PROCEDURA OPERATIVA

Onboarding cliente ed apertura conto di pagamento

Procedura emessa il 13/12/2023

Owner della procedura: Perspective Banking Services e Controls

SOMMARIO

1 OBIETTIVO DEL DOCUMENTO

Obiettivo del presente documento è illustrare il processo di *onboarding* della clientela ed apertura del conto di pagamento Flowe. In particolare, la procedura descrive:

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

Facendo riferimento alla tassonomia dei processi aziendali, il processo in esame è classificato nell'ambito dei processi di *Marketing*/ Commerciali / *Customer Relations*, secondo l'alberatura dei processi adottati dalla Società, come di seguito riportato:

2.00PROCESSI DI MARKETING/COMMERCIALI/CUSTOMER RELATIONS

2.05GESTIONE ANAGRAFE GENERALE CLIENTI

2.05.01 ONBOARDING CLIENTE E APERTURA CONTO

1.1. AMBITO DI APPLICAZIONE

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

1.2. AGGIORNAMENTO DEL DOCUMENTO

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

2 DEFINIZIONI

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

- **AML** (*Anti Money Laundering*): dicitura inglese (in italiano Antiriciclaggio) con cui si intende l'azione preventiva e la lotta al riciclaggio di beni, denaro o altre utilità in genere. L'attività di riciclaggio in sé e per sé consiste nell'investire capitali provenienti da reato all'interno di attività lecite, così da rendere difficoltosa la loro identificazione. Attraverso questo meccanismo, ogni bene frutto di attività illecita (traffico di stupefacenti, evasione fiscale, rapina, sequestro o qualsivoglia reato non colposo) viene "ripulito" dal suo alone di illiceità e reintrodotto nel circolo economico attraverso sbocchi perfettamente legali.
- ***Know Your Customer* - KYC:** insieme di procedure che, conformemente al D.Lgs. 231/2007, devono essere attuate anche dagli IMEL, per acquisire dati certi e informazioni sull'identità della clientela. La Società è quindi tenuta a verificare l'identità del cliente e ad acquisire su di lui informazioni che aiutino a valutare il rischio di riciclaggio di denaro o finanziamento alla criminalità. La procedura non comprende la sola verifica dell'identità ma anche l'acquisizione di tutte quelle informazioni che dovrebbero consentire di valutare l'esposizione ad eventuali rischi di riciclaggio e finanziamento al terrorismo, su cui la Società dovrà effettuare un controllo costante.
- **Non US Person:** cliente non soggetto al Fisco Statunitense in base alla normativa FATCA (Foreign Account Tax Compliance Act) ovvero non avente nessuno dei 7 indizi (US Indicia)[1].
- **Persona Politicamente Esposta - PEP:** qualsiasi persona che occupi (o abbia occupato) una posizione pubblica preminente/importante, o che sia strettamente collegata o in rapporto di parentela diretto con una persona in tale posizione. La Società identifica come PEP le persone fisiche che occupano, o che hanno cessato di occupare da meno di un anno, le cariche pubbliche indicate previste da decreto antiriciclaggio, nonché i loro familiari e coloro che con i predetti intrattengono notoriamente stretti legami ai sensi delle previsioni dell'art. 1, comma 2, lett. dd) del D.Lgs. 231/2007 tempo per tempo vigente.
- **Perspective:** Unità Organizzativa di Flowe.
- **Politici Italiani Locali - PIL:** qualsiasi persona che occupi (o abbia occupato) una carica politica in Italia a livello regionale, provinciale, comunale e delle città metropolitane.
- **Lista Appalti:** si intende quell'elenco di soggetti aventi ruolo pubblico di assegnatari (RUP) nelle gare di appalti.
- **Lista Indesiderati:** si intende quell'insieme di liste che la Società utilizza come fonte allo scopo di identificare eventuali profili indesiderati di *prospect* e/o clienti a livello di Gruppo.
- ***Black-list*:** si intende quell'insieme di liste che la Società utilizza come fonte allo scopo di identificare eventuali profili indesiderati, quali ad esempio liste dei protestati, di soggetti con carichi penali pendenti etc.
- **Adeguata Verifica Rafforzata** (di seguito anche AVR): le misure rafforzate di adeguata verifica (ai sensi del D.Lgs. 231/2007) si applicano quando sussiste un elevato rischio di riciclaggio e di

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

finanziamento del terrorismo, per effetto di specifiche previsioni normative o di una autonoma valutazione dell'intermediario. Le misure rafforzate di adeguata verifica della clientela vengono attuate: approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto; acquisendo informazioni aggiuntive sul cliente; intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale.

- **Pregiudizievoli:** sono atti che colpiscono i beni limitandone l'uso e/o la proprietà. Sono rilevate quotidianamente dalle Conservatorie dei registri immobiliari. Rientrano nelle pregiudizievoli: decreti ingiuntivi, sequestri conservativi, ipoteche, pignoramenti.
- **Protesto:** è l'atto attraverso il quale un Pubblico Ufficiale autorizzato, constata la mancata accettazione di una cambiale tratta o il mancato pagamento di una cambiale, di un vaglia cambiario, di un assegno bancario o postale. Gli ufficiali levatori, alla fine di ogni mese, devono trasmettere alla Camera di Commercio competente per territorio l'elenco dei protesti verbalizzati e i dati del debitore contro il quale ogni protesto è levato in modo da poter essere identificato.
- **Piattaforma IQP:** Strumento a supporto del processo di KYC, dell'*outsourcer* InfoCert.
- **Semaforo giallo in IQP:** il processo di *onboarding* risulta pendente in attesa della valutazione di un operatore.
- **Semaforo rosso in IQP:** il processo di *onboarding* ed apertura conto termina e al soggetto viene notificato il diniego dell'apertura del conto in App e via e-mail.
- **Transaction Alert manager-Gateway SIC**: sezione FMC dedicata agli *alert* di *onboarding* (es. liste PEP, PIL).
- **Piattaforma SGR**: Piattaforma utilizzata al fine di verificare la presenza di notizie di reato e/o altre notizie afferenti al *prospect*/cliente (es: assessore comunale; dirigente agenzia del demanio).
- **Input**: profilo base dell'operatore FCM. Attualmente assegnato al *Team Operations Flowe* di Banca Mediolanum.
- **Chief Service Senior:** profilo da supervisore assegnato al Team AML.
- **Head of Chief Service:** profilo del Responsabile Unità *Banking Services e Controls*.
- **Prospect:** è una persona che ha iniziato il processo di *onboarding* per l'apertura del conto.

