Regolamento del processo di adeguata verifica

Regolamento di processo emesso il 25/10/2023
Owner: Funzione Antiriciclaggio di Gruppo

1. Premessa

Scopo del presente documento è quello di regolamentare le responsabilità, compiti e modalità operative che dovranno essere svolte al fine di uniformare l'operato di Flowe S.p.A. – Società Benefit (di seguito "Società"), facente parte del Gruppo Bancario Mediolanum, alle disposizioni vigenti in materia antiriciclaggio, nonché dare attuazione ai principi richiamati nella Policy sul contrasto al riciclaggio e finanziamento del terrorismo (di seguito anche "Policy") con particolare riferimento:

- alla identificazione e adeguata verifica della clientela;
- alla modalità di individuazione, valutazione e segnalazione delle operazioni sospette;
- agli adempimenti in materia di conservazione della documentazione e delle evidenze richieste dalla normativa;
- ai controlli di secondo livello posti in essere dalla Funzione Antiriciclaggio di Gruppo

Si richiede pertanto a tutto il personale aziendale la puntuale applicazione di tali disposizioni nonché di quelle previste dai documenti di dettaglio (Manuali operativi interni), collegati al presente documento, tempo per tempo vigenti.

CONTESTO DI RIFERIMENTO

Le "*Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo*" emanate dalla Banca d'Italia con provvedimento del 26 marzo 2019 (in seguito anche "Disposizioni"), e successivamente modificate con provvedimento del 1° agosto 2023, prevedono l'obbligo, per la Funzione Antiriciclaggio di Gruppo, di redigere e trasmettere all'organo con funzione di gestione e a quello con funzione di supervisione strategica un documento che definisce dettagliatamente responsabilità, compiti e modalità operative nella gestione del rischio di riciclaggio (cd. manuale antiriciclaggio).
La Funzione Antiriciclaggio di Gruppo pone particolare attenzione: all'adeguatezza dei sistemi e delle procedure interne in materia di obblighi di adeguata verifica della clientela e di conservazione nonché dei sistemi di individuazione, valutazione e segnalazione delle operazioni sospette; all'efficace rilevazione delle altre situazioni oggetto di obbligo di comunicazione nonché all'appropriata conservazione della documentazione e delle evidenze richieste dalla normativa.

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

AMBITO DI APPLICAZIONE

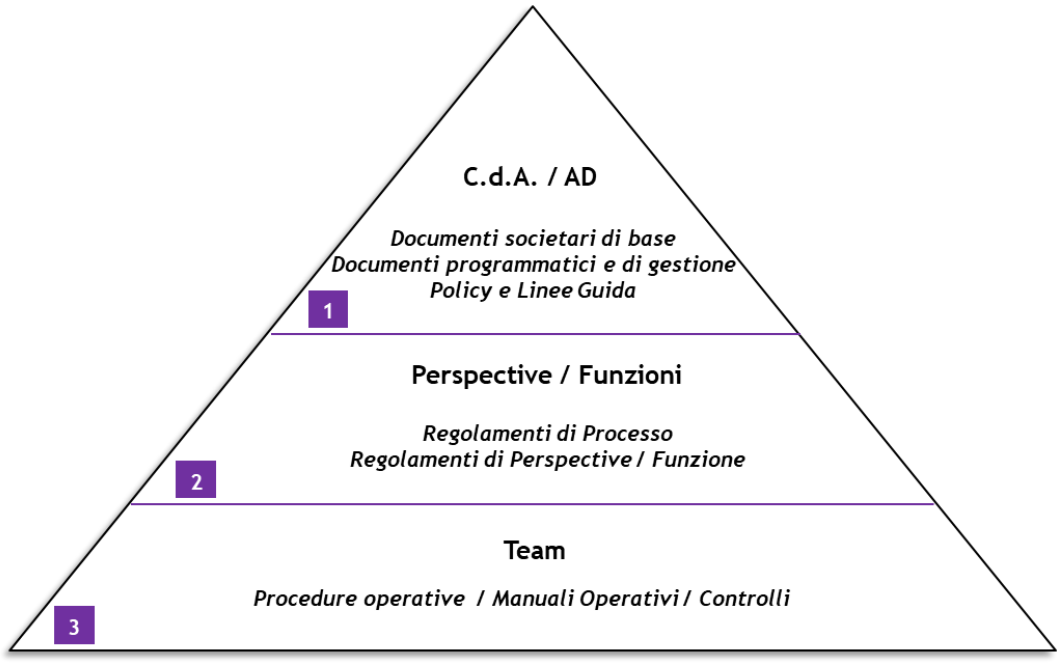
Il presente documento è approvato dal Consiglio di Amministrazione della Società, ed è rivolto a tutti i dipendenti e collaboratori della stessa.

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

OBIETTIVI DEL DOCUMENTO

Il presente Regolamento ha quale principale obiettivo quello di definire:

- le regole di governo, i ruoli e le responsabilità in materia di contrasto ai rischi di riciclaggio e finanziamento del terrorismo da adottare nell'ambito di Società;
- i principi guida, gli assetti organizzativi, le procedure e le interdipendenze per il contrasto ai rischi di riciclaggio e finanziamento del terrorismo. Con riferimento alla *"Policy sulle modalità di redazione, approvazione, diffusione ed aggiornamento della normativa interna",* il presente documento si colloca quindi al secondo livello della piramide documentale richiamata nello schema seguente.



STRUTTURA DEL DOCUMENTO

Oltre al primo capitolo contenente la premessa, la presente policy si compone dei seguenti capitoli, per i quali è fornita, di seguito, una sintetica descrizione delle principali tematiche trattate:

- Capitolo 2: Gli attori coinvolti

  Obiettivo del Capitolo è descrivere e richiamare in modo chiaro ruolo e responsabilità degli attori coinvolti nel processo oggetto del presente documento, definendo modalità di integrazione e coordinamento previste nei casi di processo di carattere interfunzionale.

- capitolo 3: Processo di identificazione e adeguata verifica della clientela Obiettivo del Capitolo è descrivere il processo generato dalle attività di identificazione e adeguata verifica della clientela;
- capitolo 4: Prodotti di terzi collocati dalla Società
  Obiettivo del capitolo è quello di illustrare alcune specificità con riferimento alle disposizioni in materia di adeguata verifica adottate nell'ambito del collocamento dei prodotti di terzi;

- capitolo 5: Normativa di riferimento
  Obiettivo del capitolo è di descrivere il contesto normativo di riferimento in ambito antiriciclaggio e contrasto al finanziamento del terrorismo.

2. Gli attori coinvolti

Gli attori, ovvero le unità organizzative aziendali coinvolte a vario titolo nel processo di "adeguata verifica" sono di seguito richiamati, con evidenza esclusivamente del ruolo specificatamente attribuito nel processo medesimo.

CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione:

- approva un sistema dei controlli interni organico e coordinato, funzionale alla rilevazione ed alla gestione del rischio di riciclaggio e di finanziamento del terrorismo e provvede al suo riesame periodico al fine di assicurarne l'efficacia nel tempo;
- assicura nel continuo che i compiti e le responsabilità in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo siano allocati in modo chiaro e appropriato, garantendo che le funzioni operative e quelle di controllo siano distinte e che le funzioni medesime siano fornite di risorse qualitativamente e quantitativamente adeguate; assicura, inoltre, che venga approntato un sistema di flussi informativi verso gli Organi Aziendali ed al loro interno adeguato, completo e tempestivo e che le carenze e le anomalie riscontrate in esito ai controlli di vario livello siano portate tempestivamente a sua conoscenza, ferma restando la necessità di garantire la tutela della riservatezza dei soggetti che hanno partecipato alla procedura di segnalazione delle operazioni sospette;
- esamina, con cadenza almeno annuale, la relazione del Responsabile della Funzione Antiriciclaggio di Gruppo sulle attività di verifica svolte, sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale nonché sulle comunicazioni inoltrate dal Collegio Sindacale e/o dall'Organismo di Vigilanza; nel caso in cui dette comunicazioni si riferiscano a infrazioni considerate rilevanti, ne viene data informativa anche alla prima riunione utile da parte del Responsabile della Funzione Antiriciclaggio di Gruppo.

AMMINISTRATORE DELEGATO

In materia di adeguata verifica, l'Amministratore Delegato assicura che i processi e le procedure interne consentano:

- la corretta identificazione anagrafica del cliente, l'acquisizione e il costante aggiornamento di tutte le informazioni funzionali all'adeguata verifica;
- la costante verifica dell'attività svolta dai dipendenti e dai collaboratori al fine di rilevare eventuali anomalie.

COLLEGIO SINDACALE

Il Collegio Sindacale:

- valuta con particolare attenzione l'idoneità delle procedure in essere per l'adeguata verifica della clientela;
- stimola l'azione di approfondimento dei motivi delle carenze, anomalie e irregolarità riscontrate e promuove l'adozione delle opportune misure correttive.

ORGANISMO DI VIGILANZA DI CUI AL D. LGS. 231/2001

L'organismo di vigilanza:

- contribuisce in via preventiva alla definizione del modello idoneo a prevenire la commissione di reati di riciclaggio, di autoriciclaggio, di finanziamento del terrorismo, di impiego di denaro, beni o utilità di provenienza illecita di cui agli articoli 648 bis, 648 ter, 648-ter-1 del Codice penale;
- monitora nel continuo il rispetto delle procedure ivi previste e, nel caso in cui un reato sia comunque commesso, ne analizza le cause per individuare le misure correttive più idonee;
- vigila, nell'ambito delle proprie attribuzioni e competenze, sull'osservanza delle norme in materia di riciclaggio e finanziamento del terrorismo, contenute nel d. lgs. 231/2007;
- comunica senza ritardo, agli organi di vertice, tutti gli atti o i fatti di cui venga a conoscenza nell'esercizio dei propri compiti che possa costituire una violazione delle disposizioni in materia.

FUNZIONE INTERNAL AUDIT

La Funzione Internal Auditing verifica in modo continuativo, secondo un approccio *risk based*, il grado di adeguatezza dell'assetto organizzativo aziendale e la sua conformità rispetto alla disciplina di riferimento e vigila sulla funzionalità del complessivo sistema dei controlli interni.
Con specifico riferimento agli obiettivi del presente documento, la Funzione Internal Auditing verifica:

- il costante rispetto dell'obbligo di adeguata verifica, sia nella fase di instaurazione del rapporto che nello svilupparsi nel tempo della relazione;

- l'effettiva acquisizione e l'ordinata conservazione dei dati e documenti prescritti dalla normativa;
- l'effettivo grado di coinvolgimento del personale dipendente e dei collaboratori nonché dei responsabili delle strutture centrali e periferiche, nell'attuazione dell'obbligo della "collaborazione attiva".

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

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

FUNZIONE ANTIRICICLAGGIO DI GRUPPO

La Funzione Antiriciclaggio di Gruppo, a diretto riporto del Consiglio di Amministrazione della Banca capogruppo, in virtù di specifico contratto infragruppo di *outsourcing*:

- identifica le norme applicabili in tema di presidio del rischio di riciclaggio e di contrasto al finanziamento del terrorismo e valuta il loro impatto sui processi e le procedure interne;
- collabora all'individuazione delle procedure e dei controlli finalizzato alla prevenzione e al contrasto dei rischi di riciclaggio e finanziamento del terrorismo;
- verifica l'adeguatezza delle procedure e dei controlli adottati in materia di contrasto al riciclaggio e al finanziamento del terrorismo e propone le modifiche organizzative e procedurali necessarie o opportune al fine di assicurare un adeguato presidio dei rischi;
- collabora con le funzioni aziendali competenti nella progettazione e nella erogazione di corsi specialistici in materia;
- predispone, almeno una volta l'anno, una Relazione sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale, da sottoporre al Collegio Sindacale, all'Amministratore Delegato ed al Consiglio di Amministrazione della Compagnia;
- assicura l'inoltro dei flussi informativi di competenza al Collegio Sindacale, all'Organismo di Vigilanza ex D. Lgs. 231/2001 ed al Consiglio di Amministrazione della Compagnia e all'Amministratore Delegato;
- svolge, anche in collaborazione con le strutture operative, le attività di adeguata verifica rafforzata della clientela, nei casi in cui - per circostanze oggettive, ambientali e/o soggettive - appaia particolarmente elevato il rischio di riciclaggio;
- nell'ambito di competenza, predispone/valida e aggiorna la normativa interna, le *policy* ed i regolamenti in materia di antiriciclaggio e antiterrorismo e predispone, ove necessario, le correlate linee guida di Gruppo;

Inoltre, per le attività svolte in *outsourcing* da Banca Mediolanum, Il Responsabile Antiriciclaggio di Flowe:

- monitora periodicamente le attività svolte dall'outsourcer e ne riporta tempestivamente gli esiti al Consiglio di Amministrazione al fine di impartire le direttive per l'adozione di adeguate misure correttive correlate alle eventuali carenze e anomalie riscontrate.

RESPONSABILE ANTIRICICLAGGIO

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.
Il Responsabile Antiriciclaggio ha libero accesso ai flussi informativi diretti agli organi aziendali e alle strutture, a vario titolo, coinvolte nella gestione e contrasto del riciclaggio e del finanziamento al terrorismo.
Al Responsabile Antiriciclaggio competono funzioni complesse, da esercitarsi trasversalmente su tutta l'operatività svolta dalla Compagnia, qualificabili sia in termini di verifica della funzionalità di procedure, strutture e sistemi, sia di supporto e consulenza agli Organi e alle Funzioni aziendali interessate.

DELEGATO ALLE SEGNALAZIONI DELLE OPERAZIONI SOSPETTE

Il Delegato alle segnalazioni delle operazioni sospette, nominato dal Consiglio di Amministrazione:

- ha la responsabilità di valutare le segnalazioni di operazioni sospette ricevute e di autorizzare la trasmissione delle segnalazioni ritenute fondate alla UIF;
- intrattiene i rapporti con l'UIF e risponde tempestivamente ad eventuali richieste di approfondimento provenienti dalla stessa unità;
- ha libero accesso ai flussi informativi diretti agli organi aziendali nonché alle strutture coinvolte, a vario titolo, nella gestione e contrasto del riciclaggio e del finanziamento al terrorismo;
- comunica, con le modalità operative ritenute più appropriate, l'esito della propria valutazione alla struttura di Banca che gestisce, secondo l'Accordo di Servizio', le operazioni sospette.
- ferma la tutela della riservatezza dell'identità del soggetto di primo livello che ha effettuato la segnalazione, il Delegato alla segnalazione di operazioni sospette può consentire che i nominativi dei clienti oggetto di segnalazione di operazione sospetta siano consultabili – anche attraverso l'utilizzo di idonee basi informative – dai responsabili delle diverse strutture operative aziendali, stante la particolare pregnanza che tale informazione può rivestire in sede di apertura di nuovi rapporti contrattuali ovvero di valutazione dell'operatività della clientela già in essere.

FUNZIONE COMPLIANCE

La Funzione Compliance presiede la gestione dei rischi di non conformità alle norme, secondo un approccio *risk based*, con riguardo a tutta l'attività aziendale, ad esclusione degli ambiti normativi demandati *ex lege* alle altre funzioni di controllo. Si avvale, per il presidio di determinati ambiti normativi per cui sono previste forme di presidio specializzato, di unità specialistiche cui sono attribuite determinate fasi del processo di *compliance*.

PERSPECTIVE BANKING SERVICES & CONTROLS

La perspective Banking Services & Controls costituisce il primo livello del processo di gestione dei rischi. Nel corso dell'operatività giornaliera tale struttura è chiamata, infatti, ad identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi. Inoltre, la struttura deve rispettare i limiti operativi assegnati coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi.

Tutti i dipendenti ed i collaboratori – anche outsourcers - dell'Unità, nell'ambito delle mansioni a cui sono assegnati, sono tenuti a conoscere e uniformarsi alle leggi, ai regolamenti ed alle norme emanate dalla Società. I documenti aziendali che disciplinano aspetti organizzativi e comportamentali afferenti il rispetto delle norme vigenti, sia di legge sia definite internamente dalla Società, sono portati a conoscenza di tutti i dipendenti e dei collaboratori attraverso la loro pubblicazione e diffusione secondo le modalità previste da dalla Società stessa.

