comune / paese di residenza / comune di nascita (es. Reggio di Calabria vs. Reggio Calabria); • verifica corrispondenza n. documento; • verifica data emissione documento; • verifica indirizzo di residenza (se non risulta in Italia); • verifica correttezza CF.			
Report a supporto	Manuale	Giornaliero	Piattaforma Easybox; T24; Legal Doc
Cruscotto anomalie rilevate da Easybox	Manuale	Giornaliero	Piattaforma Easybox; T24; Legal Doc

10.1.1 Quadratura alimentazione AUI

Giornalmente viene effettuata, da parte dell'*outsourcer Team Operations Flowe* di Banca Mediolanum, una verifica sulla completezza dei dati confluiti su Easybox (anagrafiche soggetti, anagrafiche rapporti, estinzioni, movimenti).
Qualsiasi discrepanza viene integrata manualmente dagli operatori *Team Operations Flowe* di Banca Mediolanum. In caso di anomalia massiva, le attività vengono gestite dalla *Perspective Happiness & Services - Team Monitoraggio Segnalazioni* - coinvolgendo direttamente i fornitori impattati.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica che il file (prodotto attraverso il sistema di *Core Banking*) relativo alle anagrafiche sia stato recepito e caricato nella piattaforma Easybox	Manuale	Giornaliero	Piattaforma Easybox; T24
Verifica che il file (prodotto attraverso il sistema di *Core Banking*) contenga tutte le aperture e le estinzioni della settimana precedente	Manuale	Settimanale	Piattaforma Easybox; T24

(incluso il *weekend* se si tratta del file del lunedì)			
Verifica che il file (prodotto attraverso il sistema di *Core Banking*) relativo alle transazioni di importo >= 5.000€ sia stato recepito e caricato nella piattaforma Easybox	Manuale	Giornaliero	Piattaforma Easybox; T24
Verifica che il file (prodotto attraverso il sistema di *Core Banking*) contenga tutte le transazioni da segnalare della settimana precedente (incluso il *weekend* se si tratta del file del lunedì)	Manuale	Settimanale	Piattaforma Easybox; T24

11 GESTIONE DEI BLOCCHI

La *Perspective Happiness & Services - Team AML* - a seguito delle puntuali e attente verifiche effettuate sul conto di pagamento del cliente, sulla documentazione fornita, nonché sui comportamenti eventualmente considerati sospetti o reticenti in sede di adeguata verifica rafforzata, può disporre diverse tipologie di blocchi ai servizi e prodotti del cliente.
In particolare, i blocchi che possono essere apposti possono essere così distinti:

- blocco accesso in App mediante Power Apps;
- blocco conto mediante T24;
- blocco carta mediante GUI.

La Perspective Happiness & Services – Team AML – procede a disporre i tre suddetti blocchi quando:

- quando richiesto dagli Organi Investigativi e/o dall'Autorità Giudiziaria in caso di pignoramento, sequestro, richieste A.G., per soggetti considerati potenzialmente sospetti;
- in caso di mancato riscontro ad adeguata verifica rafforzata;
- a seguito di verifica preventiva sui "*selfie*" già presenti in database – Face Manager in *onboarding*. In particolare, a seguito della verifica bloccante che rifiuta il *prospect* qualora il suo *selfie* effettua un *match* con un altro *selfie* già presente nel nostro database, con soglia > 80%, l'operatore del *Team AML* della *Perspective Happiness & Services* procederà ad approfondimento sul cliente in *match*, apponendo un blocco preventivo (in questo caso anche sul conto e sulla carta).

Per tutti i casi in cui viene coinvolto il *Team Account Monitoring* della *Perspective Happiness & Services* per l'apposizione di eventuali blocchi si rimanda alla "Procedura Operativa di monitoraggio e gestione conto ai fini antifrode".

11.1 Blocco Accesso in App

Il blocco "accesso in App", effettuato mediante il gestionale Power Apps - Fan Base, è un blocco che impedisce al cliente di accedere all'App, scaricata sul dispositivo mobile, con cui si è registrato in fase di apertura del conto.