3 STRUMENTI A SUPPORTO DEL PROCESSO

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

3.1 PIATTAFORMA IQP

Durante il processo di *onboarding* Flowe si avvale della piattaforma applicativa IQP "*Strumento a supporto del processo di KYC"* dell'*outsourcer* InfoCert, la quale fornisce supporto per la gestione di alcuni *steps* del processo di *onboarding* ed apertura conto di pagamento, con riferimento alla verifica dell'identità del *prospect*.

Nello specifico, attraverso questo strumento la *Perspective Banking Services e Controls – Team AML* - anche mediante gli operatori del *Team Operations Flowe* di Banca Mediolanum, valuta l'esito del processo di KYC, effettua controlli manuali, accetta o respinge la richiesta di *onboarding* del soggetto. Inoltre, la *Perspective Banking Services e Controls - Team AML* -

approfondisce laddove necessario inviando “adeguata verifica rafforzata”.

3.2 TOP

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

3.3 LEGAL DOC

“Legal DOC” è la 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. Per “pratiche finalizzate” s’intende che è necessario che il Prospect, nel processo di onboarding, venga identificato; in caso contrario, non essendo giunta a compimento l’asserzione d’identità, non è possibile mantenere dei dati riferiti a soggetti non qualificabili. Si rappresenta, inoltre, che tale logica è seguita anche dagli applicativi di Flowe.

3.4 TEMENOS - FCM

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

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

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

3.5 P0 PLATFORM

P0 è la Piattaforma della Società (*full cloud* – Microsoft Azure) sulla quale è implementata la logica applicativa. Mediante la piattaforma è possibile integrare sistemi esterni.

P0 supporta il processo di *onboarding* effettuando dei controlli sia sui dati acquisiti tramite App Flowe sia comunicando con le piattaforme messe a disposizione da InfoCert oltre a svolgere controlli quali “*ID document manager*”, "*Face manager*" e “*Unwanted subject*” utilizzando la tecnologia di intelligenza artificiale fornita da Microsoft.

3.6 APP FLOWE

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

Tramite l'App Flowe il *prospect*:

- inizia il processo di *onboarding* fornendo tutti i dati e le informazioni necessarie al fine dell'apertura del conto Flowe e dell'Adeguata Verifica;
- usufruisce di un sistema *chatbot* al fine di ricevere supporto anche durante le varie fasi del processo di *onboarding*;
- usufruisce di un sistema di notifiche in App che gli consente di essere informato sull'esito dell'*onboarding*;

compila il modulo di Adeguata Verifica Rafforzata in caso di profilo di rischio medio o alto.

3.7 FANBASE

Fanbase è la 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*).

3.8 SIA CRYSTAL GATE (GUI)

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

Nel presente processo di *onboarding* e apertura del conto, GUI si occupa dell'associazione della carta di debito al cliente - tipologia di carta (fisica o virtuale), dettagli dell'intestatario della carta (luogo di spedizione, dati anagrafici e residenza)- .

3.9 EXPERIAN

Experian è la 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").

3.10 DIFFERENT DEVICE COUNTS USERS

In questa Dashboard si evidenziano utenti che hanno sottoscritto il Contratto, che risultano avere diversi codici di Device in *P0 (Platform)* e in *App Flowe*. Si tratta di un'evidenza che segnala possibili tentativi di frode in *Onboarding*. I dati vengono utilizzati dagli operatori del Team AML Monitoring per effettuare approfondimenti in base ad ulteriori indici di anomalia presenti sulle

posizioni dei clienti (es. numero di telefono, mail, selfie ecc.).

4 ATTORI, RUOLI E RESPONSABILITÀ

Di seguito sono indicati i principali attori, coinvolti nel processo di *onboarding* ed apertura Conto di pagamento della clientela di Flowe e i relativi ruoli e responsabilità nell'ambito delle attività descritte.

4.1 FUNZIONE ANTIRICICLAGGIO

La *Funzione Antiriciclaggio*, nell'ambito del presente processo, fornisce, qualora necessario, le linee guida e/o consulenza alla *Perspective Banking Services e Controls – Team AML* nelle varie fasi del processo di acquisizione dei nuovi clienti.

Identifica le norme applicabili individuando procedure e controlli al fine di contrastare rischi di riciclaggio e di finanziamento del terrorismo; predispone annualmente una Relazione sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale, da sottoporre al Collegio Sindacale, all'Amministratore Delegato ed al Consiglio di Amministrazione della Società; valida e aggiorna la normativa interna, le policy ed i regolamenti in materia di antiriciclaggio e antiterrorismo.

4.2 RESPONSABILE ANTIRICICLAGGIO

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

4.3 DELEGATO ALLE SEGNALAZIONI DELLE OPERAZIONI SOSPETTE

Valuta le segnalazioni di operazioni sospette ricevute, autorizza la trasmissione delle segnalazioni ritenute fondate alla UIF e risponde tempestivamente ad eventuali richieste di approfondimento; comunica con le modalità operative ritenute più appropriate, l'esito della propria valutazione all'*outsourcer* di Banca Mediolanum che gestisce le operazioni sospette (Funzione Antiriciclaggio Banca di secondo livello).