Allorché dipendenti e collaboratori, nell'espletamento delle proprie attività, rilevino che i processi operativi non siano aderenti alle norme di riferimento o i presidi adottati non siano efficaci al fine di prevenire il coinvolgimento, anche inconsapevole, della Società operazioni di riciclaggio o finanziamento del terrorismo devono darne tempestiva comunicazione al proprio responsabile. Alla perspective Banking Services & Controls è assegnata l'amministrazione e la gestione concreta dei rapporti con la clientela, alla medesima compete il processo di identificazione e di adeguata verifica della clientela assegnata quale primo livello di controllo, sviluppando la conoscenza della medesima ed assicurando un monitoraggio continuo nel corso del rapporto, in funzione del rischio sotteso. Ad essa compete, inoltre, lo svolgimento del processo di adeguata verifica rafforzata nei casi previsti dalla normativa e, laddove richiesto dalla Funzione Antiriciclaggio di Gruppo, nonché l'onere di segnalare tempestivamente, ove possibile prima di compiere l'operazione, eventuali operazioni sospette, secondo le procedure e le modalità definite internamente, allorché sappiano sospettino o abbiano ragionevoli motivi di sospettare che sia stata compiuta, sia in corso o sia tentata un'operazione di riciclaggio o finanziamento del terrorismo.

L'Unità svolge le istruttorie delle attività di adeguata verifica e di adeguata verifica rafforzata gestendo quale primo livello, la gestone degli Alerts corrispondenti (scadenza adeguata verifica).. In particolare:

- 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*;*
- monitora e aggiorna la profilatura di rischio della clientela della Società, in base alle informazioni emerse dalle istruttorie.

In particolare il Team AML della perspective Banking Services & Controls, procede con l'ADV in momenti distinti della vita del rapporto: in fase di onbording e nel monitoraggio delle transazioni.

In fase di onbaording:

- In seguito a match con liste (SGR e liste pubbliche): qualora il cliente risulti PEP si procede con l'invio del modulo di Adeguata verifica e richiesta dell'ultima dichiarazioni dei redditi; in caso di notizia di reato si procede a chiedere al cliente lo stato del procedimento.

In merito al monitoraggio giornaliero il transato dei clienti attraverso diversi INPUT - alert su FCM; richieste dell'A.G.; segnalazione interna, ecc.. -. Procede ad analizzare il conto del cliente attenzionato attendendosi ad alcuni parametri, ad es:

1. Conformità del reddito dichiarato con la movimentazione;
2. Provenienza dei fondi;
3. Coerenza con lo storico del cliente;

Se in seguito alle analisi si ritiene necessario chiedere informazioni al cliente si procede con l'invio di AVR.

In merito al controllo sui possibili match con le liste successivo all'apertura del conto è esternalizzato a Banca, con il team Operation Flowe.

Il team AML si occupa di gestire il secondo livello di analisi con conferma del match:

- In caso di PEP non riconosciuto in fase di onboarding si procede a chiedere al cliente, attraverso AVR la conferma della carica ricoperta, la compilazione del modulo di adeguata verifica e l'ultima dichiarazione dei redditi, nonché a chiedere parere preventivo obbligatorio alla Funzione Antiriciclaggio prima di presentare la pratica all'alto dirigente preposto alla autorizzazione all'instaurazione/mantenimento del rapporto;
- In caso di *sanction* e *crime* si procede a valutare l'entità della notizia, chiedere informazioni al cliente sullo stato del procedimento e valutazione di mantenere o meno il rapporto in essere.

RESPONSABILE PERSPECTIVE BANKING SERVICES & CONTROLS

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

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

Qualora il Responsabile decida di non seguire il parere preventivo ed obbligatorio della Funzione Antiriciclaggio, lo stesso deve mantenere evidenza di tale decisione e adottare apposite iniziative per mitigare i rischi segnalati dalla Funzione Antiriciclaggio.

STRUTTURE AZIENDALI DI BANCAMEDIOLANUM S.P.A.

In relazione alle attività disciplinate all'interno del **contratto di appalto per la fornitura di servizi** di gestione aziendale (accordo di servizio) – con riferimento alle attività inerenti il processo in questione, la società Flowe si avvale delle strutture di Banca Mediolanum S.p.A. per l'istruttoria delle attività di adeguata verifica e di adeguata verifica rafforzata in tutti i casi in cui sia necessaria.
Di seguito si dettagliano le attività svolte dalle strutture aziendali della Banca in ambito.

2.12.1 Ufficio Atti Giudiziari

L'ufficio Atti Giudiziari è il referente verso gli Organi Investigativi e l'Autorità Giudiziaria. A seguito di formali richieste pervenute, l'Ufficio può accedere a tutta la documentazione detenuta da tutte le unità aziendali affinché possano essere effettuate le necessarie verifiche e predisposte le opportune risposte, sempre nel rispetto della riservatezza prevista dagli artt. 45 e 46 del d.lgs. 231/2007. Qualora emergessero elementi di sospetto dalle richieste pervenute, l'Ufficio effettua senza indugio una segnalazione alla Funzione Antiriciclaggio di Gruppo, per le opportune valutazioni di competenza.

2.12.2 Unità Operations Flowe

L'Unità per quanto di competenza del seguente regolamento esegue le seguenti attività operative relative alla lavorazione e sistemazione di pratiche di onboarding, meglio descritte nel contratto di appalto con la Banca, per la gestione posizioni in "stand by" per *alert* nel Gestionale Antiriciclaggio.

ATTORI ESTERNI

2.13.1 INFOCERT SPA

InfoCert S.p.A. - Società soggetta alla direzione e coordinamento di TINEXTA S.p.A. opera in qualità di prestatore di servizi fiduciari qualificati, sulla base di una valutazione di conformità effettuata dal *Conformity Assessment Body* CSQA Certificazioni S.r.l., ai sensi del Regolamento (UE) 910/2014 e delle norme ETSI EN 319 401, ETSI EN 319 411-1; ETSI EN 319 411-2, secondo lo schema di valutazione eIDAS definito da ACCREDIA a fronte delle norme ETSI EN 319 403 e UNI CEIISO/IEC 17065:2012. Opera quale certificatore accreditato ai sensi dell'art. 29 del D.L.vo 82/2005 e ss.mm.ii.("Codice dell'Amministrazione Digitale", di seguito denominato brevemente "CAD").

In qualità di fornitore presta a Flowe i seguenti servizi:

- Trusted Onboarding Platform TOP è una soluzione brevettata di InfoCert in grado assolvere agli aspetti di identificazione dei clienti a distanza e la sottoscrizione di contratti, su tutti i dispositivi – desktop, tablet, smartphone – con il massimo livello di affidabilità. L'interazione con l'Utente è interamente mediata dall'App messa a disposizione da Flowe, la quale integra i servizi messi a disposizione da InfoCert per le componenti di OCR reader, NFC reader, Liveness Detection e Face Matching[1];

[1] Vedi par. "Processo digital onboarding"

- servizio di archiviazione sostitutiva [2], tramite LegalDoc Service che garantisce la conservazione di dati e documenti informatici, ai sensi del DPCM 3.12.2013 e ss.mm.ii. Le funzioni di indicizzazione, ricerca ed esibizione dei documenti conservati in forma elettronica a mezzo del servizio LegalDoc Service saranno garantite dal medesimo LegalDoc Service attraverso l'integrazione applicativa con il sistema informativo legacy del Produttore, in conformità alla normativa applicabile, ed inoltre alle previsioni di cui al D.M.E.F 17.06.2014.

2.13.2 EXPERIAN ITALIA SPA

La Società fornisce quale infoprovider accesso a banche dati (fonti affidabili e indipendenti) utili al processo di onboarding (identificazione della clientela) e permette, tramite piattaforma IQP la gestione di approfondimenti (obblighi rafforzati) su clientela che genera report di evidenza.

2.13.3 TEMENOS

La Società fornisce quale il sistema di Core Banking (T24) e diversi moduli per le gestione dei presidi in materia di prevenzione al riciclaggio e finanziamento del terrorismo (FCM).

2.13.4 UIF - Unità di Informazione Finanziaria

L'Unità di informazione finanziaria per l'Italia (UIF), istituita presso la Banca d'Italia, è autonoma e operativamente indipendente. In attuazione di tale principio, la Banca d'Italia ne disciplina con regolamento l'organizzazione e il funzionamento, ivi compresa la riservatezza delle informazioni acquisite, attribuendole i mezzi finanziari e le risorse idonei ad assicurare l'efficace perseguimento dei suoi fini istituzionali. Alla UIF e al personale addetto si applica l'articolo 24, comma 6-bis, della legge 28 dicembre 2005, n. 262. In materia, La UIF esercita le seguenti funzioni:

- riceve le segnalazioni di operazioni sospette e ne effettua l'analisi finanziaria;
- analizza i flussi finanziari, al fine di individuare e prevenire fenomeni di riciclaggio di denaro e di finanziamento del terrorismo;
- assicura la tempestiva trasmissione alla Direzione nazionale antimafia e antiterrorismo dei dati, delle informazioni e delle analisi, secondo quanto stabilito dall'articolo 8, comma 1, lettera a). Assicura, altresì, l'effettuazione delle analisi richieste dalla Direzione nazionale antimafia e antiterrorismo ai sensi dell'articolo 8, comma 1, lettera d).

2.13.5 CSF - Comitato Sicurezza Finanziaria

Il Comitato di sicurezza finanziaria esercita i poteri e le funzioni previsti dal decreto legislativo 22 giugno 2007, n. 109, e successive modificazioni, recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, elabora le strategie di prevenzione del riciclaggio e di finanziamento del terrorismo

[2] Vedi "Regolamento del processo di conservazione e controlli"

e coordina le misure di contenimento del relativo rischio da parte delle autorità di cui all'articolo 21, comma 2, lettera a).
Il decreto 22 giugno 2007, n. 109 e successive modificazioni disciplina il funzionamento del Comitato di sicurezza finanziaria nello svolgimento dei propri compiti e delle proprie funzioni.
In materia, propone al Ministro dell'economia e delle finanze le misure nazionali di designazione e congelamento dei fondi e delle risorse economiche detenuti, anche per interposta persona, da persone fisiche, persone giuridiche, gruppi o entità che commettono, o tentano di commettere, atti di terrorismo, ai fini dell'adozione dei decreti di cui all'articolo 4, comma 4 .

2.13.6 NSPV – Nucleo Speciale Polizia Valutaria della Guardia di Finanza

Il Nucleo speciale di polizia valutaria della Guardia di finanza, nel quadro degli obiettivi e priorità strategiche individuati annualmente dal Ministro dell'economia e delle finanze con la Direttiva generale per l'azione amministrativa e la gestione, esegue i controlli sull'osservanza delle disposizioni di cui al presente decreto da parte dei soggetti obbligati non vigilati dalle Autorità di vigilanza di settore nonché gli ulteriori controlli effettuati, in collaborazione con la UIF che ne richieda l'intervento a supporto dell'esercizio delle funzioni di propria competenza. In materia, il Nucleo speciale di polizia valutaria della Guardia di finanza svolge gli approfondimenti investigativi delle informazioni ricevute ai sensi dell'articolo 13 e delle segnalazioni di operazioni sospette trasmesse dalla UIF ai sensi dell'articolo 40. A tal proposito definisce e demanda per competenza l'esecuzione formale dei sequestri conservativi in ambito della procedura di congelamento prevista in materia.

3. Identificazione e adeguata verifica della clientela

In generale, l'art. 17 del Decreto antiriciclaggio, e le disposizioni attuative tempo per tempo vigenti, stabiliscono che i soggetti obbligati procedono all'adeguata verifica della clientela e del titolare effettivo, almeno nei seguenti momenti:

- in occasione della instaurazione di un rapporto continuativo;
- quando viene eseguita un'operazione occasionale[3] disposta dal cliente che: (i) comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che sia effettuata con un'operazione unica o con più operazioni frazionate; o (ii) consista in un trasferimento di fondi[4] superiore a 1.000 euro;
- quando vi è sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile; i destinatari si avvalgono degli indicatori di anomalia e degli schemi rappresentativi di comportamenti anomali emanati dalla UIF, in base al decreto antiriciclaggio;

[3] Rientrano tra le operazioni occasionali anche i casi in cui le banche, gli istituti di moneta elettronica, gli istituti di pagamento o Poste Italiane S.p.A. agiscano da tramite o siano comunque parte nei trasferimenti di denaro contante o titoli al portatore effettuati a qualsiasi titolo tra soggetti diversi, di importo complessivo pari o superiore a 15.000 euro

[4] Come definito dall'articolo 3, paragrafo 1, punto 9, del regolamento (UE) n. 2015/847 del Parlamento europeo e del Consiglio.

- quando sorgono dubbi sulla completezza, attendibilità o veridicità delle informazioni o della documentazione precedentemente acquisita (es., nel caso di mancato recapito della corrispondenza all'indirizzo comunicato o di incongruenze tra documenti presentati dal cliente o comunque acquisiti dal destinatario).

I destinatari adempiono agli obblighi di adeguata verifica nei confronti dei nuovi clienti. In relazione ai clienti già acquisiti, i destinatari svolgono nuovamente l'adeguata verifica quando opportuno, in ragione dell'innalzamento del livello di rischio di riciclaggio e di finanziamento del terrorismo associato al cliente.

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.

In caso di impossibilità oggettiva di svolgere l'adeguata verifica della clientela, così come previsto dall'art. 42 del Decreto Antiriciclaggio, i soggetti obbligati si astengono dall'instaurare, eseguire ovvero proseguire il rapporto, la prestazione professionale e a dar corso alle operazioni e valutano se effettuare una segnalazione di operazione sospetta all'UIF.

RIFERIMENTO CLIENTELA, PRODOTTI E SERVIZI

La clientela target è composta, in via prevalente, da studenti, neodiplomati, neolaureati, soggetti di età inferiore ai 40 anni che si sono recentemente affacciati sul mondo del lavoro. L'obiettivo è quello di acquisire un segmento di clienti non avvezzo all'utilizzo di prodotti e servizi bancari, al fine di consentire loro una crescente familiarizzazione con i medesimi, nell'ambito di un più ampio percorso formativo di matrice economica – finanziaria, supportato da una apposita piattaforma informatica.

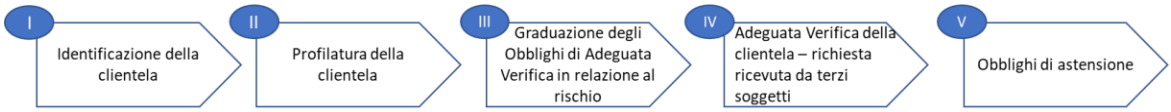
In considerazione di quanto sopra, l'offerta si rivolge esclusivamente a persone fisiche, residenti in Italia.
Non è quindi prevista la possibilità di instaurare rapporti, da parte di soggetti (clausole di esclusione):

- residenti in paesi diversi dall'Italia;
- diversi da persone fisiche.

Con riferimento all'offerta di prodotti e servizi, si precisa che la Società prevede la configurazione di un conto di pagamento monointestato, denominato in euro, sottoscrivibile on line mediante l'accesso ad una APP dedicata, in relazione al quale sono definiti specifici limiti e massimali di utilizzo. Al conto di pagamento è associata una carta di debito internazionale ed, eventualmente, una carta prepagata accessoria dedicata inizialmente ai minori di età. A fianco dei suddetti servizi di pagamento, la Società includerà nella propria offerta prodotti e servizi afferenti all'area "*wellbeing*".

La Società collocherà, inoltre, servizi di micro e *instant insurance* e di credito al consumo erogati da terze parti e fornirà accesso a piattaforme di terzi per la sottoscrizione di conti deposito.