CONTROLLO	TIPO ATTIVITÀ	FREQUENZA ATTIVITÀ	APPLICATIVO
L'operatore del *Team AML* della *Perspective Happiness & Services* nella posizione del cliente crea un "*claim* AML" di tipo "*Block User*"	Manuale	Ad Evento	Power Apps
Inserisce le note al fine di condividere le informazioni con tutta la *Perspective Happiness & Services* (laddove non coperte da riservatezza)	Manuale	Ad Evento	Power Apps
Attiva il blocco ("*Block on sign In*")	Manuale	Ad Evento	Power Apps
Verifica la corretta ed avvenuta apposizione del blocco sul cliente in oggetto	Manuale	Ad Evento	Power Apps
Appurata la verifica bloccante in *onboarding - Face Manager* (cfr. "Procedura onboarding cliente ed apertura conto di pagamento"), l'operatore del *Team AML* della *Perspective Happiness & Services* procederà ad approfondimento sul cliente in *match*, apponendo un blocco preventivo.	Manuale	Ad Evento	Power Apps

11.2 Blocco Conto

Il blocco "conto", effettuato mediante il gestionale Temenos - T24, è un blocco, apposto dal *Team AML* della *Perspective Happiness & Services*, che impedisce al cliente di disporre

delle somme presenti sul conto. In questi casi il cliente può accedere all'App ed utilizzare la carta di debito ma tutte le operazioni disposte sono automaticamente rifiutate dal Sistema di *Core Banking* in quanto il conto risulta di fatto inibito.

Il gestionale T24, per garantire un più alto livello di sicurezza del processo, prevede l'apposizione di blocco attraverso una doppia approvazione.

CONTROLLO	TIPO ATTIVITÀ	FREQUENZA ATTIVITÀ	APPLICATIVO
L'operatore del *Team AML* della *Perspective Happiness & Services* inserisce la tipologia di blocco c.d. "*Posting Restriction*": • solo in addebito (blocco 1) • solo in accredito (blocco 2) • totale (blocco 3)	Manuale	Ad Evento	T24
Inserisce le note al fine di condividere le informazioni con tutta la *Perspective Happiness & Services* (laddove non coperte da riservatezza)	Manuale	Ad Evento	T24
Inserisce la data del blocco	Manuale	Ad Evento	T24
Un secondo operatore del *Team AML* procede poi con approvazione del blocco precedentemente inserito	Manuale	Ad Evento	T24

11.3 Blocco Carta

Il blocco "carta", effettuato mediante il gestionale SIA Crystal Gate (GUI) è un blocco che impedisce al cliente l'utilizzo della carta (sia fisica che virtuale) e di effettuare tutte le operazioni ad essa collegata.

Dopo aver selezionato il cliente da bloccare, l'operatore del *Team AML* della *Perspective Happiness & Services*, applica il blocco solo alla carta di debito attiva in quel momento.

CONTROLLO	TIPO ATTIVITÀ	FREQUENZA ATTIVITÀ	APPLICATIVO
L'operatore del *Team AML* della *Perspective Happiness & Services* seleziona la funzionalità dedicata "*Change*	Manuale	Ad Evento	GUI

Account Status" modificando lo status da *Open* a *Generic Bank Block Temporary (KD)*			
L'operatore del *Team AML* della *Perspective Happiness & Services* verifica la corretta ed avvenuta apposizione del blocco sul cliente in oggetto	Manuale	Ad Evento	GUI

12 PROCEDURA OPERATIVA DEL PROCESSO DI SEGNALAZIONE OPERAZIONI SOSPETTE (SOS)

La segnalazione delle operazioni sospette alla U.I.F. della Banca d'Italia costituisce uno dei pilastri fondamentali della normativa in materia di antiriciclaggio e contrasto al finanziamento del terrorismo. In particolare, gli obblighi di segnalazione delle operazioni sospette sono regolamentati dal Capo III – Obblighi di segnalazione - dell'art. 35 del D. Lgs. 231/2007 (cfr. Regolamento del processo di Segnalazione Operazioni Sospette -SOS).

12.1 Attori coinvolti

Il processo di segnalazione delle operazioni sospette prevede il coinvolgimento degli organi e delle strutture aziendali della Società.