4.4 FUNZIONE COMPLIANCE

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

4.5 PERSPECTIVE BANKING SERVICES E CONTROLS – TEAM AML

La *Perspective Banking Services e Controls – Team AML* -, nell'ambito del presente processo, è responsabile di:

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

4.6 OUTSOURCERS

4.6.1 Banca Mediolanum - Team Operations Flowe

Nell'ambito del presente processo l'*outsourcer* Banca Mediolanum attraverso il *Team Operations Flowe* del *Settore Product Operations* si occupa di:

- effettuare un primo controllo delle posizioni presenti sulla piattaforma IQP e su FCM e, laddove necessario, richiedere i dovuti approfondimenti al Team AML, che valuta se procedere con invio AVR;
- effettuare una prima analisi a supporto del *Team AML* della *Perspective Banking Services e Controls* in merito alle evidenze dei *match* tra i *prospect* e i soggetti inclusi nelle liste utilizzate dal Gestionale Antiriciclaggio (quali ad esempio *black-list*, liste PEP, liste PIL, liste appalti) al fine di escludere eventuali casi di omonimia attraverso l'utilizzo della piattaforma SGR;
- supportare il *Team AML* della *Pespective Banking Services e Controls*, nell'ambito dell'adeguata verifica (*Batch Alert Manager*) al fine di procedere alla verifica delle regole scattate in FCM (*Input*) passando le posizioni da dover approfondire in valutazione al *Team AML - Chief Service Senior*.

4.6.2 Temenos

Flowe si avvale dell'*outosourcer* Temenos - applicativo di *Core Banking* T24 – attraverso il quale apre la posizione anagrafica del cliente e il conto di pagamento a fronte dell'esito positivo di tutti i controlli di *onboarding*. T24 permette inoltre di gestire i processi "*core*" della Società per la

gestione delle operazioni di pagamento. L'*outsourcer* fornisce anche il modulo *Financial Crime Mitigation* (FCM) per lo svolgimento di una serie di attività e controlli ai fini AML supportando la Società dalla fase di acquisizione del cliente e per tutta la durata del rapporto.

4.6.3 SIA

Flowe si avvale dell'*outosourcer* SIA per la consultazione delle informazioni della carta associata al cliente - tipologia di carta (fisica o virtuale), dettagli dell'intestatario della carta (luogo di spedizione, dati anagrafici e residenza)-.

4.6.4 InfoCert

Nell'ambito del presente processo InforCert supporta Flowe nell'ambito di alcune attività di "*Know Your Customer*".

L'*outsourcer* riceve ed elabora, in collaborazione con Experian, le informazioni del potenziale cliente raccolte tramite apposita sezione dedicata all'interno dell'App Flowe in fase di *onboarding* e necessarie ai fini dell'adempimento dei relativi obblighi normativi. Effettua, inoltre, alcuni controlli sulla correttezza delle informazioni di identità fornite dal *prospect* in fase di *onboarding* tramite App Flowe. Nello specifico mediante questo strumento gli operatori della *Perspective Banking Services e Controls* possono consultare l'esito del processo di KYC e visualizzare le regole applicate che non hanno consentito di proseguire nel processo di *onboarding*.

InfoCert supporta e gestisce il processo di archiviazione sostitutiva del *dossier* del cliente, conformemente alla normativa vigente (anche in caso di future eventuali variazioni della stessa).

5 PROCESSO DI ONBOARDING CLIENTE ED APERTURA CONTO DI PAGAMENTO

Il processo di *onboarding* cliente ed apertura conto di pagamento si compone dei seguenti quattro sottoprocessi:

- Acquisizione dati cliente;
- Sottoscrizione contratto;
- *Know Your Customer*;
- Censimento anagrafico ed apertura rapporto.

Per ciascun sottoprocesso, di seguito è riportata una descrizione delle attività svolte dagli attori coinvolti, unitamente a:

- la descrizione del controllo effettuata;
- il tipo di controllo;
- la frequenza del controllo;
- lo strumento informatico (c.d. applicativo) a supporto delle attività operative svolte e dei controlli eseguiti.

5.1 ACQUISIZIONE DATI CLIENTE

È la fase che dà avvio alla procedura di *onboarding* della clientela, durante la quale vengono raccolte le informazioni utili alla verifica dell'identità del *prospect* e alla sua adeguata profilazione.

5.1.1 *Registrazione prospect in APP*

Il *prospect*, dopo aver installato l'app, inserisce le informazioni necessarie a registrare il *device* ed assicurare i presidi di sicurezza dello strumento sul quale è scaricata l'app, quali:

- "*pass code*";
- numero di cellulare, certificato inserendo il codice OTP ricevuto via sms;
- indirizzo e-mail, certificato inserendo il codice OTP ricevuto via *e-mail*.

Qualora il *prospect* avesse difficoltà nell'inserimento delle informazioni richieste, può avvalersi delle funzioni di supporto quali ad. es *Chatbot*, gestite dagli operatori della *Perspective Business Acceleration* dedicati alle attività di *Customer Interaction*.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica bloccante su correttezza e corrispondenza OTP (ricevuto via sms) per certificare il numero di cellulare	Automatico	Continuativo	App Flowe; P0
Verifica bloccante su correttezza e corrispondenza codice OTP (ricevuto via e-mail) per certificare l'indirizzo e-mail	Automatico	Continuativo	App Flowe; P0
Verifica bloccante numero di cellulare non italiano (prefisso diverso da "+39")	Automatico	Continuativo	App Flowe
Verifica bloccante indirizzo e-mail e cellulare già utilizzati da altri utenti	Automatico	Continuativo	App Flowe; P0

5.1.2 *Presa visione del materiale informativo e precontrattuale ed accettazione dell'informativa privacy*

Il *prospect* conferma la presa visione del materiale informativo relativo all'offerta di Flowe (es.: norme contrattuali in bianco idonee alla stipula e il foglio informativo) e prosegue con

l'accettazione in app dell'informativa *privacy* (principi e modalità di utilizzo dei dati personali da parte di Flowe).