Il processo di adeguata verifica, in base alla tassonomia dei processi aziendali è classificato tra i processi direzionali, nell'ambito dei processi di controllo e gestione del rischio.
Graficamente, il processo di adeguata verifica è così rappresentabile:



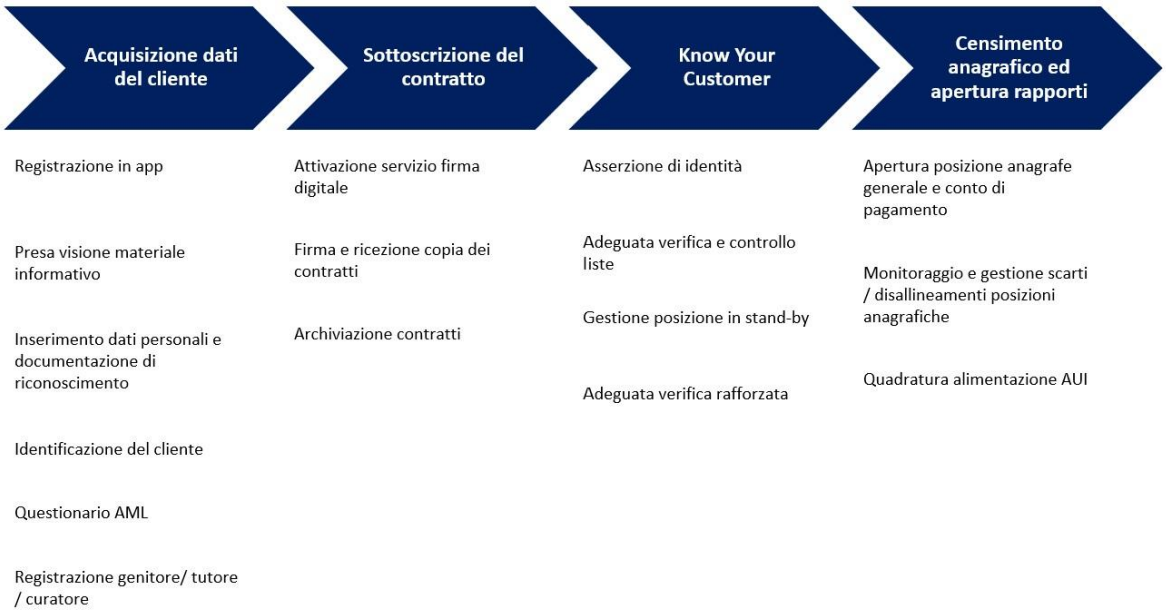
(I) IDENTIFICAZIONE DELLA CLIENTELA (ONBOARDING)

Prima dell'instaurazione di un rapporto continuativo, la Società svolge, l'attività di adeguata verifica, avvalendosi delle procedure messe a disposizione.
Per operatività a distanza si intende quella complessivamente svolta senza la compresenza fisica del cliente e del Personale incaricato della Società, ovvero attraverso i sistemi di comunicazione informatica tipici messi a disposizione (es. APP, sito internet, Mobile etc..) dalla Società stessa.
In particolare, l'identificazione del cliente, dell'esecutore e/o del titolare effettivo rappresenta la prima attività del processo di adeguata verifica della clientela; il controllo della identità del soggetto operante e degli eventuali poteri di rappresentanza, nonché la conservazione della relativa documentazione sono da ritenersi sempre necessari, a comprova della corretta operatività della Società.

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

PROCESSO DI "DIGITAL ONBOARDING"

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



Per quanto attiene il dettaglio del processo e delle relative fasi sopra descritte si rimanda per competenza al contenuto della "Policy sul contrasto al riciclaggio e al finanziamento del terrorismo" e della relativa "Procedura Operativa Onboarding" tempo per tempo vigenti.

Descrizione applicativi coinvolti nel processo

Nome applicativo	Breve descrizione	Fornitore	Certificazioni di sicurezza ottenute

Flowe (mobile app)	Applicazione mobile con cui operano i clienti della Società (versione iOS e Android sviluppata in tecnologia nativa) per l'apertura e la gestione del conto di pagamento e della carta ad esso associata. Durante il processo di onboarding l'app è utilizzata per l'acquisizione dei dati anagrafici (inseriti manualmente o acquisiti automaticamente tramite NFC usando carta di identità/passaporto elettronico), la foto dei documenti e l'immagine del cliente (tramite video selfie). Periodicamente (in linea con i rilasci delle nuove versioni dell'applicazione quindi bisettimanalmente o mensilmente) vengono effettuati dei test di vulnerabilità su entrambe	N/A	N/A
	le versioni dell'applicazione da parte di un fornitore specializzato. I test vengono effettuati in modalità black-box (questa modalità prevede che il fornitore non sia a conoscenza delle nuove funzionalità rilasciate) ed applicando e simulando una violazione seguendo l'approccio "red team" (approccio che consiste nel simulare un attaccante reale attenendosi quanto più possibile alla mentalità e alle risorse che lo stesso avrebbe a disposizione). A fronte delle attività effettuate viene creato e condiviso con la Società un report di dettaglio per entrambe le applicazioni (iOS e Android) all'interno del quale vengono elencate tutte le vulnerabilità opportunamente classificate secondo il criterio di scoring CVSS 3.1 (https://www.first.org/cvss/specificationdocument). Sulla base delle risultanze ottenute, la Società pianifica gli interventi di rimedio volti a sanare le vulnerabilità riscontrate.		

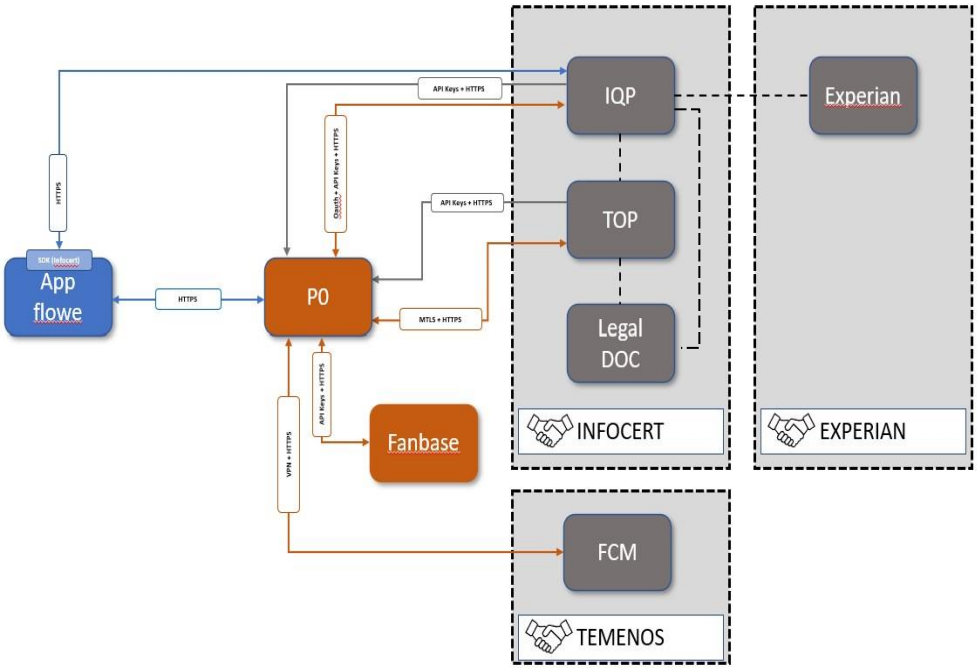
P0	Piattaforma della Società (*full cloud* – Microsoft Azure) sulla quale è implementata la logica applicativa mediante tecnologia a micro servizi. Tramite meccanismi forti di autenticazione i clienti accedono in modalità sicura alle risorse applicative. Tutte le informazioni vengono persistite su repository dati cifrate *at rest* e ridondate geograficamente in tempo reale (*Near Real Time*) su una regione secondaria al fine di garantire alta affidabilità. Mediante la piattaforma è possibile integrare sistemi esterni. Tutti gli accessi alla piattaforma rispettano le politiche di sicurezza di accesso logico definite dalla Società e in particolare tutti gli accessi vengono loggati e monitorati. L'autenticazione degli utenti (privilegiati e non) avviene tramite MFA.	N/A	N/A

	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 Azure.		

Fanbase	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*). In particolare tale soluzione può interfacciarsi con la piattaforma P0 attraverso API specificatamente sviluppate. Tutti gli accessi alla piattaforma rispettano le politiche di sicurezza di accesso logico definite dalla Società e in particolare tutti gli accessi vengono loggati e monitorati. L'autenticazione degli utenti (privilegiati e non) avviene tramite MFA.		
TOP (*trusted onboarding platform*)	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 dell'utente. Nello specifico, attraverso questo strumento è possibile effettuare la firma digitale del contratto ed effettuare l'archiviazione sostitutiva su Legal Doc.	Infocert	ISO 27001 SOC2 Type II
IQP	Piattaforma applicativa a supporto del processo di KYC che consente la gestione di alcune fasi del processo di onboarding del cliente.		

	Nello specifico, attraverso questo strumento vengono svolte le attività di *identity assertion*. Gli operatori incaricati consultano l'esito del processo di KYC e visualizzano, tramite un sistema di segnalazione codificato in semafori (rosso per regola bloccante, giallo per necessità di ulteriori verifiche, verde per regola rispettata) le regole di identificazione cliente che non hanno consentito di proseguire nel processo di onboarding. Si specifica che l'operatore gestisce esclusivamente le pratiche che hanno almeno una regola non rispettata. A valle del processo di identificazione del cliente, le evidenze raccolte vengono inviate in conservazione sostitutiva su Legal Doc. La piattaforma applicativa può essere interfacciata attraverso un processo automatico mediante web API (integrazione da SDK o da P0), oppure da un operatore attraverso un'interfaccia web. Quest'ultimo è consentito esclusivamente a personale opportunamente identificato all'interno della Società attraverso un sistema di profilazione gestito da Infocert.		
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.		
FCM	Il modulo *Financial Crime Mitigation* (FCM) permette lo svolgimento di una serie di attività e controlli ai fini AML durante il processo di onboarding e nello specifico: • registra al suo interno per ogni cliente Flowe una posizione anagrafica contenente le informazioni fornite in App Flowe dallo stesso cliente; • gestisce il processo di calcolo del profilo di rischio, sulla base delle regole di impianto definite da Flowe; • permette la sospensione del processo di onboarding per i potenziali clienti sui quali, grazie ad uno *screening* del potenziale cliente con liste terze certificate, sono rilevate possibili corrispondenze con i soggetti presenti	Temenos	ISO 27001 SOC2

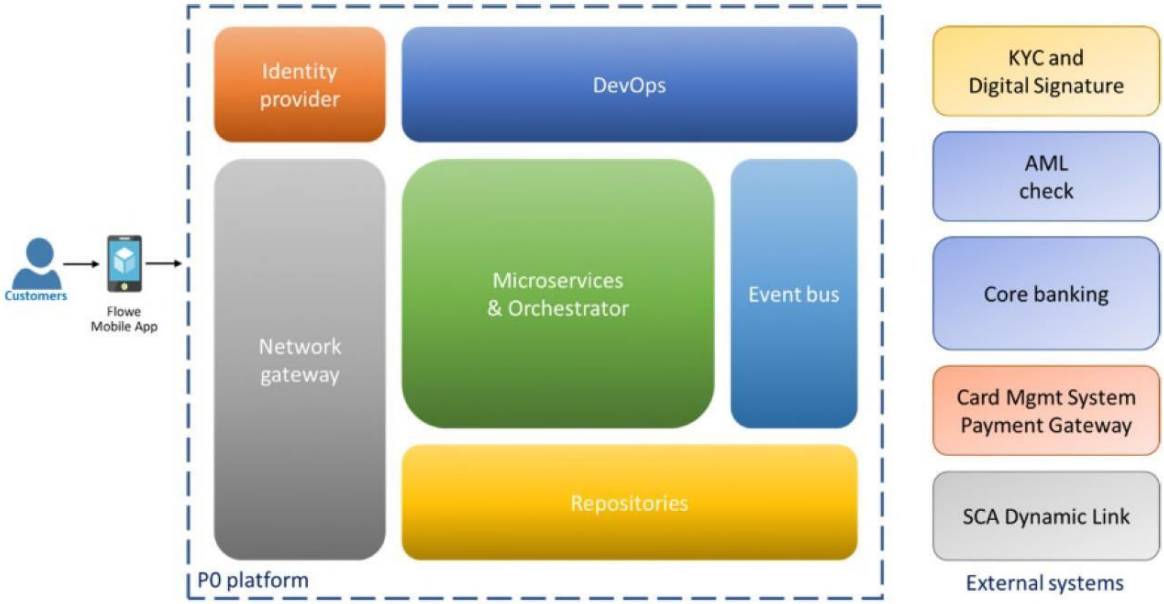
	nelle menzionate liste, ponendo degli "alert" sulle posizioni che l'operatore incaricato può consultare e gestire al fine di accertare il livello di rischio del profilo e certificare o meno il prospect con il soggetto "listato"; in tal caso, applicare, ove necessarie misure di adeguata verifica rafforzata, al fine di valutare se accettare o respingere la richiesta di onboarding del soggetto. La piattaforma applicativa può essere interfacciata attraverso un processo automatico mediante web API (integrazione da P0), oppure da un operatore attraverso un'interfaccia web. L'accesso all'interfaccia web è consentito esclusivamente a personale opportunamente identificato all'interno della Società ed il profilo applicativo viene assegnato attraverso un workflow autorizzativo.		
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).	Experian	ISO 27001 ISO 22301



Schema delle interfacce applicative e modello di integrazione

ARCHITETTURA TECNOLOGICA FLOWE

Per sviluppare la propria app ed offrire alla clientela i servizi sopra descritti, Flowe si è dotata di una architettura basata sul cloud per la propria piattaforma (denominata P0), adottando la soluzione Microsoft Azure6e di sistemi ed applicazioni esterne, offerti da fornitori specializzati, come di seguito sinteticamente rappresentato:



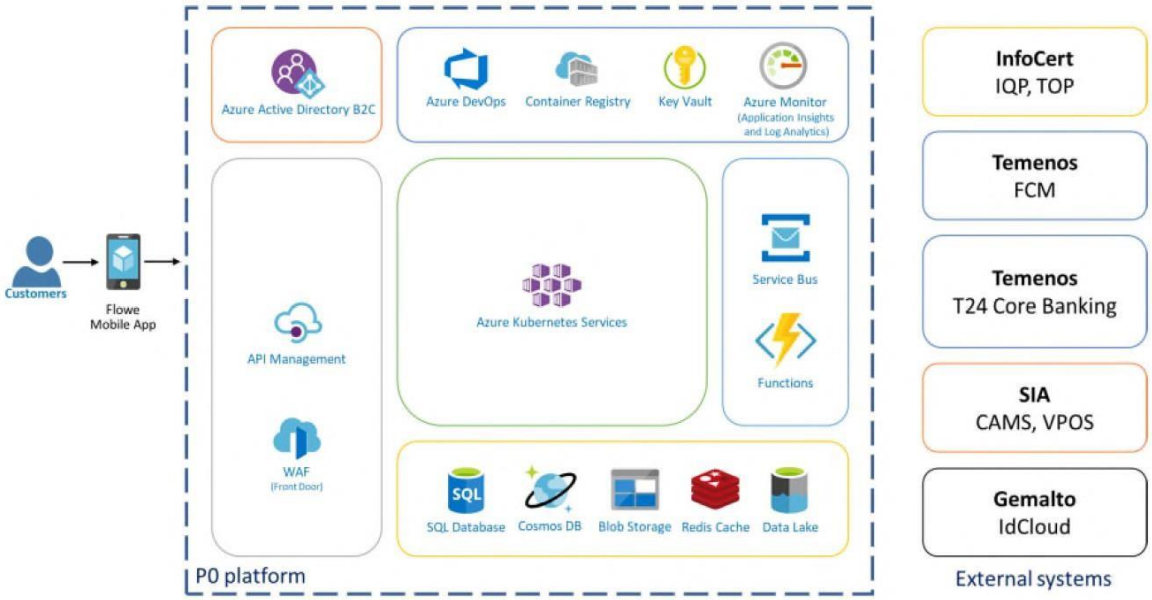
Il servizio cloud di Azure prevede l'acquisto annuale di crediti da "consumare" attivando all'interno dei Data Center Azure dei blocchi applicativi, che consentono di creare la propria architettura di servizi base, erogati appunto in cloud; Flowe definisce e crea la propria istanza del singolo "*building block*" e la relativa configurazione accedendo direttamente tramite una console web, mentre Microsoft ne gestisce il software e l'infrastruttura.
Flowe ha scelto di utilizzare i servizi cloud esclusivamente di tipologia SaaS (Software as a Service) e PaaS (*Platform as a Service)*[5].

[5] SaaS (Software as a Service): è la tipologia cloud più completa, in quanto l'utente finale non ha bisogno di nessuna conoscenza informatica per utilizzare l'applicazione o i servizi erogati, non ha bisogno di installare nessun tipo di file, ma i servizi sono utilizzabili con una connessione internet e un browser, avendo il vantaggio di usare i servizi su qualsiasi dispositivo e in qualsiasi luogo. La sottoscrizione è basata sul tempo di utilizzo o sul numero delle utenze; tendenzialmente riduce i costi derivanti dalle licenze, dalla gestione e installazione degli aggiornamenti. PaaS (Platform as a Service): il cloud è una piattaforma ponte tra le applicazioni (SaaS) e l'infrastruttura (IaaS). Il fornitore si occupa dell'infrastruttura hw, mentre l'utente dovrà installare il sistema operativo e sviluppare la sua applicazione, avendo il vantaggio di sfruttare la scalabilità dinamica, l'automazione per i backup dei database e un set di linguaggi di programmazione specifici; la fatturazione è periodica. IaaS (Infrastructure as a Service): il provider offre un hw virtuale (CPU, RAM, spazio e schede di rete) e quindi la flessibilità di un'infrastruttura fisica, senza l'onere per l'utente che avrà un hw virtuale, scalabile e misurabile automaticamente. La fatturazione è basata sul tempo di utilizzo, senza canoni fissi.
Le caratteristiche principali dei microservizi sono riassumibili in: "Piccoli" - incapsulano un cliente o uno scenario aziendale e sono sviluppabili da piccoli team; "Indipendenti dal linguaggio di sviluppo" - scritti in qualsiasi linguaggio di programmazione, utilizzano qualsiasi framework; "Indipendenti" - sono costituiti da codice e (facoltativamente) stato, entrambi con versione, distribuzione e dimensionamento indipendenti; "Interoperabili" - interagiscono con altri microservizi su interfacce e protocolli ben definiti; "Indipendenti dalla posizione" - hanno nomi univoci (URL); "Resilienti" - restano coerenti e disponibili in presenza di guasti.