12.1.1 Responsabile Antiriciclaggio e Delegato alla segnalazione di operazioni sospette

Il Delegato alla Segnalazione delle Operazioni Sospette di Flowe:

- ha libero accesso ai flussi informativi diretti agli Organi Aziendali e alle strutture coinvolte nel contrasto del riciclaggio e del finanziamento del terrorismo;
- può acquisire ogni informazione utile dalla struttura che svolge il primo livello di analisi;
- può consentire, con le indispensabili cautele di riservatezza e senza far menzione del nominativo del segnalante, che i Responsabili delle strutture aziendali abbiano conoscenza dei nominativi dei clienti segnalati, anche attraverso l'utilizzo di idonee basi informative, stante la particolare pregnanza che tale informazione può rivestire per l'accettazione di nuovi clienti ovvero per la valutazione dell'operatività di clienti preesistenti;
- gestisce, per quanto di competenza, i rapporti con la UIF e corrisponde tempestivamente alle eventuali richieste di approfondimento provenienti dalla medesima;

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

12.1.2 Strutture operative con particolare riferimento alla Perspective Happiness & Services

I *Team* interni alle *Perspective* sono i primi responsabili del processo di gestione dei rischi antiriciclaggio in quanto amministrano e gestiscono i rapporti con la clientela. Nel corso dell'operatività giornaliera tali strutture sono chiamate, infatti, a identificare, misurare o valutare, monitorare, attenuare i rischi antiriciclaggio derivanti dall'ordinaria attività aziendale nonché attivare le opportune azioni di *escalation* in conformità con il processo di gestione dei rischi antiriciclaggio.
Nell'ambito delle strutture operative della Società, assume particolare rilevanza, la *Perspective Happiness & Services - Team AML*, che costituisce il primo livello del processo di gestione dei rischi.
Già in fase di acquisizione del *prospect*/cliente è possibile procedere con l'avvio della segnalazione di operazioni sospette nel caso in cui ad es. si rileva un esito positivo del *Face manager*.
Il *Team AML* della *Perspective Happiness & Services*, inoltre, procede ad analizzare e monitorare giornalmente il transato dei clienti attraverso diversi *INPUT* (*alert profile*, richieste dell'A.G., segnalazioni interne, ecc.).
Procede ad analizzare il conto del cliente attenzionato attendendosi ad alcuni parametri, come la:

- conformità del reddito dichiarato con la movimentazione;
- provenienza dei fondi ed origine della provvista;

- coerenza con lo storico del cliente.

Nel caso di operazioni sospette ritenute illecite ai fini antiriciclaggio, il *Team AML* della *Perspective Happiness & Services* che ha gestito le attività di analisi, raccoglie tutte le informazioni necessarie per procedere all'avvio dell'iter della SOS all'Unità di Informazione Finanziaria (UIF) della Banca d'Italia, tramite l'applicativo Workflow. In particolare, inserisce all'interno del *dossier*:

- il dettaglio della movimentazione sospetta, risalente al giorno della prima verifica sul cliente;
- il dettaglio della movimentazione sospetta, risalente al giorno del caricamento del *dossier*, al fine di verificare se dal giorno della prima verifica al caricamento del *dossier* ci siano ulteriori operazioni sospette;
- una scheda contenente i dati anagrafici del cliente ed i riferimenti del conto di pagamento Flowe;
- cronologia delle mail di AVR inviata, con relativi moduli compilati dal cliente;
- documenti di identità, solo se vi siano fondati dubbi sulla loro veridicità;
  qualora l'avvio dell'analisi del cliente provenga da segnalazione esogena, si allega copia dell'atto/provvedimento degli Organi Investigativi e dell'Autorità Giudiziaria.

Una volta completo, il *dossier* viene automaticamente inoltrato, tramite il Workflow, alla *Funzione Antiriciclaggio* di Banca Mediolanum che analizza ed istruisce la presunta operazione sospetta inoltrata dal *Team AML* della *Perspective Happiness & Services* e la sottopone al Delegato alla Segnalazione di Operazioni Sospette, per la valutazione in merito all'eventuale trasmissione alla UIF delle segnalazioni ritenute fondate.
In caso di conferma da parte del Delegato SOS, la *Funzione Antiriciclaggio* si occupa delle attività di segnalazione delle operazioni secondo le modalità previste dalla normativa antiriciclaggio. Il Delegato SOS può valutare se, a fronte delle segnalazioni di operazioni sospette pervenutegli, innalzare o diminuire il profilo di rischio dei soggetti correlati all'operatività analizzata, indipendentemente dall'esito conclusivo delle stesse, tenendo traccia delle motivazioni sottostanti.