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica bloccante su presa visione materiale informativo	Automatico	Continuativo	App Flowe
Verifica bloccante su fornitura consensi *privacy* (accettazione / negazione)			

5.1.3 *Inserimento dati personali e documentazione di riconoscimento*

Ai fini dell'identificazione al potenziale cliente è richiesto:

- il codice fiscale (può essere inserito dal *prospect*, fotografato o calcolato automaticamente in app);
- una fotografia chiara del documento identificativo scelto per la registrazione; i dati anagrafici sono acquisiti automaticamente dal documento identificativo, tramite l'*Optical Character Recognition* (c.d. OCR).

Il *prospect*, inoltre, conferma o completa le sue informazioni personali quali indirizzo di residenza ed eventuale domicilio (se diverso da residenza). In caso di anomalie/incongruenze sui dati inseriti, il processo di apertura conto non arriva a finalizzarsi.

Anche in questa fase, qualora il *prospect* avesse difficoltà nell'inserimento delle informazioni richieste, può avvalersi delle funzioni di supporto presenti all'interno dell'App Flowe (es. *Chatbot*).

Nel caso di utilizzo di documento elettronico ed attivazione dell'NFC, il *prospect* può decidere di far leggere elettronicamente i dati del documento (i dati dei documenti contraffatti non vengono letti). In questo caso, P0 *Platform* acquisisce automaticamente i dati del documento (inclusa la foto del soggetto) senza necessità di digitarli/caricare una foto. Si specifica che i dati dei documenti letti tramite NFC non sono modificabili negli step successivi da parte del *prospect*.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Impossibilità di modifica dei dati (carta d'identità o passaporto elettronico) acquisiti tramite NFC	Automatico	Continuativo	App Flowe
Blocco del processo in caso di incongruenza (lunghezza) del numero identificativo della carta d'identità (elettronica e	Automatico	Continuativo	App Flowe;

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
cartacea)			
Blocco del processo in caso di inserimento, da parte del potenziale cliente, di un codice fiscale che non rispetta le regole del DM 12/03/1974	Automatico	Continuativo	App Flowe;
Blocco del processo in caso di codice fiscale già registrato in anagrafica*	Automatico	Continuativo	App Flowe; P0
Verifica bloccante età *prospect* minore di 12 anni	Automatico	Continuativo	App Flowe; P0
Verifica bloccante su residenza anagrafica del *prospect* diversa da Italia	Automatico	Continuativo	App Flowe;
Verifica bloccante su documento già associato ad altro utente (tipo di documento e numero)	Automatico	Continuativo	App Flowe; P0

**Attualmente Flowe consente l'apertura di un nuovo conto da parte di un vecchio cliente. Il calcolo sull'inibizione della riapertura di un conto per un cliente che ne aveva già avuto (e chiuso) uno in precedenza è basato sulla data di chiusura del conto. Dopo un periodo di 15 giorni dall'avvenuto completamento della procedura di estinzione, viene data facoltà al cliente di effettuare un nuovo onboarding. Risulta, pertanto, in essere esclusivamente il controllo sul codice fiscale già associato ad un cliente con il conto attivo o nel suddetto periodo di inibizione.*

5.1.4 *Identificazione cliente*

La *Perspective Banking Services e Controls- Team AML* - con l'ausilio del *Team Operations Flowe* di Banca Mediolanum effettua l'identificazione formale del cliente.

Gli esiti delle verifiche automatiche vengono riportate – ed eventualmente gestite tramite controlli manuali – in IQP.

Il processo si compone di:

a) identificazione soggetto (tramite video selfie)

   Per procedere con l'identificazione il *prospect* viene guidato, attraverso l'app, nella realizzazione di un video selfie (nr. 5 selfie in sequenza) così da consentire, tramite sistemi biometrici, la verifica della corrispondenza tra le immagini acquisite e la foto presente nel documento identificativo (si precisa che per device i Android - al fine di evitare intromissioni nel sistema di face recognition – è stato eliminato il passaggio c.d. di

"approvazione selfie" da parte del prospect); viene valutato l'esito del "*face-matching*" in base alla percentuale di corrispondenza (score) tra l'immagine del *prospect* riportata sul documento identificativo e il video selfie realizzato. Nel caso in cui la percentuale di corrispondenza sia inferiore alle soglie minime definite dalla Società, il *prospect* deve ripetere l'inserimento delle informazioni identificative avvalendosi, ove necessario, del supporto del *Chatbot* (dove sono fornite soluzioni *standard* per risolvere problemi di riconoscimento). Qualora la soglia di corrispondenza venga raggiunta, il *prospect* può proseguire il processo di *onboarding* e contemporaneamente la *Platform* provvede ad inviare i dati raccolti in App Flowe ad InfoCert.

Per avere un maggior livello di confidenza del *match* tra *selfie* e documento, vengono utilizzati anche 2 diversi algoritmi di "*face recognition*" da parte dei fornitori InfoCert e Microsoft. I due controlli sono sequenziali e possono portare ad un "semaforo giallo" in IQP. Il "*face-matching*" di InfoCert, inoltre, sotto una soglia stabilita può portare anche al diniego dell'*onboarding*.

b) Verifica preventiva sui "selfie" già presenti in *database – Face Manager e Unwanted Subject*

Flowe si avvale dei Cognitive Services Microsoft, ai fini della prevenzione di eventi fraudolenti commessi sia nei confronti della società che ai fini AML, per fare una verifica preventiva della presenza di "*selfie*" già presenti nel *database* rispetto al *selfie* di un *prospect* che tenta ulteriori *onboarding*.