P0 è il cuore della soluzione in cui, semplificando, avviene l'autenticazione sicura del cliente (Network gateway ed Identity provider), sono salvati i dati anagrafici e finanziari (Repositories), sono sviluppati collegamenti e funzionalità per i clienti e necessari alla gestione (DevOps), sono attivati i "contatti" con gli enti esterni (Event bus), il tutto attraverso applicazioni di microservizi opportunamente configurate (*Microservices & Orchestrator*), indipendenti dalla versione, scalabili ed incentrati sul cliente, che comunicano tra loro tramite protocolli standard ed interfacce definite[6].

Tali scelte tecniche coniugano gli obiettivi di Flowe di essere una società smart, flessibile con un modello di sviluppo "agile", ovvero secondo un approccio meno strutturato, focalizzato sull'obiettivo di consegnare al cliente in tempi brevi e frequentemente, software funzionante e di qualità. Le pratiche promosse dai metodi agili sono la formazione di team di sviluppo piccoli, poli-funzionali e auto organizzati, lo sviluppo iterativo e incrementale, la pianificazione adattiva e il coinvolgimento diretto e continuo del cliente nel processo di sviluppo. Il metodo adottato trova riscontro anche nell'attuale modello organizzativo sopra descritto (sezione "contesto operativo).

Un maggiore dettaglio è rappresentato nella successiva figura.



Flowe è una App software, nativa per iOS ed Android, scaricabile dai market place "Google Play Store" e "Apple Play Store".
L'accesso all'applicazione mobile viene realizzato mediante autenticazione forte e sfruttando le tecnologie a disposizione degli utenti. In particolare, l'iscrizione dell'utente ai servizi offerti dalla Società è gestita all'interno dell'applicazione, utilizzando in sede di prima iscrizione l'autenticazione a due fattori (secondo fattore un SMS), mentre per tutti gli altri accessi l'autenticazione è a due fattori con possibilità di utilizzare un codice OTP oppure il sensore biometrico implementato nello smartphone/tablet da cui si opera.

La piattaforma P0 comunica con la App e con gran parte dei fornitori, mediante chiamate API Rest[7], con protocollo SSL[8] ed autenticazione forte.

All'interno della piattaforma P0 vi sono diversi elementi messi a disposizione dal servizio Cloud Azure di Microsoft, configurati da Flowe con il supporto degli esperti Microsoft:

- WAF -Web Application Firewall[9] - di Azure, offre protezione centralizzata alle applicazioni Web da attacchi infrastrutturali e vulnerabilità comuni (SQL injection, scripting, DDOS etc). È un servizio SaaS gestito da Microsoft e costituisce l'ingresso "entry point" "sicuro" alla piattaforma con i principali controlli di sicurezza; è in replica mondiale, gestito da Microsoft. Flowe ha creato la propria istanza e la configurazione accedendo direttamente tramite una console;
- API management infrastruttura che consente di esporre le web API Rest verso la App ed i fornitori, ovvero i servizi e di governarle gestendone il *versioning*, la reperibilità e definendone i limiti d'uso. Le API conducono all'interno dei microservizi (Azure Kubernetes Services)[10];
- Azure Active Directory (AD) offre la gestione delle identità e degli accessi; qui risiedono le utenze ed i gruppi "di sicurezza" che forniscono l'accesso a tutte le componenti e funzionalità dei singoli blocchi, secondo diversi ruoli; qui sono staccati i token di sessione che consentono l'accesso sicuro ai clienti; l'accesso a tale servizio è limitato a due persone della struttura Augmented Intelligence (di cui un consulente Microsoft) opportunamente loggate. Al fine di limitare il rischio di cancellazione dei dati (i dati sono infatti mascherati) è previsto un meccanismo che consente di ricostruire i profili utente (in quanto salvati in SQL db). Azure AD è in replica sul sito secondario. In sintesi, Azure AD è LDAP (Lightweight Directory Access Protocol[11]) centrale, dove sono mappate tutte le utenze di Flowe o Guest per accedere al mondo Microsoft, sia Office 365 (Owa, dashboard, powerBI, Teams, etc) che Azure per la parte infrastrutturale, secondo vari grant;

---

[7] Le funzionalità che un servizio web offre prendono nel complesso il nome di API ossia Application Programming Interface. Il modello REST, Representational State Transfer consiste in una serie di linee guida e di approcci che definiscono lo stile con cui i dati vengono trasmessi, basato sui comandi HTTP (ovvero GET, POST, PUT e DELETE) e formato JSON. I vantaggi derivanti dall'utilizzo di API Rest per un e-commerce sono ad esempio: Indipendenza: le API Rest sono indipendenti dai linguaggi o da precise piattaforme. Separazione client-server che consente di trattare indipendentemente l'evoluzione delle diverse componenti, modificare solo una parte progettuale senza, essere obbligati a mettere mano sia al server che al client. Scalabilità: la separazione client-server si traduce in una miglior scalabilità del sistema. API non è altro che la creazione di una serie di endpoint (delle URL) che rispondono alle richieste fatte da uno sviluppatore. L'esposizione delle API dipende da Flowe, mentre i fornitori sono gli owner degli endpoint e delle funzioni che consentono di recuperare e modificare il dato; Flowe si collega e definisce il modello di sicurezza da erogare verso le Terze parti mediante l'API Gataway ed Azure AD.

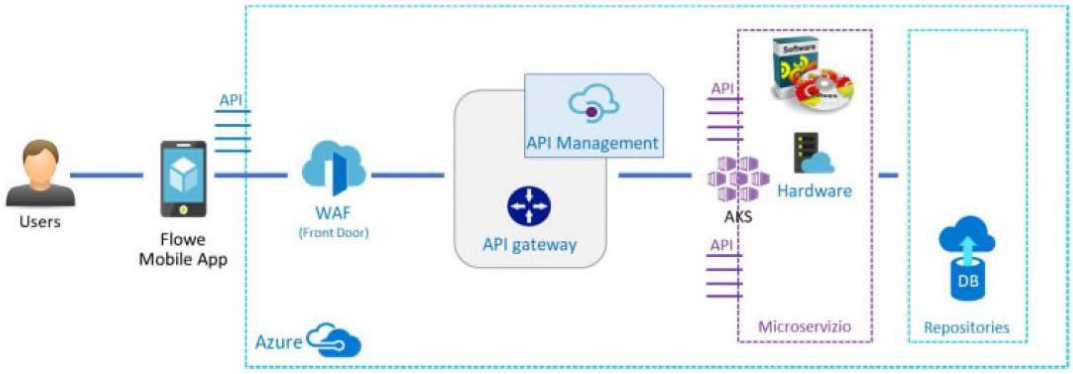
[8] "Secure Sockets Layer" (Livello di socket sicuri), una tecnologia standard finalizzata a garantire la sicurezza di una connessione a Internet e proteggere i dati sensibili scambiati fra due sistemi impedendo ai criminali informatici di leggere e modificare le informazioni trasferite. La comunicazione fra sistemi può riguardare un server o client o due server.

[9] Web Application Firewall (WAF) di Azure nel gateway applicazione di Azure, offre protezione centralizzata delle applicazioni Web da exploit e vulnerabilità comuni, in quanto le applicazioni Web sono sempre più vittime di attacchi che sfruttano le più comuni e note vulnerabilità (attacchi SQL injection e scripting intersito sono tra i più comuni). Il WAF si aggiorna automaticamente per la protezione contro le nuove vulnerabilità, senza alcuna configurazione aggiuntiva.

10 Azure Kubernetes Services: contiene i microservizi, ovvero le funzionalità e tutta l'infrastruttura tecnologica necessaria per la loro erogazione; possono essere considerate scatole logiche con sw, hw e a volte anche i relativi DB; i microservizi sono esposti all'esterno mediante le API (passando per API Gatway eWAF). Questo consente di "isolare" il microservizio rispetto alla app, dove il flusso dati avviene tramite API (linguaggio Json). Anche i microservizi sono ridondati sul sito primario, oltre che sul secondario.

[11] LDAP è un protocollo standard per l'interrogazione e la modifica dei servizi di directory, come ad esempio un elenco aziendale di email o una rubrica o qualsiasi raggruppamento di informazioni che può essere espresso come record di dati e organizzato in modo gerarchico

- Key Vault è una “cassaforte” a salvaguardia delle credenziali delle chiavi crittografiche e altri segreti usati dalla app e per la progettazione dei servizi cloud. Le informazioni riservate (come la password) sono mascherate sulle interfacce e criptate sui database e le chiavi per accedere a queste sezioni sono in Key Vault;
- Repositories: l’area che identifica tutti i database dove sono memorizzati i dati applicativi, in DB NoSQL (non relazionali) dove ci sono tutti i profili dei clienti Flowe, che consentono quindi il ripristino delle informazioni (il cliente sarebbe contattato ed invitato a fare un nuovo on boarding); tali DB sono in Alta Affidabilità, con backup giornaliero, ridondati.



Flowe, mantiene i DB esterni al microservizio per assicurare maggiore Alta Affidabilità e consistenza delle informazioni (per evitare che un *fail* di un microservizio abbia un impatto forte verso il cliente).

- Azure Monitor (*Applications Insights*), consente di accedere ai log di tutta l’applicazione, ad esempio è usato per analizzare tutte le chiamate fatte alle API verso Temenos. Anche l’accesso a questo strumento è gestito dal Portale Azure AD. Sono stati definiti Alert basati sui log, monitoratiti dal team ITMO. I log registrati hanno molti dettagli dell’operatività eseguita e lo strumento consente di analizzarli puntualmente, permettendo la ricostruzione di tutte le attività effettuate sull’applicazione da un singolo utente.
- Azure Sentinel: componente di sicurezza di Azure, che processa tutti i log di accessi e applica i controlli tradizionali per intercettare eventuali accessi di persone non abilitate. Sono definiti Alert basati sui log. Sui log lo strumento consente di effettuare delle ricerche puntuali, in quanto sono registrati molti dettagli dell’operatività eseguita; è stato attivato anche un controllo che consente di vedere cosa è stato ricercato sull’applicazione da una singola persona (es: query fatta dall’utente).
- Service Bus: tramite i microservizi i clienti effettuano la loro operatività; i microservizi non parlano direttamente tra loro, ma accodano messaggi sul service bus, dichiarando ad esempio di aver concluso il proprio lavoro, pubblicando sul bus il relativo risultato. I microservizi interessati all’esito di un servizio, si iscrivono alle code di messaggi per poter essere informati circa quelli di proprio interesse e leggerseli appena disponibili, trattando di conseguenza l’informazione; nell’attesa intanto possono effettuare altre attività. Quindi sul service bus sono gestiti tutti gli eventi (*integration event*). In questo modo il Service Bus è un “distributore” degli eventi e consente di disaccoppiare i microservizi (es. il mondo carte dai bonifici out), il mondo operativo (dove vi sono i servizi offerti ai clienti) da quello analitico (mondo Data Platform e Dashboard) e far in modo che

i diversi DB operazionali non abbiano una dipendenza diretta (quindi meno carico). E' un punto nevralgico della architettura, è in Alta Affidabilità con alto livello di efficienza e replica (nei tre siti nell'area geografica di Amsterdam), inoltre l'accodamento resta sempre disponibile e nel caso in cui un microservizio non riesca a contattare il Service Bus, è previsto un alert.

Le informazioni qui contenute sono poi riversate anche sul Data Lake mediante Data Platform (flusso monodirezionale incrementale, in tempo pressoché reale da Service Bus verso Data Platform verso Data Lake).

- Data Lake: contiene gli eventi dei microservizi presenti sul Service Bus in formato grezzo. Tali informazioni sono poi codificate, normalizzate o aggregate in DB più strutturati SQL o Cosmos. Qui mediante Power BI, sono applicate logiche di intelligenza artificiale utili a rendere visibili informazioni al cliente direttamente sulla App (es: il numero degli on boarding; le emissioni CO2 su acquisti con carta) o attivare azioni di *push notification*.
- Functions: costituiscono un modello più avanzato di cloud serverless[12], dove il cliente (Flowe) fa lo sviluppo del software senza preoccuparsi del servizio sottostante, dell'infrastruttura, della sua gestione e quindi del linguaggio di programmazione. La *function* consente di ottenere la scalabilità automatizzata e flessibile in base al volume del carico di lavoro e l'utilizzo è pagato a consumo (in base al numero di eventi in ingresso). Possono essere anche complesse come un servizio web ed è codice software con input e output, per il quale non mi interessa sapere su quale servizio è ospitata. In fase di design si decide se modellizzare i servizi come microservizi o *fuction* in base alla loro dimensione ed evoluzione. Flowe le usa per inoltrare le informazioni dal Service Bus ad altri sistemi o DB e per avere maggiore libertà di poter scalare su altri cloud più convenienti (es: AWS di Amazon).
- Azure DevOps: ambiente per lo sviluppo e test di tutte le componenti applicative di Flowe e per la tracciatura degli incidenti.
- Container Register: ad oggi non attivo.

Tutto il sistema è sotto audit log, consentendo il monitoraggio degli accessi e per le azioni dispositive, anche delle azioni effettuate sui singoli componenti.

Tutti i microservizi, gli storage e i DB sono replicati a livello di region sul sito primario (composto da tre siti nell'area geografica di Amsterdam con Alta Affidabilità) e a livello geografico "*near real time*" sul sito secondario (tre siti nell'area geografica di Dublino); il monitoraggio di entrambi i siti avviene tramite dashboard e l'attivazione del sito secondario avviene tramite WAF. Quando una qualsiasi componente o microservizio non funziona è prevista l'attivazione della replica complessiva (attivo DR).

(II) PROFILATURA DELLA CLIENTELA

Al fine di graduare la profondità e l'estensione degli obblighi di adeguata verifica, la Società si avvale di uno specifico software - Temenos FCM - per la profilazione di rischio della clientela attraverso il

[12] Serverless: i servizi, le prassi e le strategie che consentono di creare applicazioni più agili, in quanto le attività di gestione dell'infrastruttura come il provisioning e il patching delle capacità sono gestite dal fornitore di servizi cloud.

quale sono attribuiti appositi punteggi in realtime, a ciascun cliente, 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, all'esecutore e titolare effettivo;
- relativi a prodotti, servizi, operazioni o canali di distribuzione;
- geografici.

In APPENDICE 2 (**file riservato**) si allega l'impianto di profilatura in linea nel sistema.

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 (cfr. Profilo di rischio).

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)

Si specifica che il sistema di profilazione attribuisce il profilo di rischio più elevato tra quelli assegnati:

- a ciascun soggetto coinvolto nel rapporto continuativo (es. genitore titolare del conto/figlio minore intestatario di carta prepagata);
- da tutte le società del Gruppo, nel caso di clientela condivisa.

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

Il software in uso effettua, giornalmente con storicizzazione mensile, l'aggiornamento del profilo di rischio.
La Funzione Antiriciclaggio di Gruppo monitora ed aggiorna periodicamente i punteggi e le regole attribuite al sistema di profilazione del rischio, avendo anche a riferimento l'evoluzione del contesto

di riferimento, tenuto conto delle specificità della Società e del Gruppo di appartenenza, nonché della *leading practice* di mercato.

FATTORI DI RISCHIO GEOGRAFICO

Al fine di valutare i rischi geografici, la Società considera, i seguenti fattori di rischio:

- paesi soggetti a sanzioni, embargo o misure analoghe adottate dai competenti organismi nazionali e internazionali;
- paesi terzi che fonti autorevoli e indipendenti ritengono carenti di efficaci presidi di prevenzione del riciclaggio;
- paesi e aree geografiche che finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche;
- paesi valutati da fonti autorevoli e indipendenti come carenti sotto il profilo della conformità agli standard internazionali sulla trasparenza e lo scambio di informazioni a fini fiscali;
- paesi e aree geografiche valutati ad elevato livello di corruzione o di permeabilità ad altre attività criminose da fonti autorevoli e indipendenti.