Inoltre, all'interno della *Perspective Happiness & Services* - il *Team Account Monitoring* - ha l'obbligo di segnalare operazioni sospette alla *Funzione Antiriciclaggio* con le modalità previste nella seguente procedure, nei casi in cui nello svolgimento della loro attività di monitoraggio di presunte e/o sospette frodi, rilevino operatività sospetta (per le casistiche di segnalazione SOS alla *Funzione Antiriciclaggio* da parte del *Team Account Monitoring* della *Perspective Happiness & Services* si rimanda alla "Procedura Operativa di monitoraggio e gestione conto ai fini antifrode".

In ultimo, solo dopo aver proceduto al caricamento del *dossier* SOS sul Workflow, la *Perspective Happiness & Services - Team AML* - procede alla creazione di un *case* denominato "*Suspicious customers*" in FCM. Laddove la *Funzione Antiriciclaggio* procede con la trasmissione del *dossier* SOS alla UIF, appone il dato aggiuntivo in FCM.

12.1.3 Strutture aziendali di Banca Mediolanum S.p.A.

Con riferimento all'attività di segnalazione delle operazioni sospette, Flowe si avvale della struttura preposta della *Funzione Antiriciclaggio* di Banca Mediolanum, per quanto attiene la lavorazione e gestione delle segnalazioni di operazioni sospette, ivi compreso l'archiviazione delle pratiche e l'invio delle segnalazioni tramite abilitazione al portale Infostat-UIF.

12.1.4 Attori esterni

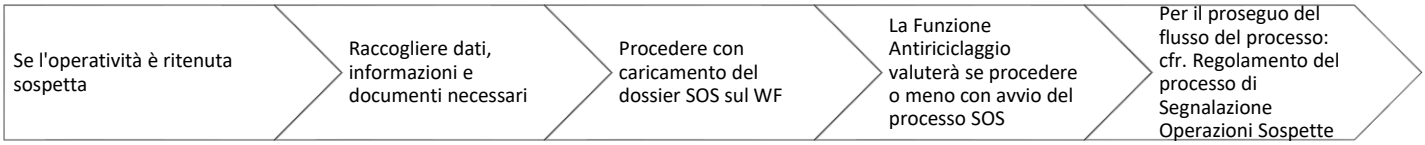
Di seguito, sono descritti i ruoli e le responsabilità degli attori esterni che partecipano al processo.

- **CSF (Comitato di Sicurezza Finanziaria)**: è l'Autorità competente responsabile di monitorare, in Italia, il funzionamento del sistema di prevenzione e di sanzioni del finanziamento del terrorismo e del riciclaggio. È presieduto dal Direttore generale del Tesoro e composto da rappresentanti del Ministero dell'Economia e delle Finanze, del Ministero degli Affari Esteri, del Ministero dell'Interno, del Ministero della Giustizia, della Banca d'Italia, della Commissione Nazionale per le Società e la Borsa, dell'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo, dell'Unità di Informazione Finanziaria, della Guardia di Finanza, della Direzione Investigativa Antimafia, dell'Arma dei Carabinieri e della Direzione nazionale antimafia. Ai fini dello svolgimento dei compiti riguardanti il congelamento delle risorse economiche, il CSF è integrato dall'Agenzia del demanio. Ai fini della lotta alla proliferazione delle armi di distruzione di massa, il CSF è integrato dal Ministero dello Sviluppo Economico e dall'Agenzia delle Dogane.
- **MEF (Ministero dell'Economia e delle Finanze)**: è responsabile delle politiche di prevenzione dell'utilizzo del sistema finanziario e di quello economico per fini di riciclaggio dei proventi di attività criminose e/o di finanziamento del terrorismo. In tali materie, promuove la collaborazione tra l'UIF, le Autorità di Vigilanza di Settore, gli ordini professionali, la DIA e la Guardia di Finanza. Sentito il Comitato di Sicurezza Finanziaria, individua, con proprio decreto, una lista di paesi in ragione di rischio di riciclaggio e di finanziamento di terrorismo ovvero della mancanza di un adeguato scambio di informazioni anche in materia fiscale.
- **NSPV (Nucleo Speciale di Polizia Valutaria della Guardia di Finanza)**: è costituito all'interno del Corpo della Guardia di Finanza ed opera in prima linea sul fronte della lotta al riciclaggio sia come organismo investigativo di polizia, sia come organo amministrativo di controllo del settore dell'intermediazione finanziaria, unitamente alla Banca d'Italia e alla DIA.
- **DIA (Direzione Investigativa Antimafia)**: trasmette alle Autorità di vigilanza di settore le violazioni degli obblighi di cui al decreto antiriciclaggio riscontrate nell'esercizio delle sue attribuzioni ed effettua approfondimenti investigativi, attinenti alla criminalità organizzata, delle segnalazioni di operazioni sospette trasmesse dalla UIF.
- **UIF (Unità di Informazione Finanziaria per l'Italia)**: riceve e acquisisce informazioni riguardanti ipotesi di riciclaggio e di finanziamento del terrorismo, ne effettua l'analisi finanziaria e, su tali basi, ne valuta la rilevanza ai fini della trasmissione agli organi