In caso di rilevazione di un *match* – secondo le soglie stabilite dalla società - per un *prospect* minorenne, l'*onboarding* viene sospeso (semaforo giallo) con verifiche manuali da parte di un operatore *Banking Services e Controls– Team AML* – sul *prospect* e il "*selfie*" con cui effettua il *match*. Si specifica che tale controllo viene eseguito a valle della ricezione di una dashboard che evidenzia i soggetti da approfondire (sia *prospect* sia clienti presenti in *database*). Tale modalità di controllo risulta applicabile anche per il caso dei gemelli.

In caso di rilevazione di un *match* per un *prospect* maggiorenne, l'*onboarding* viene rifiutato senza passaggio in IQP (semaforo rosso).

Inoltre, a partire dal quarto trimestre 2023 è stato implementato il nuovo controllo "Unwanted Subject". Si tratta di un controllo che viene effettuato dall'AI di Microsoft attraverso il quale è possibile effettuale una verifica preventiva della presenza del selfie già presente nel *database* (riferito ai volti degli ex clienti considerati "indesiderati" da parte della società) rispetto al *selfie* di un *prospect* che tenta una nuova apertura.

In caso di rilevazione di un *match* – secondo le soglie stabilite dalla società - l'*onboarding* viene sospeso (semaforo giallo) con verifiche manuali da parte di un operatore *Banking Services e Controls– Team AML* – sul *prospect* e il "*selfie*" con cui effettua il *match*. Si specifica che tale controllo viene eseguito a valle della ricezione di una dashboard che evidenzia i *prospect* da approfondire.

c) asserzione di identità (liveness detection)

La "*Liveness detection*" permette (vedi anche par. 5.3) di determinare la "*liveness*" del *prospect* che in una determinata sessione sta per sottoporre il proprio volto per una verifica di compatibilità con la foto estratta dal proprio documento. In particolare, tale servizio è in grado di fornire funzionalità per: (a) guidare il *prospect* nella fase di inquadramento in modo da realizzare il *selfie* rispettando l'allineamento del volto in fase di scatto; (b) realizzare un riconoscimento *liveness* del volto durante la procedura. Il modulo di *liveness detection* esegue anche alcuni controlli aggiuntivi per aumentare il livello di sicurezza ed assicurarsi che la persona che sta seguendo la procedura di *onboarding* sia una persona

reale, in particolare: (a) la sequenza di movimenti richiesti al *prospect* è sempre casuale (e ciò impedisce che la soluzione sia sottoposta ad un video del volto del *prospect* che esegue esattamente i movimenti richiesti); (b) la procedura deve essere eseguita entro un tempo massimo definito.

d) US Person

Nel caso in cui il soggetto si dichiari *US Person* la procedura non permette di proseguire portando al termine il processo di *onboarding*.

Inoltre, Flowe effettua dei controlli manuali di conformità sulla documentazione identificativa e sulle informazioni acquisite, qualora emergano "semafori gialli" in IQP al fine di validare l'identità del *prospect*.

Qualora i controlli effettuati portino ad un esito positivo, l'operatore del *Team Operations Flowe* di Banca Mediolanum, a valle di indicazione del *Team AML* della *Perspective Banking Services e Controls*, modifica la posizione del *prospect* da "giallo" in "verde" in IQP ed il processo di *onboarding* ed apertura conto prosegue. Al contrario, qualora l'esito sia negativo (posizione del *prospect* da "giallo" a "rosso"), il processo di *onboarding* ed apertura conto termina e al soggetto viene notificato il diniego dell'apertura del conto in App e via e-mail. In ogni caso, l'operatore del Team Operations Flowe di Banca Mediolanum, provvederà a tracciare su IQP la motivazione dell'approvazione/rigetto del prospect in base alle indicazioni fornite dal *Team AML* della *Perspective Banking Services e Controls*.

CONTROLLO	**TIPO CONTROLLO**	**FREQUENZA CONTROLLO**	**APPLICATIVO**
Verifica sulla veridicità del documento elettronico (carta di identità e passaporto) tramite lettura MRZ del codice ICAO (e verifica *check digit*), con esito semaforico. In caso di semaforo giallo, l'operatore controlla la corretta lettura MRZ del codice ICAO e, qualora fosse errata, procede alla verifica manuale dell'ICAO attraverso un apposito strumento in Power Apps.	Automatico + Manuale	Continuativo	App Flowe; P0; Piattaforma IQP; Power Apps controllo codice ICAO.
Verifica del *prospect* identificato come già cliente Verifica bloccante che rifiuta il prospect qualora il suo selfie fa match con un altro selfie già presente nel nostro database, con soglia >80% (algoritmo di	Automatico + Manuale	Continuativo	App Flowe; P0; Dashboard

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Face Manager sviluppato tramite i Cognitive Services di Microsoft). L'operatore del Team AML procederà ad approfondimento sul cliente in match, apponendo un blocco preventivo.			
Verifica sulla veridicità della carta d'identità cartacea e/o della patente, con esito semaforico: • documento dubbio (giallo) con soglia al 70% → il prospect passa nella piattaforma IQP per un controllo manuale dell'asserzione d'identità; • documento vero (verde) → il processo di *onboarding* prosegue se la soglia è > 70% di confidence. Algoritmo di ID Document Manager sviluppato tramite i Cognitive Services di Microsoft.	Automatico - Manuale	Continuativo	App Flowe; P0; Piattaforma IQP
Prospect con età > 89 anni In questo caso l'*onboarding* si ferma per valutazione da parte di un operatore del Team di Operations Flowe di Banca Mediolanum attraverso la Piattaforma IQP, il quale effettua una prima disamina, passando poi il controllo al Team AML per la valutazione definitiva. Il Team AML procede con la valutazione del video selfie della persona rifiutando l'*onboarding* laddove sia evidente che si tratti di una foto e non di un selfie.	Automatico + Manuale	Continuativo	App Flowe; P0; Piattaforma IQP
Verifica cittadinanza secondo	Automatico	Continuativo	App Flowe; P0