La Società a tal proposito utilizza il "Basel AML Index"[13] (di seguito BAI) costituito da nr. 14 indicatori, aggregati in un unico punteggio complessivo di rischio.

I 14 indicatori prendono in considerazione i seguenti ambiti (vedi anche le fonti nella tabella in APPENDICE 3) come da fattori di rischio sopra esposti:

- i regolamenti AML / CFT;
- la corruzione;
- la trasparenza delle norme finanziarie;
- la trasparenza e la responsabilità pubblica;
- la situazione politica e stato di diritto.

Ogni indicatore è espresso in una scala da 0 a 10, in funzione del rischio attribuito.

Gli indicatori convertiti vengono quindi aggregati utilizzando un sistema di ponderazione sulla base di una perizia qualitativa. Di conseguenza, i singoli indicatori non hanno lo stesso peso né sono ponderati in conseguenza della loro qualità statistica. I singoli pesi sono valutati da esperti antiriciclaggio del *Basel Institute on Governance e ICAR*. L'istituto rivede le fonti e le ponderazioni ogni anno prendendo in considerazione anche esperti esterni.

Per quanto attiene l'operatività da e verso i paesi esteri, la Società ha realizzato indicatori di anomalia basati sulle operazioni di segno dare e avere, per fasce di importo e frequenza (mensile) effettuate dalla clientela che concorrono alla profilatura *real-time* del cliente. Pertanto allo scattare di detti indicatori ed al superamento della soglia di rischiosità prevista (alto), la perspective Banking

[13] Fornito dal Basel Institute on Governance: www.baselgovernance.org - centro di competenza indipendente e non lucrativo specializzato nel contrasto della corruzione e di altri crimini finanziari, il quale contiene ulteriori Paesi rispetto a quelli contenuti nelle liste ufficiali (UE, GAFI, OFAC - Sanzioni Finanziarie Internazionali, Fiscalità Agevolata), individuati attraverso criteri quali la trasparenza finanziaria / pubblica, il rischio di corruzione ed i rischi legati alla stabilità politica.

Services & Controls 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.
-

(III) GRADUAZIONE DEGLI OBBLIGHI DI ADEGUATA VERIFICA IN RELAZIONE AL RISCHIO

L'adeguata verifica può assumere, in funzione del grado di rischio associato al cliente modalità diverse di esecuzione: adeguata verifica ordinaria e adeguata verifica rafforzata

ADEGUATA VERIFICA ORDINARIA DELLA CLIENTELA

La Società ha definito il set di informazioni concernenti l'adeguata verifica ordinaria della clientela, nonché il processo di identificazione della stessa (cfr. par. Identificazione della clientela (onboarding)).

Il sistema di profilatura della Società elabora in *real time* il profilo di rischio associato al soggetto richiedente in base ai controlli ed ai dati previsti nella fase del processo di *onboarding*.

In tutti i casi il profilo di rischio attribuito al soggetto sia "alto":

- in specifiche casistiche individuate (es. processo di identificazione non andato a buon fine per codice fiscale non esistente/coerente, documento falso/rubato, match positivo con c.d. liste negative, etc…), **rifiuta la richiesta di instaurazione del rapporto** e (i) inserisce il nominativo del soggetto proponente nella c.d. lista clienti indesiderati della Società e (ii) genera un "*case*" per gli approfondimenti del caso a cura della perspective Banking Services & Controls che sentita la Funzione Antiriciclaggio di Gruppo pone poi la pratica alla valutazione del Delegato alla segnalazione di operazioni sospette per la valutazione di competenza;
- in specifiche casistiche individuate (es. match dubbio con c.d. liste negative, etc…), **la richiesta di instaurazione viene sospesa fino al termine delle verifiche** e la perspective Banking Services & Controls genera un "case" per gli approfondimenti del caso che, sentita la Funzione Antiriciclaggio di Gruppo, pone poi la pratica alla valutazione del Delegato alla segnalazione di operazioni sospette che, congiuntamente al Responsabile della perspective Banking Services & Controls valuta gli esiti dell'istruttoria al fine di accettare o meno la richiesta di instaurazione del rapporto;

- infine, nel caso di soggetto qualificabile come PEP, pone la richiesta di instaurazione in stand by e genera un "case" per gli approfondimenti del caso a cura della perspective Banking Services & Controls e la prevista autorizzazione da parte del Responsabile della perspective Banking Services & Controls (cfr. par. Persone Esposte Politicamente (c.d. PEP)).

Inoltre nel caso di processo di onboarding di soggetto "minore", viene prevista la raccolta del legame con soggetto "adulto" che conferma i dati e firma il contratto digitalmente.
Qualora il legame indicato sia Tutore o Curatore, il sistema notifica a mezzo email immediata all'adulto la necessità di fornire alla società idonea documentazione entro 21 gg atta a verificare la sussistenza dell'indicato potere di rappresentanza del minore. Un sistema di *reminder* automatico sollecita il cliente e alla scadenza concordata, se non pervenuta la documentazione richiesta, pone il blocco al rapporto e notifica lo stesso alla perspective Banking Services & Controls per la azioni di competenza.

ADEGUATA VERIFICA RAFFORZATA DELLA CLIENTELA

I destinatari applicano 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.
In particolare, la Società considera a più alto rischio di riciclaggio:

a) clienti che rientrano nella definizione di "Persone Esposte Politicamente";
b) clienti con riferimento ai quali sono stati rilevati degli indici reputazionali negativi, sulla base di:
    - ricorrenza dei nominativi nelle liste delle persone o degli enti associati ai fini degli obblighi di congelamento previsti dai Regolamenti comunitari o dai decreti emanati dal MEF, ai sensi del D. Lgs. n. 109/2007;
    - notizie negative provenienti dai media o da altre fonti informative;
    - notizie negative fornite direttamente dal cliente, aventi ad oggetto procedimenti penali, procedimenti per danno erariale, procedimenti per responsabilità amministrativa degli enti (ex D. Lgs. 231/01), etc.;
    - richieste/provvedimenti provenienti dall'Autorità Giudiziaria, ai sensi: del Codice Antimafia (accertamenti richiesti dall'Autorità Penale ai sensi del D. Lgs. 159/2011 - Antimafia - fase delle indagini preliminari) o della normativa antiriciclaggio (accertamenti richiesti dall'Autorità Penale ai sensi del Decreto Antiriciclaggio - Antiriciclaggio - fase delle indagini preliminari);
    - decreti di sequestro, ovvero misure cautelari reali e di prevenzione adottate dall'Autorità Giudiziaria;
c) clienti oggetto di precedente segnalazione alla UIF;

d) qualunque altro caso in cui il dipendente incaricato ravvisi, in fase di perfezionamento di un'operazione o di accensione di un nuovo rapporto continuativo, un più elevato rischio di riciclaggio o finanziamento del terrorismo. In particolare, deve essere opportunamente considerato dal dipendente incaricato, il comportamento tenuto dal cliente o dall'esecutore, quale, (elenco non esaustivo, per ulteriori indicatori di anomalia si rimanda al provvedimento contenente indicatori di anomalia pubblicato dalla UIF - https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia):

- la riluttanza o incapacità nel fornire informazioni anche rispetto all'operatività svolta e/o sulla origine dei fondi la ripetuta modifica delle informazioni fornite o il fatto che siano fornite informazioni incomplete o erronee;
- l'interposizione di soggetti terzi senza apparente giustificazione (es. viene costantemente accompagnato da altre persone che appaiono estremamente interessate all'operatività ovvero alle modalità di esecuzione della prestazione) e/o il rilascio di deleghe o procure del tutto incoerente con l'attività svolta o varia molto frequentemente i soggetti delegati;
- porre ripetuti quesiti in ordine alle modalità di applicazione della normativa antiriciclaggio e antiterrorismo e cerca di indurre l'Agente in Attività Finanziaria ad eludere tali presidi, anche tentando di stabilire relazioni eccessivamente confidenziali;
- l'indisponibilità o l'impossibilità di produrre documentazione in merito alla propria identità (fatto salvo il caso dei richiedenti asilo);
- la ripetuta modifica delle informazioni fornite o il fatto che siano fornite informazioni incomplete o erronee e/o significativamente difformi, contraddittorie o comunque non coerenti con quelli tratte da fonti affidabili e indipendenti (es. testate giornalistiche o altri siti di divulgazione notizie via web);
- la volontà di ricevere le comunicazioni a esso rivolte ad un recapito diverso da quello indicato (ad esempio, residenza, domicilio, indirizzo di posta elettronica, numero di cellulare, applicazione web o mobile o altro strumento di comunicazione a distanza) o non risulta rintracciabile ai recapiti indicati ovvero chiede l'invio diretto delle comunicazioni a soggetti a lui non collegati ovvero varia molto frequentemente Agente in Attività Finanziaria/Agenzie, indirizzi e-mail, etc..);
- l'indisponibilità di esibire la documentazione o le informazioni di prassi, con conseguente rinuncia immotivata all'operatività o richiesta di svolgerne una differente, soprattutto se quest'ultima comporta un aggravio di costi a proprio carico;
- l'esecuzione o l'intenzione di eseguire operazioni caratterizzate da importi insolitamente elevati o rispetto alle quali sussistano dubbi circa la finalità cui le medesime sono, in concreto, preordinate;
- la mancata ragionevolezza dell'operazione in funzione dell'abituale operatività/patrimonio/reddito, delle caratteristiche, delle competenze o delle conoscenze normalmente attese per il settore di attività dichiarate dal Cliente.

e) clienti classificati a rischio alto, in base al sistema di profilatura della clientela adottato internamente ovvero su richiesta del Delegato alla segnalazione di operazioni sospette a seguito del prudente apprezzamento dello stesso;

f) clienti bloccati dalla matrice dei controlli di onboarding per permettere approfondimenti tramite operatore dei dati/informazioni trasmessi.

Inoltre, la Società, visti i fattori di rischio elevato previsti dal decreto antiriciclaggio e, ai sensi dell'art. 24, comma 4, del decreto antiriciclaggio, gli ulteriori fattori di rischio rilevanti ai fini della eventuale applicazione delle misure rafforzate previsti nelle disposizioni attuative tempo per tempo vigenti, considera inoltre a maggior rischio di riciclaggio:

g) l'esecuzione o l'intenzione di eseguire operazioni caratterizzate da importi insolitamente elevati o rispetto alle quali sussistano dubbi circa la finalità cui le medesime sono, in concreto, preordinate;
h) tipo di attività economica riconducibile a settori particolarmente esposti a rischi di corruzione;
i) cliente o titolare effettivo che ricoprono cariche pubbliche in ambiti non ricompresi dalla nozione di PEP ma per i quali comunque sussiste una rilevante esposizione al rischio di corruzione;
j) pagamenti ricevuti da terzi privi di un evidente collegamento con il cliente o con la sua attività;
k) operatività da e verso paesi terzi ad elevato rischio geografico (rif. PROFILATURA DELLA CLIENTELA).

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

La Società prevede, nel caso di:

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

L'autorizzazione dei soggetti titolari di poteri di amministrazione o direzione ovvero di loro delegati o, comunque, di soggetti che svolgono una funzione equivalente, per quanto sopra riportato deve essere fornita dal Responsabile della Unità Banking Services & Controls, previa valutazione del parare obbligatorio e preventivo della Funzione Antiriciclaggio.

MODALITÀ ESECUZIONE OBBLIGHI RAFFORZATI

In sede di adeguata verifica rafforzata, è compito della Funzione Antiriciclaggio di Gruppo o della perspective Banking Services & Controls (Team AML e Team Account Monitoring) di:

- acquisire maggiori informazioni sul cliente e sul titolare effettivo.
- acquisire/aggiornare e valutare informazioni sulla reputazione del cliente e/o del titolare effettivo ivi comprese eventuali pregiudizievoli, tramite la consultazione di fonti aperte, attraverso, ad esempio, l'utilizzo di motori di ricerca su internet.
- valutare attentamente le informazioni fornite dal cliente sullo scopo e sulla natura del rapporto, mettendole in relazione con le altre informazioni conosciute all'atto di apertura del medesimo o, nel caso di clienti che già intrattengono rapporti con la Società, con l'operatività effettivamente rilevata sullo stesso; a tal riguardo, sono presi in considerazione elementi quali: il numero, l'entità e la frequenza delle operazioni effettuate, la

provenienza/destinazione dei fondi, la natura dell'attività svolta dal cliente e/o dal titolare effettivo, la ragionevolezza delle operazioni effettuate in relazione al profilo complessivo del cliente.

- svolgere approfondite verifiche sull'origine del patrimonio e dei fondi impiegati nel rapporto continuativo, attraverso un processo articolato che prenda in considerazione, in primis, la attendibilità delle informazioni a disposizione della Società, tenuto conto della eventuale disponibilità di informazioni economico – patrimoniali prodotte direttamente dal cliente o rilevabili dalla movimentazione del rapporto (es. accredito emolumenti, accredito dividendi, etc.) o reperibili tramite fonti aperte o banche dati pubbliche (es. bilanci, dichiarazioni IVA e dei redditi, atti notarili, dichiarazioni di successione, dichiarazioni/documenti provenienti dal datore di lavoro o da altri intermediari); a tal riguardo, assumono specifica valenza aspetti, quali il grado di conoscenza del cliente e/o l'anzianità della relazione, la coerenza tra il profilo del cliente e la sua situazione economico-patrimoniale.
- condurre in modo più frequente la verifica e l'aggiornamento delle informazioni anagrafiche.

PERSONE ESPOSTE POLITICAMENTE (C.D. PEP)

Si rimanda al Regolamento di Gestione della Persone Esposte Politicamente (c.d. PEP) tempo per tempo vigente.

CLIENTI A RISCHIO ALTO

La Società si avvale del software fornito da Temenos per la profilatura di rischio della clientela (cfr. par. Profilatura della clientela), attraverso il quale sono attribuiti specifici punteggi, a ciascun cliente, in funzione delle informazioni anagrafiche, dell'operatività e dei dati di relazione con la Società.

In base alle regole attualmente in vigore, sono considerati ad alto rischio i soggetti cui è attribuito un punteggio pari o superiore a 25 punti.

Il Delegato alla segnalazione di operazioni sospette può in ogni caso, ad esito del processo di analisi svolto dal medesimo, chiedere di innalzare prudenzialmente il profilo di rischio del soggetto analizzato di 25 punti, mantenendo traccia delle valutazioni effettuate.

L'incremento del profilo di rischio su richiesta del Delegato viene effettuato valorizzando apposito dato all'interno della procedura. L'eventuale rimozione di tale incremento può essere disposta solo dal Delegato, mantenendo traccia, delle valutazioni effettuate.

INDICI REPUTAZIONALI NEGATIVI Rileva, tra l'altro, la sussistenza di:

- procedimenti penali, quando questa informazione è notoria o comunque nota al destinatario e non coperta da obblighi di segretezza che ne impediscono l'utilizzo da parte del destinatario ai sensi del codice di procedura penale;
- procedimenti per danno erariale;
- procedimenti per responsabilità amministrativa ai sensi del decreto legislativo 8 giugno 2001, n. 231;
- sanzioni amministrative irrogate per violazione delle disposizioni antiriciclaggio a carico del cliente o del titolare effettivo.

I destinatari tengono conto anche di informazioni - pubblicamente accessibili - esterne al patrimonio informativo aziendale.
Nel valutare le notizie negative provenienti dai media o da altre fonti informative, i destinatari ne considerano la fondatezza e l'attendibilità basandosi, in particolare, sulla qualità e sull'indipendenza delle fonti informative e sulla ricorrenza delle informazioni.
Rilevano, tra l'altro, le informazioni relative all'attività esercitate, anche in passato, dal cliente e dal titolare effettivo e quelle riguardanti soggetti notoriamente legati al cliente o al titolare effettivo in virtù, ad esempio, di rapporti familiari o d'affari.

Nel caso di specie la perspective Banking Services & Controls, con riferimento alle richieste o ai provvedimenti ricevuti dalla Società da parte degli Organi Investigativi e dell'Autorità Giudiziaria provvede, alla ricezione dei medesimi, al relativo censimento nel gestionale di riferimento, affinché tale informazione sia tenuta in debito conto per la profilatura di rischio della clientela.
L'Unità provvede, inoltre, a comunicare tempestivamente alla Funzione Antiriciclaggio di Gruppo, tramite inserimento di apposito "dossier":

- le richieste provenienti dall'Autorità Giudiziaria, predisposte ai sensi del Codice Antimafia (accertamenti richiesti dall'Autorità Penale ai sensi della D. Lgs 159/2011 – Antimafia – fase delle indagini preliminari);
- le richieste provenienti dalle Autorità Giudiziarie, predisposte ai sensi della normativa antiriciclaggio (accertamenti richiesti dall'Autorità Penale ai sensi del D.Lgs 231/07 – Antiriciclaggio – fase delle indagini preliminari);
- i decreti di sequestro.