investigativi (Nucleo speciale di polizia valutaria della Guardia di Finanza -NSPV e Direzione investigativa antimafia-DIA) e della collaborazione con l'Autorità Giudiziaria. Esercita le proprie funzioni in piena autonomia e indipendenza. In attuazione di tali principi, la Banca d'Italia disciplina con un regolamento l'organizzazione e il funzionamento della UIF, ivi compresa la riservatezza delle informazioni acquisite. La Banca d'Italia attribuisce alla UIF mezzi finanziari e risorse idonee ad assicurare l'efficace perseguimento dei suoi fini istituzionali (cfr. Regolamento del processo di Segnalazione Operazioni Sospette - SOS).

12.2 Il processo delle segnalazioni delle operazioni sospette

Le diverse fasi del processo di segnalazione delle operazioni sospette possono essere così riassunte:



12.2.1 Segnalazioni Esogene

L'avvio del processo segnaletico può scaturire dalle richieste ricevute da altre strutture, tra cui l'Ufficio Atti Giudiziari, dal *Team Customer Interaction* della *Perspective Happiness & Services*, dalla *Funzione Antiriciclaggio*. In questo caso, la *Perspective Happiness & Services - Team AML* - provvede, laddove ritenuto necessario, a raccogliere documenti e dati relativi al cliente e a caricare *dossier* sul Workflow. Sarà la *Funzione Antiriciclaggio* ad effettuare gli approfondimenti di competenza e sottoporre al Delegato SOS le segnalazioni da valutare ai fini dell'eventuale inoltro alla UIF.

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

12.2.2 Segnalazioni Endogene

La *Perspective Happiness & Services - Team AML* – carica il *dossier* SOS sul Workflow, senza ritardo, sicuramente nei seguenti casi:

- cliente reticente a fornire delucidazioni e/o documentazione sulla operatività rilevata (mancato riscontro ad AVR) in caso di presenza di operatività almeno pari a 10.000 euro e/o in presenza di ulteriori elementi/indici di anomalia;
- ricezione atto giudiziario (fatto salvo pignoramenti) e denuncia;
- cliente che, a fronte delle verifiche, risultasse avere documentazione falsa;
- cliente che, a fronte delle verifiche, risultasse avere pregiudizievoli e/o protesti.

La *Perspective Happiness & Services - Team AML* – valuta, inoltre, il caricamento del *dossier* SOS sul Workflow in caso di impossibilità oggettiva di procedere con adeguata verifica del *prospect*/cliente (es: mancata risposta ad AVR).

Per i casi in cui il *Team Account Monitoring* della *Perspective Happiness & Services* è obbligato a procedere con segnalazione di operazione sospetta si rimanda alla "Procedura Operativa di monitoraggio e gestione conto ai fini antifrode".

12.3 Sistemi automatici di rilevazione

La *Perspective Happiness & Services - Team AML* - provvede ad analizzare gli "inattesi" (*alert profile* - sezione *Batch Alert manager*) che emergono dal sistema FCM Temenos. Tali sistemi rilevano giornalmente, settimanalmente e mensilmente possibili anomalie, individuate in funzione di specifiche regole messe a punto e costantemente aggiornate, in conformità agli indicatori di anomalia emanati dalla Banca d'Italia ed agli schemi rappresentativi di comportamenti anomali pubblicati, tempo per tempo, dalla UIF. Rientrano tra i sistemi automatici di rilevazione anche le analisi dei rilievi generali, pervenuti tramite il portale Infostat-UIF, relativi al flusso S.AR.A.