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
una logica di paesi in *whitelist*			
Verifica *Liveness* del *prospect* nel *video selfie* Se il *prospect* non rispetta le indicazioni date in app per il selfie, è previsto un blocco automatico che non consente di proseguire nel processo di *onboarding*	Automatico	Continuativo	App Flowe
Verifica bloccante, tramite sistemi biometrici, della corrispondenza tra le immagini acquisite tramite *videoselfie* e la foto presente nel documento identificativo. • Se la % di confidenza è >=75% e <99,8%→ l'*onboarding* prosegue • Se la % di confidenza è >99,8% l'*onboarding* si ferma per valutazione da parte di un operatore attraverso la Piattaforma IQP • Se la % di confidenza è <75% e >=65% → l'*onboarding* si ferma per valutazione da parte di un operatore attraverso la Piattaforma IQP • Se la % di confidenza è <65% → si ha diniego dell'*onboarding*	Automatico - Manuale	Continuativo	App Flowe; Piattaforma IQP
Verifica tramite sistemi biometrici, della corrispondenza tra le immagini acquisite tramite video-selfie e la foto presente nel documento identificativo. Se "IsIdentical=False >> "Giallo" in IQP Se "IsIdentical=True >> "Verde"	Automatico - Manuale	Continuativo	App Flowe; Microsoft; Piattaforma IQP

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica bloccante che non sia stato inserito il valore "US Person"	Automatico	Continuativo	App Flowe

5.1.5 *Questionario AML*

Il *prospect* compila il questionario AML che comprende, ad esempio, domande inerenti all'occupazione, alla fonte di reddito, o se si tratta di un soggetto PEP.

Al completamento di tale questionario, ad esclusione del caso in cui il soggetto si dichiari *US Person* per il quale la procedura non permette di proseguire portando al termine il processo di *onboarding*, si prosegue con la sottoscrizione del contratto.

Qualora il *prospect* si dichiari un soggetto PEP, l'*onboarding* viene sospeso in attesa dell'esito della valutazione da parte dell'operatore della *Perspective Banking Services e Controls – Team AML*. In particolare, attraverso la piattaforma FCM, il *Team AML* procederà, attraverso il controllo manuale, all'invio dell'adeguata verifica rafforzata (cfr. *Procedura Operativa del Processo di adeguata verifica, SOS e gestione conto*); qualora tale *status* venga confermato, l'apertura del rapporto è oggetto di approvazione da parte del Responsabile della *Perspective Banking Services e Controls*[2].

a) Utenti maggiorenni

Per gli utenti maggiorenni, a seguito della compilazione del questionario AML, il processo prosegue con l'assegnazione del profilo di rischio AML sulla base delle regole definite (a partire dal giorno successivo all'effettivo censimento anagrafico in T24).

b) Utenti minori di 16 anni e/o studenti

In caso di *prospect* con età minore di 16 anni oppure *prospect* con età maggiore o uguale a 16 anni e professione "studente", il sistema Flowe richiede il numero di cellulare del soggetto di maggiore età che agisce in qualità di genitore/tutore/curatore, il quale sarà il solo che potrà portare a termine il processo di *onboarding* del minore (confermando i dati inseriti dal minore e compilando a suo nome il questionario AML).

c) Utenti maggiori di 16 anni (ma minore di 18 anni) e lavoratori

In caso di *prospect* con età maggiore o uguale di 16 anni (ma minore di anni 18) e professione "lavoratore", il processo prosegue con la richiesta al minore di compilazione del questionario AML (ad esclusione delle domande PEP/*US PERSON* proposte al maggiorenne) utilizzato per la valutazione del suo profilo di rischio, successivamente registrato nel Gestionale Antiriciclaggio come un cliente di maggiore età. In seguito, l'App Flowe richiede il numero di cellulare del

[2] A tal proposito si rimanda per competenza e ulteriore dettaglio al "Regolamento del processo di gestione delle Persone Esposte Politicamente (c.d. PEP), tempo per tempo vigente

soggetto di maggiore età che agisce in qualità di genitore/tutore/curatore, il quale sarà il solo che potrà portare a termine il processo di *onboarding* del minore (confermando i dati inseriti dal minore e compilando a suo nome il questionario AML).

5.1.6 *Registrazione genitore/ tutore/curatore*

Nel caso in cui il genitore/tutore/curatore del minore non sia cliente Flowe, quest'ultimo deve percorrere il processo di *onboarding* in tutte le sue fasi (compresa l'indicazione del tipo di legame con il minore) in quanto responsabile legale del conto di pagamento intestato al minore.