A seguito delle segnalazioni ricevute, la Funzione Antiriciclaggio di Gruppo avvia un'apposita istruttoria, raccordandosi con la perspective Banking Services & Controls, per l'esecuzione del processo di adeguata verifica rafforzata e sottoponendo la pratica al Delegato per le valutazioni di competenza.

Resta ferma la necessità di verificare la ricorrenza di nominativi nelle liste delle persone o degli enti associati ai fini dell'applicazione degli obblighi di congelamento previsti dai Regolamenti comunitari o dai decreti adottati ai sensi del decreto legislativo 22 giugno 2007, n. 109 (cfr. liste negative o *sanction list*). Per quanto attiene le verifiche si rimanda al par. Liste Negative.

RAPPORTI CONTINUATIVI INSTAURATI IN CIRCOSTANZE ANOMALE

Nel caso in cui il dipendente incaricato ravvisi, in fase di perfezionamento di un'operazione o di accensione di un nuovo rapporto continuativo, un elevato rischio di riciclaggio o finanziamento del terrorismo procede segnalarlo tempestivamente alla Funzione Antiriciclaggio di Gruppo. In particolare, deve essere opportunamente considerato il comportamento tenuto dal cliente o dall'esecutore come, ad esempio, quanto previsto dal par. Adeguata Verifica rafforzata della clientela.

CLIENTE SEGNALATO UIF O CON PROFILO DI RISCHIO INCREMENTATO DA DELEGATO

Qualora ad esito delle analisi svolte e delle valutazioni condotte dal Delegato alla segnalazione di operazioni sospette un cliente sia oggetto di segnalazione alla UIF, il sistema attribuisce un incremento di punteggio pari a 25 punti.

L'eventuale rimozione degli incrementi di punteggio relativi ai clienti segnalati può essere disposta solo dal Delegato, mantenendo traccia, delle valutazioni effettuate.

TIPO ATTIVITÀ ECONOMICA (C.D. TAE) A RILEVANTE ESPOSIZIONE RISCHIO CORRUZIONE

Si tratta, in particolare, di settori economici interessati dall'erogazione di fondi pubblici, anche di origine comunitaria, appalti pubblici, sanità, edilizia, commercio di armi, difesa, industria bellica, industria estrattiva, raccolta e smaltimento dei rifiuti, produzione di energie rinnovabili.

Il sistema di profilatura considera detti settori nelle elaborazioni *real time*, e vi sono indicatori e regole per quanto attengono le operazioni registrate sui rapporti continuativi. Nel caso di profilatura ad alto rischio derivante da operatività o da elementi soggettivi/oggettivi del cliente il sistema genera automaticamente un "case" che la perspective Banking Services & Controls provvede a comunicare tempestivamente alla Funzione Antiriciclaggio di Gruppo per gli approfondimenti del caso.
Le aree oggetto di analisi sono:

- origine dei fondi utilizzati nel rapporto;
- situazione economica (fonti di reddito) e patrimoniale;
- scopo e natura del rapporto rispetto alla/e operazione/i oggetto di analisi;
- eventuali relazioni di affari (es. partecipazioni societarie, cariche societarie, etc.);
- eventuali relazioni e i rapporti con altri soggetti che intrattengono legami senza averne lo status (es. intestatari di carte prepagate, titolari di altri conti correnti);
- eventuale presenza di c.d. *bad notice* da fonti pubbliche e/o da banche dati specialistiche;
- verifica match con banca dati tra CF cliente e CF_RUP da banca dati avvisi, i bandi e gli esiti di gara in formato aperto raccolti dalla Banca dati SCP - Servizio Contratti Pubblici[14].

A seguito delle segnalazioni ricevute, la Funzione Antiriciclaggio di Gruppo avvia un'apposita istruttoria, raccordandosi con la perspective Banking Services & Controls, per l'esecuzione del processo di adeguata verifica rafforzata e sottoponendo la pratica al Delegato per le valutazioni di competenza.

PAGAMENTI RICEVUTI DA TERZI PRIVI DI UN EVIDENTE COLLEGAMENTO CON IL CLIENTE O CON LA SUA ATTIVITÀ

Il sistema gestionale intercetta le operazioni in accredito che presentano un beneficiario indicato differente dall'intestatario del rapporto (vedi anche cfr. par. Controllo costante).

[14] http://dati.mit.gov.it/catalog/dataset/scp/resource/1f08fc66-0b04-4c1c-a398-cdb17f3ea8f4

Dette operazioni sono "scartate" dal sistema, e per ciascuna di esse il sistema genera un "case" che viene inviato alla attenzione della perspective Banking Services & Controls, che, dopo l'avvio dell'istruttoria ingaggia la Funzione Antiriciclaggio di Gruppo per eventuali approfondimenti laddove richiesti.

Le aree oggetto di analisi sono:

1) motivazione della operazione (rapporto con ordinante, causale etc…);
2) situazione economica (fonti di reddito) e patrimoniale;
3) scopo e natura del rapporto rispetto alla/e operazione/i oggetto di analisi;
4) eventuali relazioni di affari (es. partecipazioni societarie, cariche societarie, etc.);
5) eventuali relazioni e i rapporti con ordinante e beneficiario indicato nella operazione (qualora non vi siano riscontri dal controllo di cui al precedente punto);
6) eventuale presenza di c.d. *bad notice* da fonti pubbliche e/o da banche dati specialistiche;
7) eventuale supporto documentale (es. acquisizione giustificativo afferente l'operazione)

A seguito delle segnalazioni ricevute, la Funzione Antiriciclaggio di Gruppo avvia un'apposita istruttoria, raccordandosi con la perspective Banking Services & Controls, per l'esecuzione del processo di adeguata verifica rafforzata e sottoponendo la pratica al Delegato per le valutazioni di competenza ed al Responsabile della perspective Banking Services & Controls per le opportune valutazioni sulla possibilità di dare seguito alla operazione o respingere la stessa.

OPERATIVITÀ DA/VERSO PAESI TERZI AD ELEVATO RISCHIO GEOGRAFICO

Il sistema di profilatura considera dette operazioni nelle elaborazioni real time, e vi sono indicatori e regole per quanto attengono le operazioni registrate sui rapporti continuativi in base al paese. Nel caso di profilatura ad alto rischio derivante da operatività o da elementi soggettivi/oggettivi del cliente il sistema genera automaticamente un "case" che la perspective Banking Services & Controls provvede a comunicare tempestivamente alla Funzione Antiriciclaggio di Gruppo per gli approfondimenti del caso.
Le aree oggetto di analisi sono:

1) origine/destinazione dei fondi della/e operazione/i evidenziate;
2) situazione economica (fonti di reddito) e patrimoniale;
3) scopo e natura del rapporto rispetto alla/e operazione/i oggetto di analisi;
4) eventuali relazioni di affari (es. partecipazioni societarie, cariche societarie, etc.);
5) eventuali relazioni e i rapporti con ordinante/beneficiario della/e operazione/i evidenziate;
6) eventuale presenza di c.d. bad notice da fonti pubbliche e/o da banche dati specialistiche;
7) eventuale supporto documentale (es. acquisizione giustificativo afferente l'operazione)

A seguito delle segnalazioni ricevute, la Funzione Antiriciclaggio di Gruppo avvia un'apposita istruttoria, raccordandosi con la perspective Banking Services & Controls, per l'esecuzione del

processo di adeguata verifica rafforzata e sottoponendo la pratica al Delegato per le valutazioni di competenza.

Vedi anche rif. par. Controllo costante ed elenco paesi in APPENDICE 3.

ADEGUATA VERIFICA SEMPLIFICATA DELLA CLIENTELA

In presenza di un basso rischio di riciclaggio e finanziamento del terrorismo, la Società può applicare misure semplificate di adeguata verifica della clientela sotto il profilo della estensione e della frequenza degli adempimenti, nei confronti di soggetti e/o prodotti specificamente indicati dalla normativa primaria e dalle disposizioni attuative tempo per tempo vigenti.

L'applicazione di obblighi semplificati di adeguata verifica è comunque esclusa quando vi sia sospetto di riciclaggio o finanziamento del terrorismo e/o vi siano elementi di più elevata rischiosità.

Stante l'attuale perimetro target della clientela, la Società non prevede l'applicazione di obblighi semplificati.

ADEGUATA VERIFICA DELLA CLIENTELA – RICHIESTA ESEGUITA A TERZI SOGGETTI

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

MOTORE DI ADEGUATA VERIFICA DELLA CLIENTELA

Il processo di aggiornamento periodico della profilatura della clientela avviene con una frequenza commisurata al relativo livello di rischio, mediante conferma (o aggiornamento), da parte del cliente, dei dati acquisiti precedentemente (adeguata verifica) e mediante compilazione di apposito questionario di adeguata verifica rafforzata (rischi alti – vedi flow https://overflow.io/s/QRAODZG3?node=8051d71a).

Il processo di aggiornamento della profilatura è gestito informaticamente attraverso apposito strumento (cd. motore adeguata verifica). 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 secondo la tabella seguente:

- IRRILEVANTE – aggiornamento ogni 48 mesi;
- BASSO – aggiornamento ogni 36 mesi;
- MEDIO – aggiornamento ogni 24 mesi;
- ALTO – aggiornamento ogni 12 mesi.

- effettuare il ricalcolo automatico della data scadenza del profilo di rischio, a seguito della variazione del relativo livello, assumendo come riferimento la data dell'avvenuta variazione e del tempo trascorso dell'ultimo aggiornamento;

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 il dipendente incaricato rilevi che non sono più attuali le informazioni precedentemente acquisite.

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, il software 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 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.

PROCESSO DI COUNTDOWN

Il processo di countdown consiste nell'avvio di una serie di iniziative propedeutiche all'aggiornamento/conferma dei dati contenuti nella sezione Antiriciclaggio dei dati personali nella APP (e nel caso di cliente a rischio Alto anche dei dati previsti nella sezione di adeguata verifica rafforzata) e /o del documento identificativo partendo da 90 giorni antecedenti l'evento (scadenza documento e/o scadenza profilo di rischio).
Sono previsti:

- invio di notifiche push-app/email a 3, 2, 1 mesi precedenti alla scadenza, a 14 giorni dalla scadenza, il giorno in cui scade il documento e/o il profilo di rischio, mantenendolo in to-do-list in evidenza in homepage. **N.B.** Le notifiche successive non vengono inviate se l'utente carica un nuovo documento ai solleciti precedenti.
- notifica/email al 14-esimo giorno ed al 30-esimo giorno di operatività limitata per avvisare del blocco totale dell'operatività (e se saldo a zero, il conto verrà estinto di default).

Qualora il cliente non aggiorni i dati anagrafici obbligatori e/o il documento identificativo, la Società provvede:

- nei 90 giorni successivi all'evento (data di scadenza del profilo / data scadenza documento d'identità) il cliente potrà operare limitamente (non potrà aprire nuovi prodotti e/o aderire a nuovi servizi) a quanto già presente, fatto salvo la carta che viene bloccata;
- dal 91 giorno successivo all'evento e fino al 180 giorno al blocco delle funzionalità della APP[15];

[15] L'operatività del conto sarà bloccata per tutte le funzionalità al netto di:

- App in lettura
- Caricare un nuovo doc di identità
- Chiudere il conto

- decorsi 180 giorni, si procederà:
    - Se il saldo è zero, il conto viene chiuso automaticamente + invio estratto conto,
    - Se il saldo non è zero, resta "dormiente"

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.

E' compito del dipendente 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 di Gruppo secondo le modalità contenute nel Regolamento Segnalazione Operazioni Sospette.

(IV) ADEGUATA VERIFICA DELLA CLIENTELA – RICHIESTA RICEVUTA DA TERZI SOGGETTI

L'art. 26 del D.Lgs 231/2007 prevede che gli obblighi di adeguata verifica della Clientela, [cfr. comma 3: di cui all'art. 18 comma 1, lett. da a) a c)], possano essere assolti, pur in assenza del cliente, quando è fornita idonea attestazione da parte di particolari soggetti – intermediari e banche e loro succursali insediati in stati extracomunitari purché applichino misure e procedure equivalenti a quelle stabilite dal D.Lgs 231/2007 – con i quali i clienti abbiano rapporti continuativi in essere e siano già stati identificati di persona.
L'attestazione così prodotta deve essere trasmessa dal terzo attestante e non dal cliente, direttamente all'intermediario richiedente.
Tra gli intermediari richiedenti, che possono effettuare tutte le fasi dell'adeguata verifica, a eccezione del controllo costante dell'operatività sono ricompresi:

1) gli intermediari bancari e finanziari di cui all'art. 3, comma 2, del decreto antiriciclaggio, nonché le loro succursali insediate in paesi comunitari o quelle insediate in paesi terzi che soddisfano i requisiti previsti dall'articolo
26, comma 2, lettera d), del decreto antiriciclaggio;
2) gli intermediari bancari e finanziari comunitari;
3) gli intermediari bancari e finanziari aventi sede in paesi terzi che soddisfano i requisiti previsti dall'articolo 26, comma 2, lettera d), del decreto antiriciclaggio.

Ne consegue che qualora un cliente necessiti di una attestazione di "identificazione" da produrre ad un terzo ai fini antiriciclaggio, è suo compito attivarsi direttamente contattando la Società, oppure accordandosi con l'intermediario terzo richiedente affinché lo stesso provveda ad inviare apposita richiesta alla perspective Banking Services & Controls della Società.
Detto ufficio, una volta verificato che:

- il terzo richiedente rientri tra le categorie di cui ai succitati punti da 1) a 3);
- il cliente per conto del quale il terzo richiede l'attestazione sia con posizione anagrafica corretta ed aggiornata,

- Addebiti continuativi
- Addebiti automatici

- produrrà specifica attestazione (cfr. APPENDICE 4) allegando alla stessa la copia del documento di identità in corso di validità in possesso della Società. La richiesta di attestazione deve contenere:

a) i dati dell'intermediario richiedente e le modalità di trasmissione dell'attestazione;
b) le informazioni sulla natura e sullo scopo (i) del rapporto da aprire presso l'intermediario richiedente e/o (ii) dell'operazione occasionale da eseguire, ai fini dell'adempimento del relativo obbligo;
c) i dati identificativi del soggetto e copia di un documento di identità in corso di validità;

La Società non rilascia la lettera nel caso di richieste:

- prive delle informazioni e dei dati di cui sopra e/o qualora i dati di cui al punto c) non risultino essere coerenti con le verifiche svolte dalla Società;
- aventi ad oggetto clienti con posizione anagrafica non aggiornata (es. documento identità scaduto).
- né provvede a compilare, vidimare e ritrasmettere moduli prodotti da terzi.

(V) OBBLIGHI DI ASTENSIONE

Qualora la Società si trovi nella impossibilità oggettiva di effettuare l'adeguata verifica della clientela, si astiene dall'instaurare, eseguire ovvero proseguire il rapporto, le operazioni (c.d. obbligo di astensione) procedendo, se del caso, all'estinzione del rapporto continuativo già in essere e valutando se effettuare una segnalazione di operazione sospetta alla UIF. Prima di effettuare la segnalazione di operazione sospetta alla UIF e al fine di consentire l'eventuale esercizio del potere di sospensione, la Società si asterrà dall'eseguire le operazioni per le quali sospetta vi sia una relazione con il riciclaggio o con il finanziamento del terrorismo.

Nei casi in cui l'astensione non sia possibile in quanto sussiste un obbligo di legge di ricevere l'atto ovvero l'esecuzione dell'operazione per sua natura non possa essere rinviata o l'astensione possa ostacolare le indagini, permane l'obbligo di immediata segnalazione di operazione sospetta.
La Società si astiene dall'instaurare rapporti o eseguire operazioni e pone fine al rapporto continuativo già in essere con:

- clienti o potenziali clienti residenti in paesi esteri (clientela non in target);
- clienti o potenziali clienti cittadini Extra UE;
- operazioni con paesi esteri c.d. "ad alto rischio", come individuati dalla Società ed in linea con le previsioni della Capogruppo.

La Società si astiene altresì dall'offrire prodotti/servizi o dar corso ad operazioni che potrebbero favorire l'anonimato, ma non esclude in via preventiva e generalizzata la possibilità di aprire o mantenere Rapporti continuativi con specifiche categorie di clienti o potenziali clienti residenti o con regolare permesso di soggiorno in Italia, in ragione della loro esposizione potenzialmente elevata al rischio di riciclaggio, ma adotta processi rigorosi per valutare, caso per caso, il rischio associato al cliente o al potenziale cliente, mantenendo evidenza delle decisioni assunte.