13 Recesso del conto

In sede di adeguata verifica rafforzata tutti i clienti, le cui operazioni sono ritenute illecite o sospette rispetto ai principi cardini della Società e più in generale alla Normativa Antiriciclaggio, possono essere sottoposti al vaglio del responsabile della *Perspective Happiness & Services* per valutazione del recesso.
In particolare, l'operatore del *Team AML* svolte le opportune verifiche sul cliente, predispone l'avvio del processo di recesso unilaterale del contratto stipulato (a 60 giorni o immediato), che dovrà essere valutato dal responsabile della *Perspective Happiness & Services*. Per dettagli circa l'attività successiva all'avvio del suddetto processo si rimanda alla "Procedura operativa estinzione conto".
Si precisa che la *Perspective Happiness & Services – Team AML* – anche nel caso di suggerimento sia della *Funzione Antiriciclaggio* sia dell'Ufficio Atti Giudiziari, può predisporre l'avvio del processo di recesso unilaterale del contratto.

Per le casistiche in cui il *Team Account Monitoring* della *Perspective Happiness & Services* valuta la possibilità di recesso del conto si rimanda alla "Procedura Operativa di monitoraggio e gestione conto ai fini antifrode".

13.1 Recesso a 60 giorni

L'operatore del *Team AML* della *Perspective Happiness & Services*, laddove sussistono i presupposti per la richiesta di recesso, sottopone al responsabile della *Perspective Happiness & Services* la posizione del cliente al fine di richiedere l'autorizzazione alla chiusura del rapporto, nonché di valutare l'estinzione d'ufficio per il cliente oggetto di verifica.

RECESSO 60	TIPO ATTIVITÀ	FREQUENZA ATTIVITÀ	STRUMENTO
Valutazione da parte del responsabile della *Perspective Happiness & Services*	Manuale	Ad Evento	Mail interna
L'operatore del *Team AML* della *Perspective Happiness & Service*s notifica il recesso al cliente, mediante mail	Automatico + Manuale	Ad Evento	Power Apps
Provvede ad inserire in Power Apps l'estinzione e ad apporre specifico tag, al fine di condividere le informazioni con tutta la *Perspective Happiness & Services*	Manuale	Ad Evento	Power Apps
Invia raccomandata al cliente laddove il saldo sul conto sia uguale o maggiore di 5 euro, al fine di garantire allo stesso il trasferimento del saldo disponibile su altro suo conto a lui intestato.	Manuale	Ad Evento	Sito Web per raccomandate
Procedere con comunicazione del recesso alla *Funzione Antiriciclaggio*, nel caso di soggetto segnalato	Manuale	Ad Evento	Mail interna

13.2 Recesso Immediato

L'operatore del *Team AML* della *Perspective Happiness & Services*, solo in casi particolari e laddove sussistono i presupposti (es. nel caso di dichiarazioni mendaci sul legame genitoriale), sottopone al responsabile della *Perspective Happiness & Services* la posizione

del cliente al fine di richiedere l'estinzione del rapporto con recesso immediato, fatto salvo che la richiesta non pervenga direttamente dal Delegato alla segnalazione di operazioni sospette in applicazione delle previsioni ex art. 42 del D.Lgs. 231/2007.

RECESSO IMMEDIATO	TIPO ATTIVITÀ	FREQUENZA ATTIVITÀ	STRUMENTO
Valutazione da parte del responsabile della *Perspective Happiness & Services*	Manuale	Ad Evento	Mail interna
L'operatore del *Team AML* della *Perspective Happiness & Services* notifica il recesso al cliente, mediante mail	Automatico-Manuale	Ad Evento	Power Apps
Provvede ad inserire in Power Apps l'estinzione e ad apporre specifico tag, al fine di condividere le informazioni con tutta la *Perspective Happiness & Services*	Manuale	Ad Evento	Power Apps
Invia raccomandata al cliente laddove il saldo sul conto sia uguale o maggiore di 5 euro, al fine di garantire allo stesso il trasferimento del saldo disponibile su altro suo conto.	Manuale	Ad Evento	Sito Web per raccomandate
Procede con comunicazione del recesso alla *Funzione Antiriciclaggio*, nel caso di soggetto segnalato	Manuale	Ad Evento	Mail interna