Nel caso in cui, invece, il genitore/tutore/curatore del minore sia già cliente Flowe, è richiesta solo la conferma dei dati del minore (ai fini dell'adeguata verifica), l'indicazione del tipo di legame con quest'ultimo e, previa visione della documentazione contrattuale, la sottoscrizione della modulistica prevista.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica bloccante differenza di età fra genitore e figlio < 15 anni, l'*onboarding* viene rifiutato	Automatico	Continuativo	App Flowe; P0
Verifica bloccante su numero massimo di minori associabili ad un maggiorenne (max 5 minori per ogni maggiorenne)	Automatico	Continuativo	App Flowe; P0
Controllo manuale (ex-post) se il *prospect* maggiorenne dichiaratosi inizialmente come "tutore / curatore" ha in seguito modificato la sua posizione in "genitore" (tramite apertura di un Activity in Fan BASE con alert diretto al Team AML). La procedura di *onboarding* per i tutori/curatori sarà oggetto di ulteriore revisione con lo sviluppo di nuove funzionalità dell'app.	Manuale	Continuativo	App Flowe; Fan base
Verifica documentazione comprovante il ruolo di tutore/curatore attestante la reale qualifica dei soggetti maggiorenni indicati in fase di apertura.	Manuale	Ad evento	App Flowe

In particolare, attualmente è inibita l'apertura automatica ove il maggiorenne si identifichi quale tutore/curatore del minore, consentendo l'apertura di un rapporto solo attraverso il censimento di un genitore.			
Vengono inoltre eseguiti periodicamente dei controlli a campione, post *onboarding*, sulla documentazione comprovante il ruolo di genitore.	Manuale	Ad Evento	App Flowe; Fan Base

5.2 SOTTOSCRIZIONE CONTRATTO

Rappresenta la finalizzazione, attraverso la sottoscrizione del contratto dedicato, della richiesta di apertura del conto di pagamento Flowe.

5.2.1 Attivazione servizio firma digitale

Il *prospect* richiede in app il "Certificato Qualificato di Firma Digitale" InfoCert e in seguito visualizza il modulo di sottoscrizione del servizio precompilato con i dati forniti in precedenza.

5.2.2 Firma e ricezione copia contratti

Il *prospect* prende visione dei documenti contrattuali e delle clausole vessatorie ed accorda la conferma definitiva alla sottoscrizione del contratto firmando digitalmente tramite OTP.

Successivamente il modulo firmato viene inviato, tramite *e-mail*, al *prospect* insieme ai restanti documenti contrattuali. Il *prospect* deve poi confermare in app di aver ricevuto tutto il pacchetto contrattuale via *e-mail*.

Tutto il materiale contrattuale viene reso disponibile al *prospect* all'interno di una sezione dedicata dell'app Flowe.

Il *prospect*, perfezionato il contratto, riceve quindi una *e-mail* che lo informa che la Società provvederà nei giorni successivi a comunicargli l'esito delle ultime opportune verifiche. Solo al termine di questi controlli, in caso di esito positivo, il *prospect* diventa cliente Flowe a tutti gli effetti (verifiche descritte in corrispondenza dell'attività denominata "Asserzione identità").

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifica bloccante qualora il cliente non abbia effettuato la firma digitale del contratto (azione eseguibile tramite la ricezione di	Automatico	Continuativo	App Flowe; TOP

un OTP sul numero di cellulare inserito in fase di registrazione e l'inserimento del codice stesso in app). Inoltre, viene verificata anche la conferma che il cliente abbia accettato in app di aver ricevuto copia del contratto (tramite operazione di opt-in)			

5.2.3 Archiviazione contratti

A fronte della firma dei contratti, tutto il set documentale (Contratti, foto, documento d'identità) viene inviato in archiviazione sostitutiva su sistema InfoCert (Legal Doc).
Oltre all'archiviazione sostitutiva su sistema Infocert, Flowe ha adottato uno strumento di archiviazione delle attestazioni di avvenuta consegna di copia del contratto fornite dal cliente in via telematica (mediante l'APP di Flowe e per il tramite di specifici file di log).

5.3 KNOW YOUR CUSTOMER

Durante la fase di *Know Your Customer*, avviata a seguito della registrazione e raccolta dei dati del *prospect* in app, sono svolte tutte le verifiche necessarie per accertare l'identità del potenziale cliente e calcolare il profilo di rischio da associare allo stesso. Durante questa fase sono identificati eventuali *prospect* non acquisibili in linea con le normative AML e i principi della stessa Flowe.

5.3.1 Asserzione d'identità

Tutto il dossier informativo e documentale raccolto viene storicizzato in P0 ed inviato in maniera automatica a InfoCert che, con il supporto di Experian, svolge i controlli definiti da Flowe nella Piattaforma IQP, volti a valutare la sussistenza di tutti i requisiti richiesti che consentono di proseguire con l'asserzione di identità e l'apertura del conto di pagamento.

Gli esiti di tali controlli definiscono lo stato della posizione nell'ambito del processo di *onboarding*:

- "rosso", tradotto in un automatico diniego notificato al soggetto tramite app e via e-mail, in tal caso la procedura termina;
- "giallo", l'*onboarding* risulta sospeso per necessaria gestione da parte dell'operatore della *Perspective Banking Services e Controls- Team AML;*
- "verde", i controlli sono superati, l'*onboarding* prosegue.

Qualora entro 30 giorni dalla richiesta da parte del *prospect* dell'OTP per la firma del contratto il processo di *onboarding* non venga completato (per motivi tecnici) si ravvisano due soluzioni differenti:

- se non è ancora avvenuta l'asserzione di identità i dati in P0 vengono cancellati attraverso un automatismo attivato dal *Team Customer interaction* della *Prospective Banking Services e Controls* e viene mandata comunicazione al *prospect* che per un problema tecnico non è stato possibile procedere con l'*onboarding*, ma che laddove avesse intenzione di effettuare un nuovo tentativo è legittimato a farlo.

- se, invece, c'è già stata l'asserzione di identità non sarà possibile cancellare i dati del cliente ma il contratto non si riterrà in ogni caso perfezionato.

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
Verifiche su dati e documenti. (Riattivazione servizio Scipafi in data 08.08.2022.*) InfoCert/Experian (Detect) attivano una serie di controlli automatici sul corredo informativo raccolto quali: • verifica *Conformity check* (percentuali di dati modificati dal *prospect* rispetto a quanto letto dall'OCR) → se i dati modificati dal *prospect* sono superiori al 50% del totale dei dati acquisiti tramite OCR, il processo si ferma per valutazione da parte di un operatore in IQP • verifica della presenza di Protesti/Pregiudizievoli → se presenti, si ha il diniego per l'*onboarding* • verifica se numerazione carta di identità o passaporto (elettronico o cartaceo) o patente non risultano formalmente congruenti. Se incongruenti, si ferma per valutazione da parte di un operatore in IQP • Verifica se la data di rilascio della carta di identità è corrispondente ad una festività (comprese le festività comunali) o una data elettorale • Verifica se la data di rilascio della carta di identità è incongruente con la data di scadenza • Verifica se il passaporto risulta	Automatico + Manuale	Continuativo	App Flowe; Piattaforma IQP; Experian

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
scaduto • Verifica se la patente è stata emessa in un giorno festivo • Verifica se codice fiscale è inesistente o è sostituito per Omocodia o è di persone giuridiche o è invalido • Verifica se il numero della patente è inesistente o è esistente ma non corrispondente a CF o è positivo ma non valido o è patente sostituita o non è conforme allo standard previsto • Verifica se il numero del passaporto è inesistente o è esistente ma non corrispondente ai dati anagrafici o è positivo ma non valido o non è conforme allo standard previsto • Verifica se la data di rilascio della patente o del passaporto è non disponibile o è sintatticamente scorretto o è negativo • Verifica se cognome e/o nome sono sintatticamente scorretti • Verifica se il domicilio fiscale sull'Anagrafe Tributaria riportato è senza fissa dimora o è AIRE o è anagrafe non residenti • Verifica se la data di rilascio del passaporto corrisponde a una festività nazionale o ad una domenica o rileva incongruenze tra la data di rilascio e la data di scadenza • Verifica se la numerazione della carta d'identità non è conforme allo standard previsto o non rientra nel range di			

CONTROLLO	TIPO CONTROLLO	FREQUENZA CONTROLLO	APPLICATIVO
lotto/numero assegnato a ogni comune sulla base di analisi statistiche			

*Si precisa che ad oggi il Ministero dell'Interno non fornisce gli esiti dei controlli su clienti nati nei seguenti paesi: Aland Islands; Antarctica; Bouvet Island; Christmas Islands; Heard Island and McDonald Islands; Norfolk Island; Svalbard; Tokelau; United States Minor Outlying Islands; Virgin Islands.

5.3.2 Adeguata verifica, adeguata verifica rafforzata e gestione alert antiriciclaggio

Per le attività di adeguata verifica, adeguata verifica rafforzata e gestione degli *alert* antiriciclaggio in fase di *onboarding* si rimanda alla procedura "*Procedura operativa del Processo di adeguata verifica, SOS e gestione conto*".

5.4 CENSIMENTO ANAGRAFICO ED APERTURA RAPPORTO

Durante l'ultima fase del processo, si procede automaticamente con l'apertura della posizione del cliente (anagrafica, conto e carta di debito) ed all'alimentazione del rapporto nell'Archivio Unico Informatico (si veda "*Procedura operativa del Processo di adeguata verifica, SOS e gestione conto*").

5.4.1 Apertura posizione anagrafe generale e conto di pagamento

A conclusione dei controlli relativi all'asserzione di identità e dei controlli AML con esito positivo, si scatena un processo completamente automatizzato che apre contestualmente:

- l'anagrafica del cliente (in T24);
- il conto di pagamento (in T24);
- la carta di debito (in GUI-SIA).

Il *prospect* diviene, quindi, ufficialmente cliente Flowe e può iniziare ad operare con l'App, venendo informato tramite *e-mail* e notifica *push* in app che le verifiche svolte sono terminate.

6 NORMATIVA

6.1 NORMATIVA INTERNA

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

- *Policy di prevenzione e sul contrasto al riciclaggio e al finanziamento del terrorismo;*
- *Regolamento del processo di Adeguata Verifica;*
- *Regolamento del processo di conservazione, controlli e reporting;*
- *Regolamento del processo di gestione delle Persone Esposte Politicamente (c.d. PEP);*
- *Regolamento del processo di Segnalazione Operazioni Sospette (SOS);*
- *Procedura operativa del Processo di adeguata verifica, SOS e gestione conto.*

6.2 NORMATIVA ESTERNA

Nel presente capitolo si richiama il contesto normativo nel quale opera la presente Procedura.

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

- *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 delle Direttive 2018/1673 del 23 ottobre 2018 sulla lotta al riciclaggio mediante il diritto penale e 2018/843/CE;*
- *le disposizioni attuative del Decreto Antiriciclaggio in materia di organizzazione, procedure e controlli interni, di adeguata verifica della clientela, di conservazione e utilizzo dei dati e delle informazioni a fini antiriciclaggio, emanate dalle Autorità di Vigilanza di Settore e tempo per tempo vigenti;*
- *Completano il quadro di riferimento a livello nazionale, i decreti del Ministro dell'Economia e delle Finanze (MEF) e gli schemi rappresentativi di comportamenti anomali emanati dalla UIF;*
- *Provvedimento Della Banca d'Italia de 23 luglio 2019, Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica e successivi aggiornamenti;*
- *Disposizioni di Trasparenza delle operazioni e dei Servizi Bancari e Finanziari - Correttezza delle relazioni tra intermediari e clienti del 29 luglio 2009 e successive modifiche e integrazioni;*
- *Direttiva PAD. Trasparenza e comparabilità delle spese relative al conto di pagamento. Terminologia standardizzata europea;*
- *Direttiva (UE) 2015/2366 PSD2 – (Payment Services Directive 2);*

- *Decreto legislativo 1° settembre 1993, numero 385. Testo unico delle leggi in materia Bancaria e Creditizia.*

Per quanto riguarda l'archiviazione sostitutiva:

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