E' fatta in ogni caso salva l'applicazione dell'articolo 35, comma 2 (ossia, dopo aver ricevuto l'atto o eseguito l'operazione, il Delegato alle SOS ne informerà immediatamente la UIF), nei casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto.

4. Prodotti/Servizi di terzi collocati da Flowe

Con riferimento ai prodotti/servizi collocati dalla Società, in base ad appositi accordi di distribuzione con società del Gruppo Mediolanum o con società terze, si elencano le specificità previste per i prodotti distribuiti.

In base ai vigenti accordi di distribuzione con controparti terze, il processo di identificazione dei soggetti sottoscrittori è curato dalla Società, secondo le modalità sopra illustrate (cfr. par. Identificazione della clientela).

La raccolta delle informazioni necessarie per lo svolgimento dell'adeguata verifica avviene tramite appositi questionari predisposti dalla Società nonché attraverso la documentazione del prodotto predisposta dalla società terza.

Nello specifico, i sottoscrittori, devono essere preventivamente identificati dalla Società analogamente a quanto previsto per i clienti della stessa

In ogni caso, la Società è tenuta a trasmettere alle società terze, su loro semplice richiesta:

- la documentazione e/o le informazioni necessarie ed aggiornate, fornite dalla clientela alla Società ai fini dell'adempimento dei predetti obblighi di adeguata verifica, ivi incluse le informazioni necessarie all'identificazione del titolare effettivo, ovvero ogni dato richiesto dalla normativa vigente;
- la documentazione comprovante l'avvenuto svolgimento delle suddette attività di adeguata verifica della clientela.

CONTROLLO COSTANTE

La Società svolge un controllo costante 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, avendo riguardo sia ai rapporti continuativi in essere sia alle operazioni specifiche eventualmente disposte, nonché mediante l'acquisizione di informazioni in sede di verifica o aggiornamento delle notizie ai fini dell'identificazione del cliente e dell'accertamento e valutazione della natura e dello scopo del rapporto o dell'operazione.
In APPENDICE 4 sono evidenziate le attuali regole impostate a sistema.

PROFILO DI RISCHIO

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.

La data di esecuzione del controllo costante è calcolata sulla base della data dell'ultimo aggiornamento anagrafico e/o del profilo di rischio di riciclaggio storicizzato mensilmente (il più alto a livello di Gruppo nel caso di clientela comune).
In caso di variazione del profilo di rischio, la data viene in automatico ricalcolata assumendo come riferimento la data dell'ultima adeguata verifica disponibile. Ai fini dell'esecuzione del controllo costante è prevista l'attivazione di alert automatici sull'APP nei confronti del cliente laddove manchino tre mesi alla scadenza del documento identificativo acquisito ovvero alla scadenza dell'ultimo controllo costante eseguito. Nello specifico:

- in caso di soggetto che abbia in scadenza il documento identificativo, è richiesto l'upload di documento identificativo in corso di validità (che verrà sottoposto a successivo controllo da parte della perspective Banking Services & Controls); • in caso di soggetto che abbia in scadenza l'adeguata verifica, è richiesta la conferma delle informazioni a disposizione della Società rivenienti dall'ultima controllo costante eseguito.

In caso di mancato aggiornamento dell'adeguata verifica o del documento identificativo entro le tempistiche definite, sono previste comunicazioni al cliente inerenti all'attivazione di successivi blocchi all'operatività sul rapporto.
Sono inoltre attivati specifici flussi informativi nei confronti della perspective Banking Services & Controls finalizzati al monitoraggio di tali posizioni. In presenza di elementi di anomalia ovvero di sospetto l'unità coinvolge la Funzione Antiriciclaggio di Gruppo per ulteriori approfondimenti e valuta se effettuare la segnalazione di una operazione sospetta al Delegato alle Segnalazioni di Operazioni Sospette.
Ove opportuno, le risultanze del controllo conducono a:

- l'effettuazione di più ampie e approfondite verifiche (anche all'applicazione dell'adeguata verifica rafforzata);
- l'aggiornamento di dati, delle informazioni e del profilo di rischio (con l'eventuale previsione di un incremento dello stesso);
- l'individuazione di anomalie e incongruenze che possono condurre alla segnalazione di operazioni sospette;
- il congelamento dei fondi;
- l'astensione dall'effettuazione dell'operazione;
- la chiusura del rapporto.

LISTE NEGATIVE

In costanza di rapporto continuativo, con periodicità giornaliera, è verificata in automatico la presenza del cliente e dell'eventuale genitore / tutore legale all'interno delle liste delle Persone Esposte Politicamente nonché delle cd. "liste negative".

Il controllo viene svolto tramite modulo FCM Temenos (funzionalità "Screen") sulle seguenti liste:

a) c.d. *sanction list* (OFAC, OCSE, ONU, EU),
b) PEP,
c) PIL,
d) Crime,
e) Lista Indesiderati,
f) Lista Appalti

Le liste di cui alinea a) sono fornite dal fornitore Temenos, mentre le liste da b) a d) sono fornite dal provider SGR Consulting, mentre la lista e) viene periodicamente importata (cadenza mensile/bimestrale) manualmente da scarico Cedacri e contiene i clienti indesiderati del Gruppo Mediolanum, mentre la lista Appalti contiene elenco dei soggetti aventi ruolo pubblico di assegnatari (RUP) gare di appalti (http://dati.mit.gov.it/catalog/dataset/scp - Il Servizio Contratti Pubblici è una delle banche dati nazionali a titolarità del Ministero delle Infrastrutture e Trasporti elencate nell'allegato B del D.Lgs n.97/2016 (art. 9) che modifica l'obbligo di pubblicazione previsto nella normativa sulla trasparenza D.Lgs n.33/2013 (art. 9bis)).

In particolare, a fronte di tali controlli automatici periodici, laddove sia generato un potenziale match con tali liste, viene attivata la perspective Banking Services & Controls che ne verifica la rispondenza, anche con l'ausilio della Funzione Antiriciclaggio di Gruppo laddove ritenuto necessario. In caso di conferma del match con:

- le cd. liste delle Persone Esposte Politicamente, la Società approfondisce la conoscenza della clientela mediante l'adozione di presidi rafforzati di adeguata verifica. Nello specifico, la perspective Banking Services & Controls contatta il cliente tramite chat al fine di recuperare, anche mediante upload di eventuale documentazione richiesta, ulteriori informazioni necessarie a valutare l'origine dei fondi impiegati nel rapporto e la relativa ragionevolezza in relazione all'attività svolta dal cliente e all'entità delle risorse economiche nella sua disponibilità. Il mantenimento del rapporto viene inoltre autorizzato dall'soggetto titolare di poteri di amministrazione o direzione ovvero di suo delegato o, comunque, di soggetto che svolge una funzione equivalente;
- le cd. *sanction list*, il mantenimento del rapporto viene bloccato e l'operatività non è più consentita. In tali casi, la perspective Banking Services & Controls coinvolge la Funzione Antiriciclaggio di Gruppo per le conseguenze del caso.

Misure di congelamento applicate ai sensi ex art. 7, comma 1, del D. Lgs. 22 giugno 2007, n. 109

Ai sensi delle previsioni normative qualora la Società rilevi un potenziale cliente presente nelle liste dei c.d. soggetti designati, il cui elenco, tempo per tempo vigente, contenuto nell'allegato I del

Regolamento UE n. 269/2014[16], provvede a darne tempestiva ed immediata comunicazione al Responsabile Antiriciclaggio al fine di valutare le eventuali implicazioni ed attivare la procedura di congelamento dei fondi e delle risorse economiche prevista.

La procedura di congelamento deve prevedere l'apposizione di immediati blocchi alla posizione del cliente (su anagrafe, per accesso all'App e alla operatività) al fine di garantire le previsioni normative in materia sul congelamento di fondi[17] e risorse economiche dello stesso.

Bisognerà quindi:

1. inviare alla struttura di Banking Services & Controls email dove richiedere la apposizione formale dei blocchi sulla posizione del cliente affinchè questi non possa in nessun modo eseguire "*movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione di portafoglio*",
2. inviare a mezzo PEC, una email urgente ai seguenti destinatari:
   - UIF - servizio.ari.cooperazione@bancaditalia.it
   - CSF - csf@pec.mef.gov.it ,
   - NSPV - rm0070000p@pec.gdf.it
3. Caricare apposito Dossier all'interno del Workflow AML al fine di effettuare la segnalazione di operazione sospetta,

Il testo della comunicazione di cui al punto 2, deve contenere[18] i nominativi e le denominazioni dei soggetti coinvolti, l'ammontare e la natura dei fondi o delle risorse economiche, nonchè i dati relativi a operazioni o rapporti, nonché ogni altra informazione disponibile riconducibili ai soggetti designati ai sensi del comma 2 della disposizione di cui in nota.

Ad esito della comunicazione, perverrà decreto di sequestro da parte Gdf (NSPV) con conseguente gestione da parte dell'Agenzia del Demanio (membro del CSF), ente che provvede all'amministrazione, alla custodia e alla gestione delle risorse congelate (i beni andranno intestati all'ente al pari del Fondo Unico Giustizia (c.d. FUG) che pertanto dovrà essere regolarmente censito).

OPERATIVITÀ CLIENTELA

La Società monitora in *real-time* l'esecuzione di eventuali operazioni anomale tramite l'utilizzo di Temenos FCM – Modulo Profile.

[16] Ampliato da ultimo dal Regolamento UE n.427/2022

[17] Art. 1, comma 2, lett. i) del D.Lgs. 231/2007 [18] Art. 1, comma 2, lett. i) del D.Lgs. 231/2007

[18] vedi Comunicato UIF del 04 marzo u.s. - https://uif.bancaditalia.it/pubblicazioni/comunicati/documenti/Comunicato_UIF_obblighi_comunicazione_misure_di_congelamento_russia.pdf

In determinati casi, è previsto che il sistema:

- blocchi l'esecuzione di operazioni da/verso paesi ritenuti dalla Società molto rischiosi (vedi par. Obblighi di astensione);
- non consenta di default l'esecuzione di talune operazioni (in via esemplificativa, non viene consentita operatività con Paesi terzi ad alto rischio ovvero operatività sottostante specifici settori a rischio, o su operazioni in accredito ricevute da terzi avente quale beneficiario della disposizione un soggetto diverso dal cliente titolare del rapporto).

Nella situazione di cui al secondo alinea precedente, l'operazione è scartata e la sua finalizzazione è subordinata all'acquisizione di ulteriori informazioni (obblighi rafforzati) necessarie a valutarne la ragionevolezza. In tal senso è previsto il contatto da parte della perspective Banking Services & Controls tramite chat nei confronti del cliente al fine di recuperare - anche mediante *upload* di ulteriore documentazione - le informazioni necessarie alle determinazioni del caso.

Sono posti altresì limiti ad alcuna operatività, nel caso si evidenzia:

Ricariche con carta di credito (operazioni Vpos)

Entità	**Tipo verifica**	**Timing**	**OK/KO**	**Soglia negata**
User ID	Nr. transazioni	24h	OK	5
User ID	Importo transazioni	24h	OK	1.500 euro (cumulato)
Indirizzo IP	15 minuti	OK + KO	1	

E' altresì stata attivata una Black List di esercenti (*merchant*) bloccati da SIA sul *Payment Getaway* su richiesta di Flowe.

5. Normativa di riferimento

Nel presente capitolo si richiama il contesto normativo nel quale opera il presente Regolamento di processo.

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

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 indicatori di anomalia emanati dalla UIF e le Disposizioni attuative emanate dalla Banca d'Italia.

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

- Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo;
- Disposizioni in materia di adeguata verifica della Clientela di Banca d'Italia;
- Disposizioni per la conservazione e la messa a disposizione dei documenti, dei dati e delle informazioni per il contrasto del riciclaggio e del finanziamento del terrorismo.

Si riportano, anche gli Orientamenti EBA:

- GL/2021/02 - del 1° marzo 2021, ai sensi dell'articolo 17 e dell'articolo 18, paragrafo 4, della direttiva (UE) 2015/849 sulle misure di adeguata verifica della Cclientela e sui fattori che gli enti creditizi e gli istituti finanziari dovrebbero prendere in considerazione nel valutare i rischi di riciclaggio e finanziamento del terrorismo associati ai singoli rapporti continuativi e alle operazioni occasionali («Orientamenti relativi ai fattori di rischio di ML/TF»), che abrogano e sostituiscono gli orientamenti JC/2017/37;,
- GL/2022/05 – del 14 giugno 2022, sulle politiche e le procedure relative alla gestione della conformità e al ruolo e alle responsabilità del responsabile antiriciclaggio ai sensi dell'articolo 8 e del capo VI della direttiva (UE) 2015/849, dove specificano il ruolo, i compiti e le responsabilità del responsabile della conformità ai requisiti in materia di antiriciclaggio e contrasto del finanziamento del terrorismo (AML/CFT), dell'organo di gestione e dell'alto dirigente incaricato della conformità ai requisiti in materia di AML/CFT nonché le politiche, i controlli e le procedure interni ai sensi degli articoli 8, 45 e 46 della direttiva (UE) 2015/849.

In data 14 giugno 2022 l'EBA ha emanato gli Orientamenti sulle politiche e le procedure relative alla gestione della conformità e al ruolo e alle responsabilità del Responsabile Antiriciclaggio ai sensi dell'articolo 8 e del capo VI della direttiva (UE) 2015/849, che specificano il ruolo, i compiti e le responsabilità del responsabile della conformità ai requisiti in materia di antiriciclaggio e contrasto del finanziamento del terrorismo (AML/CFT), dell'organo di gestione e dell'alto dirigente incaricato della conformità ai requisiti in materia di AML/CFT nonché le politiche, i controlli e le procedure interni ai sensi degli articoli 8, 45 e 46 della direttiva (UE) 2015/849. Nell'ambito di tali orientamenti al paragrafo 43 è stato previsto l'obbligo per l'alta dirigenza di acquisire il parere del Responsabile Antiriciclaggio prima di adottare una decisione definitiva sull'accettazione di nuovi Clienti ad alto rischio o sul mantenimento di rapporti d'affari con Clienti ad alto rischio.

Banca d'Italia ha recepito questa disposizione nelle Disposizioni in materia di organizzazione, procedure e controlli interni per finalità antiriciclaggio del 26 marzo 2019 ('Disposizioni'), prevedendo che quando la decisione di avviare o proseguire un rapporto continuativo è sottoposta per legge all'autorizzazione di un alto dirigente, questi acquisisce il parere preventivo della Funzione Antiriciclaggio. Il Provvedimento attuativo delle dispozioni entrerà in vigore il prossimo 14 novembre 2023.

NORMATIVA INTERNA

Il presente Regolamento fa parte del corpo normativo della Società insieme ai seguenti altri documenti:

- La Policy sul contrasto al riciclaggio e al finanziamento del terrorismo ha quale principale obiettivo quello di definire:
    - le regole di governo, i ruoli e le responsabilità in materia di contrasto ai rischi di riciclaggio e finanziamento del terrorismo da adottare nell'ambito del Gruppo;
    - le linee guida di Gruppo per il contrasto ai rischi di riciclaggio e finanziamento del terrorismo.

  I principi richiamati nella policy trovano attuazione nella documentazione interna di dettaglio (es. regolamenti di processo, procedure operative etc.), nella quale sono meglio declinati i compiti, le attività operative e di controllo, alla base del rispetto dei principi e delle normative in tema di presidio del rischio di riciclaggio e antiterrorismo.
- il Regolamento della Funzione Antiriciclaggio di Gruppo, che illustra i principî guida, l'architettura organizzativa, i processi e gli strumenti adottati dalla Funzione Antiriciclaggio di Gruppo per adempiere ai propri compiti;
- Il Regolamento del processo di segnalazione di operazioni sospette, in cui sono descritti i principî guida, l'architettura organizzativa e le interdipendenze alla base del processo di "Segnalazione delle operazioni sospette";
- il Regolamento del processo dei controlli di secondo livello svolti dalla Funzione Antiriciclaggio di Gruppo, in cui sono descritte le fasi dei processi inerenti la tracciatura dei controlli di secondo livello in materia di AML, ivi compresi quelli relativi alla conservazione e registrazione, identificando eventuali azioni a mitigazione della rischiosità rilevata;
- il Regolamento di gestione delle Persone Esposte Politicamente (c.d. PEP), in cui sono descritte le diverse fasi del processo per la corretta gestione della clientela che rientra nelle

fattispecie di Persone Esposte Politicamente come previsto dalla normativa vigente, tenuto conto altresì delle "buone prassi" richiamate nella menzionata comunicazione della Banca d'Italia, nonché richiamare ruoli e responsabilità degli attori coinvolti nel processo, in relazione all'assetto organizzativo, ai compiti e alle responsabilità;

- i manuali operativi interni alla Funzione Antiriciclaggio di Gruppo, che descrivono approfonditamente i processi operativi di dettaglio e gli elementi alla base dei modelli di presidio del rischio di riciclaggio e finanziamento del terrorismo;
- le procedure operative delle unità di primo livello che gestiscono l'amministrazione e la gestione concreta dei rapporti con la clientela in materia di gestione dei rischi e di prevenzione e presidio del rischio di riciclaggio e finanziamento del terrorismo.