14 NORMATIVA

14.1 Normativa Interna

La presente procedura fa parte del corpo normativo della Società insieme ai seguenti altri documenti:

- *Policy di prevenzione e sul contrasto al riciclaggio e al finanziamento del terrorismo;*
- *Regolamento del processo di adeguata verifica;*
- *Regolamento del processo di conservazione, controlli e reporting;*
- *Regolamento del processo di gestione delle Persone Esposte Politicamente (c.d. PEP);*
- *Regolamento del processo di Segnalazione Operazioni Sospette (SOS);*
- *Procedura operativa di onboarding cliente e apertura di pagamento;*
- *Procedura operativa estinzione conto;*
- *Procedura operativa di monitoraggio e gestione conto ai fini antifrode.*

14.2 Normativa Esterna

Nel presente capitolo si richiama il contesto normativo nel quale opera la presente Procedura.
Si riportano pertanto, di seguito i principali riferimenti normativi adottati a livello comunitario e nazionale:

Normativa SOS:

Normativa europea
La principale normativa europea è contenuta nei seguenti provvedimenti:

- *Regolamento 2580/2001/CE del Consiglio del 27/12/2001 che stabilisce l'obbligo di congelamento di capitali e il divieto di prestazione di servizi finanziari nei confronti di determinate persone fisiche, persone giuridiche, gruppi o entità che commettono o tentano di compiere atti di terrorismo e di persone giuridiche, gruppi o entità dalle prime controllate;*
- *Regolamento 881/2002/CE del Consiglio del 27/5/2002 che impone specifiche misure restrittive nei confronti di determinate persone ed entità (elencate nell'allegato al Regolamento medesimo) associate a Osama bin Laden, alla rete Al-Qaeda e ai Talebani;*
- *Regolamento 428/2009/CE del Consiglio del 5 maggio 2009 che istituisce un regime comunitario di controllo delle esportazioni, del trasferimento, dell'intermediazione e del transito dei prodotti a duplice uso (modificato da ultimo dal Regolamento Delegato (UE) 2018/1922 del 10 novembre 2018);*
- *Regolamento (UE) n. 753/2011 del Consiglio dell'1 agosto 2011, concernente ulteriori misure restrittive nei confronti di determinate persone, gruppi, imprese e entità "in considerazione della situazione in Afghanistan" e delle decisioni assunte dal "Comitato per le sanzioni" e dal "Comitato 1267" istituiti presso il Consiglio di Sicurezza delle Nazioni Unite*[2]*.*

Normativa nazionale
La normativa primaria italiana è contenuta nei seguenti provvedimenti:

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

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

21) l'applicazione di sanzioni penali e amministrative a carico di chi effettua operazioni di esportazione di beni "dual use" in violazione della normativa.

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

Normativa adeguata verifica:

In ambito comunitario, la principale normativa di riferimento in materia di prevenzione e contrasto del riciclaggio di denaro e del finanziamento del terrorismo è costituita dalla nella Direttiva (UE) 2018/843 del Parlamento Europeo e del Consiglio del 30 maggio 2018 "che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE" (c.d. V° Direttiva Antiriciclaggio) e nella Direttiva 2015/849/CE del Parlamento europeo e del Consiglio del 20/05/2015 "relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione" (c.d. IV° Direttiva Antiriciclaggio).

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

- *D. Lgs. 22/6/2007, n. 109 e successive modifiche ed integrazioni, recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo internazionale;*
- *D. Lgs. 21/11/2007, n. 231 e successive modifiche ed integrazioni, recante l'attuazione della Direttiva 2018/843/CE;*
- *le disposizioni attuative del Decreto Antiriciclaggio in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela, emanate dalle Autorità di Vigilanza di Settore;*
- *la comunicazione della Banca d'Italia del 23 gennaio 2018: "Procedure di adeguata verifica rafforzata sulle Persone Politicamente Esposte".*

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

Normativa archiviazione sostitutiva:

- *D. Lgs 82/2005 Codice dell'Amministrazione Digitale;*
- *Deliberazione CNIPA 19.02.2004 n. 11 (regole tecniche);*
- *D.M del 23 gennaio 2004 (obblighi per i documenti informatici).*