APPENDICE 1

Elenco puntuale dei controlli applicativi sul processo di onboarding

App Flowe	
Sotto processo	**Controllo**
Registrazione in app	Blocco del processo se rilevato numero di cellulare con prefisso diverso da +39
Registrazione in app	Impossibilità di modifica dei dati (carta d'identità o passaporto elettronico) acquisiti tramite NFC
Presa visione materiale informativo	Blocco del processo se non vengono effettuate le prese di visione del materiale informativo e privacy
Inserimento dati personali e documentazione di riconoscimento	Blocco del processo se rilevata residenza anagrafica diversa da Italia

Inserimento dati personali e documentazione di riconoscimento	Blocco del processo in caso di inserimento, da parte del cliente, di un codice fiscale che non rispetta le regole di formattazione del codice fiscale italiano
Inserimento dati personali e documentazione di riconoscimento	Blocco del processo in caso di incongruenza di numero identificativo del carta di identità (elettronica / cartacea), limitato alla verifica della lunghezza
Identificazione del cliente	Blocco del processo se il video selfie non rispetta le indicazioni fornite in app (chiamata verifica liveness)
Questionario AML	Blocco del processo se l'utente si è identificato come US person

P0	
Sotto processo	**Controllo**
Registrazione in app	Blocco del processo in caso di mancata corrispondenza tra codice OTP ricevuto via SMS e codice OTP inserito dal cliente

Registrazione in app	Blocco del processo in caso di mancata corrispondenza tra codice OTP ricevuto via e-mail e codice OTP inserito dal cliente
Registrazione in app	Blocco del processo in caso di recapiti (numero di cellulare, e-mail) già registrati ed assegnati ad altri clienti
Inserimento dati personali e documentazione di riconoscimento	Blocco del processo in caso di codice fiscale già registrato in anagrafica
Inserimento dati personali e documentazione di riconoscimento	Blocco del processo se età rilevata è minore di 12 anni
Identificazione del cliente	Sospensione del processo se età rilevata è maggiore di 89 anni. Il processo può riprendere solo a seguito di una verifica approfondita da parte di un operatore
Registrazione genitore/ tutore / curatore	Blocco del processo se la differenza di età fra genitore / tutore e minore risulta essere minore di 15 anni
Registrazione genitore/ tutore / curatore	Blocco del processo se vengono rilevati tutori / curatori già registrati in anagrafica ed assegnati a 5 o più minori

Identificazione del cliente	Blocco del processo se rilevata cittadinanza appartenente a paese non presente in una whitelist definita
Identificazione del cliente	Blocco del processo se rilevato paese di nascita appartenente ai paesi in Black List oppure Sospensione del processo se rilevato paese di nascita appartenente ai paesi in Grey List. Il processo può riprendere solo a seguito di una verifica approfondita da parte di un operatore
Inserimento dati personali e documentazione di riconoscimento	Blocco del processo se rilevato documento di identità già associato ad altri clienti
Identificazione del cliente	Sospensione del processo se l'esito dell'algoritmo di **ID-DOCUMENT MANAGER** sul documento di identità cartaceo non raggiunge la soglia del 70% di veridicità. Il processo può riprendere solo a seguito di una verifica approfondita da parte di un operatore
Identificazione del cliente	Sospensione del processo se l'esito dell'algoritmo (biometrico) di *age mismatch* tra foto presente sul documento e immagine del volto acquisita tramite video selfie risulta essere superiore a 20 anni. Il processo può riprendere solo a seguito di una verifica approfondita da parte di un operatore
Inserimento dati personali e documentazione di riconoscimento	Blocco del processo se l'esito dell'algoritmo (biometrico) di face manager raggiunge la soglia del 80% di corrispondenza fra volto presente nel video selfie e database dei volti presenti in anagrafica di tutti i clienti che hanno effettuato o stanno effettuando il processo di onboarding oppure

	Sospensione del processo se l'esito dell'algoritmo (biometrico) di face manager applicato ad un minore raggiunge la soglia dell'80% di corrispondenza fra volto presente nel video selfie e database dei volti presenti in anagrafica. Il processo può riprendere solo a seguito di una verifica approfondita da parte di un operatore
Inserimento dati personali e documentazione di riconoscimento	Sospensione del processo se l'esito dell'algoritmo (biometrico) di face matching (tramite funzionalità del face manager) restituisce il parametro "*IsIdentical=False*" confrontando le immagini acquisite tramite video selfie e la foto presente nel documento identificativo.

IQP	
Sotto processo	**Controllo**
Identificazione del cliente	Blocco o sospensione del processo in caso di non veridicità del documento elettronico (carta di identità e passaporto) inviato, tramite lettura MRZ del codice ICAO e verifica *check digit*. In caso di sospensione, il processo può riprendere solo a seguito di una verifica approfondita da parte di un operatore
Asserzione di identità	Sospensione del processo se il numero di modifiche manuali effettuate dal cliente risultano essere maggiori al 50% dei dati letti correttamente via OCR. Il processo può riprendere solo a seguito di una verifica approfondita da parte di un operatore
Identificazione del cliente	(Controllo performato tramite SDK): Blocco del processo se l'esito dell'algoritmo (biometrico) di *face matching* non raggiunge la soglia del 75% di corrispondenza fra volto presente nel video selfie e foto rilevata sul documento di identità oppure Sospensione del processo se l'esito dell'algoritmo (biometrico) di *face matching* supera la soglia del 99,8% di corrispondenza fra volto presente nel video selfie e foto rilevata sul documento di identità. Il processo può riprendere solo a seguito di una verifica manuale da parte di un operatore

Experian	
Sotto processo	**Controllo**
Asserzione di identità	Blocco del processo se il codice fiscale del prospect trova corrispondenza nella banca dati dando un esito positivo in caso di protesto
Asserzione di identità	Blocco del processo se il codice fiscale del prospect trova corrispondenza nella banca dati dando un esito positivo in caso di pregiudizievole
Asserzione di identità	Blocco del processo se numerazione carta di identità/passaporto (elettronico o cartaceo) o patente non risultano formalmente congruenti
Asserzione di identità	Sospensione del processo se la data di rilascio della carta di identità è corrispondente ad una festività (comprese le festività comunali) o una data elettorale
Asserzione di identità	Sospensione del processo se la data di rilascio della carta di identità è incongruente con la data di scadenza
Asserzione di identità	Sospensione del processo se il passaporto risulta scaduto

Asserzione di identità	Sospensione del processo se la patente è stata emessa in un giorno festivo

FCM	
Sotto processo	**Controllo**
Adeguata verifica e controllo liste	Sospensione del processo se l'utente appartiene ad una delle seguenti categorie: - PEP - PIL - Lista Indesiderati - Appalti - Nominativi (Liste fornite periodicamente da fornitore SGR Consulting con tutti i soggetti che sulla base di articoli di note testate giornalistiche che riportano i soggetti coinvolti in diversi reati ad. Es. truffa, spaccio, mafia, etc.) - "Sanction list" (ONU, EU, SDN, OFAC...) - Embargo (Lista di paesi soggetti a limitazioni). Il processo può riprendere solo a seguito di una verifica approfondita da parte di un operatore

TOP	
Sotto processo	**Controllo**
Firma e ricezione copia contratti	Blocco del processo in caso di mancata corrispondenza tra codice OTP ricevuto sul numero di cellulare, per la firma digitale del contratto

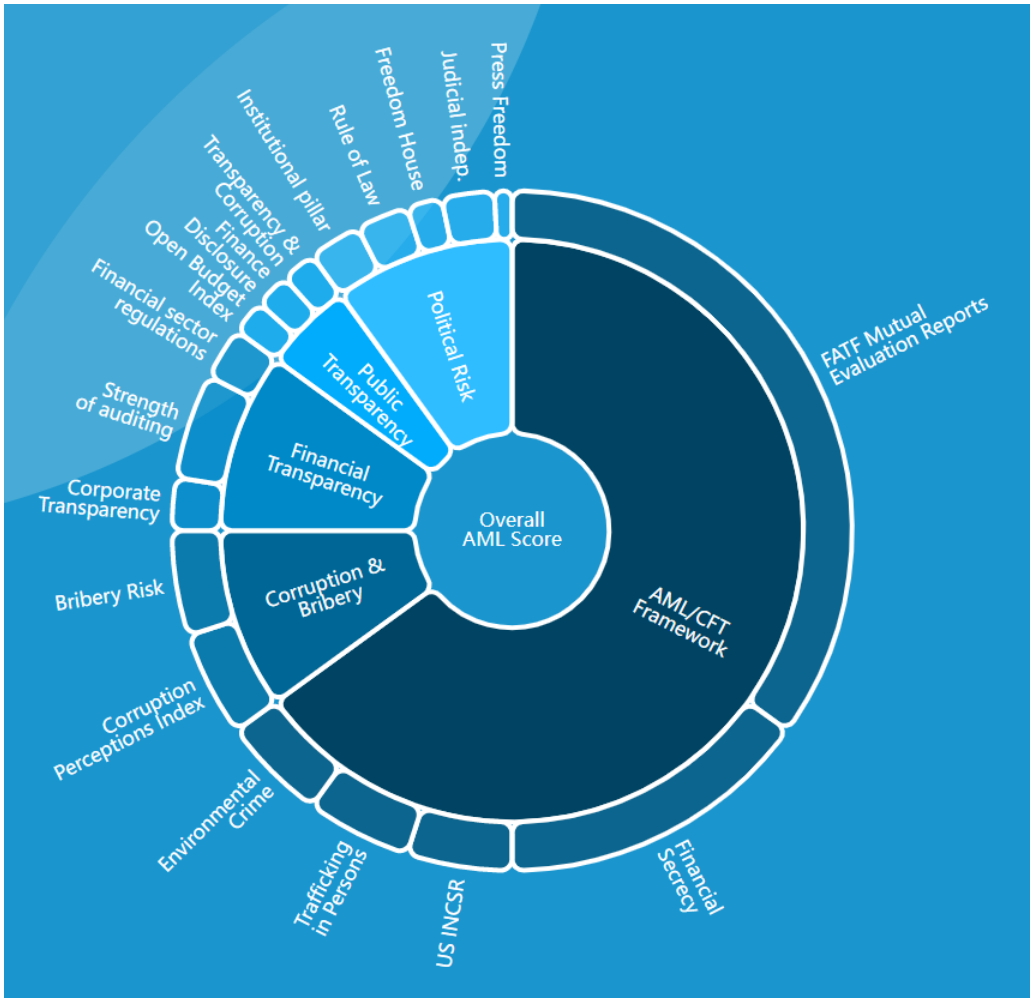
A seguito dei sovrascritti controlli applicativi vengono svolte le seguenti attività di controllo approfondite e svolte manualmente da un operatore:

- IQP: Verifica da parte di un operatore di tutti gli “alert” generati dai controlli automatici in caso di sospensione del processo (vedi sopra i dettagli dei controlli applicativi che generano sospensione del processo e quindi semaforo giallo in IQP).
- FCM: Verifica da parte di un operatore di tutti gli “alert” generati dai controlli automatici in caso di sospensione del processo (vedi sopra i dettagli dei controlli applicativi che generano sospensione del processo e quindi semaforo giallo in FCM).
- Fanbase: o Verifiche ex-post da parte di un operatore se durante l'onboarding l'utente maggiorenne dichiaratosi inizialmente come "tutore / curatore" ha in seguito modificato la sua scelta in "genitore";
    - o Verifiche aggiuntive da parte di un operatore sul codice ICAO

APPENDICE 2

Il file è riservato e deve essere richiesto alla Funzione Antiriciclaggio di Gruppo

APPENDICE 3


Overall AML Score
AML/CFT Framework
Political Risk
Public Transparency
Financial Transparency
Corruption & Bribery
FATF Mutual Evaluation Reports
Financial Secrecy
US INCSR
Trafficking in Persons
Environmental Crime
Corruption Perceptions Index
Bribery Risk
Corporate Transparency
Strength of auditing
Financial sector regulations
Open Budget Index
Disclosure
Finance
Corruption
Transparency &
Institutional pillar
Rule of Law
Freedom House
Judicial indep.
Press Freedom

Domain 1: Quality of AML / CFT Framework (65%)

- FATF: Mutual Evaluation Reports and Follow-up Reports (35%)
- Tax Justice Network: Financial Secrecy Index (15%)
- US State Department: International Narcotics Control Strategy Report (INCSR) (5%)
- US State Department: Trafficking in Persons Report (5%)
- Global Organized Crime Index – Flora, fauna, non-renewable resources (5%)

Domain 2: Corruption Risk (10%)

- Transparency International: Corruption Perceptions Index (5%)
- TRACE: Bribery Risk Matrix (5%)

Domain 3: Financial Transparency and Standards (10%)

- World Bank: Extent of Corporate Transparency Index (2.5%)
- WEF: Global Competitiveness Report – Strength of auditing and reporting standards (5%)
- World Bank: IDA Resource Allocation Index – Financial sector regulations (2.5%)

Domain 4: Public Transparency and Accountability (5%)

- International IDEA: Political Finance Database – Political disclosure (1.66%)
- International Budget Partnership: Open Budget Index – Budget transparency score (1.66%)
- World Bank: IDA Resource Allocation Index – Transparency, accountability and corruption in the ublic sector (1.66%)

Domain 5: Legal and Political Risk (10%)

- Freedom House: Freedom in the World – political rights and civil liberties (1.67%)
- Reporters Without Borders: World Press Freedom Index (0.83%)
- WEF: Global Competitiveness Report – Institutional pillar (2.5%)
- WEF: Global Competitiveness Report – Judicial independence (2.5%)
- World Justice Project: Rule of Law Index (2.5%)

Per maggiori dettagli si rimanda al sito istituzionale : https://index.baselgovernance.org/methodology

APPENDICE 4

Spett.le
[DATI INTERMEDIARIO RICHIEDENTE]
Indirizzo PEC: [email PEC]

Basiglio, 11 maggio 2021

Oggetto: Attestazione ai sensi ex art. 26 D. Lgs. 231/2007

Con la presente si attesta che il Cliente:

Cognome:
Nome:
Sesso:
Luogo di nascita:
Data di nascita:
Codice Fiscale:
Residenza:
Professione:
Documento di riconoscimento (**in allegato**): TIPO DOCUMENTO E NUMERO rilasciata da INDICARE in data GG/MM/AAAA con scadenza GG/MM/AAAA

è stato dalla scrivente identificato direttamente, ai sensi art.19, comma 1, lett. a), punto 2[19] del D.lgs. 231/2007, a valere su un rapporto continuativo attualmente in essere, del quale il Cliente risulta titolare, ed in relazione al quale sono state acquisite le informazioni sopra riportate.

[19] L'obbligo di identificazione si considera assolto, anche senza la presenza fisica del cliente, nei seguenti casi:

Si dà inoltre atto che il Cliente, alla data della presente, in base alle risultanze in nostro possesso, non risulta o risulta persona politicamente esposta ai fini dell'art. 1, lett. dd) del D. Lgs. 231/2007.

Come richiesto dal Cliente, il presente documento è rilasciato ai fini di [DESCRIZIONE OPERAZIONE RICHIESTA]. L'importo dovrà essere accreditato a favore dell'IBAN [IBAN FLOWE] a lui intestato.

Nel rimanere a disposizione per ogni ulteriore approfondimento, si porgono distinti saluti.

FLOWE S.P.A. – SOCIETÀ BENEFIT

HAPPINESS & SERVICE

CRISTINA TONIAZZO

APPENDICE 5

Il file è riservato e deve essere richiesto alla Funzione Antiriciclaggio di Gruppo

---

1) [*omissis*];
2) per i clienti in possesso di un'identità digitale, con livello di garanzia almeno significativo, nell'ambito del Sistema di cui all'articolo 64 del predetto decreto legislativo n. 82 del 2005, e della relativa normativa regolamentare di attuazione, nonché di un'identità digitale con livello di garanzia almeno significativo, rilasciata nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'articolo 9 del regolamento UE n. 910/2014, o di un certificato per la generazione di firma elettronica qualificata o, infine, identificati per mezzo di procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale;