Gruppo Bancario Igea Banca

MANUALE ANTIRICICLAGGIO DI GRUPPO

CODICE:(GRU)-GOV-DNV-MAN-02

Area	**Processi di Governo (GOV)**
Macro Ambito	**Disposizione Normative di Vigilanza (DNV)**
Ambito	**AML**
Perimetro di applicabilità	**Gruppo Bancario**
Data creazione	**19/01/2021**
Tipologia di documento	**Manuale**
Data approvazione CdA Banca del Fucino	**29/12/2021**
Data approvazione CdA Igea Digital Bank	**In corso di recepimento**

INDICE

1 PREMESSA

Il presente Manuale Antiriciclaggio (di seguito "il Manuale"), in attuazione dei principi stabiliti nella **Policy in materia di contrasto al riciclaggio di denaro proveniente da reato e al finanziamento del terrorismo** del Gruppo Igea Banca, riporta ruoli e responsabilità delle Funzioni di Controllo e dettaglia modalità operative di adempimento agli incarichi nell'ambito della gestione del rischio di riciclaggio e finanziamento al terrorismo.

Il Manuale, ove non diversamente specificato, si applica a tutto il Gruppo. Le Controllate sono tenute all'osservanza delle regole in esso contenute.

Nel Manuale sono, pertanto:

- definiti i ruoli e le responsabilità delle strutture coinvolte;
- definite e descritte le attività operative ed i relativi controlli;
- evidenziati i flussi di comunicazione tra i soggetti (interni ed esterni) coinvolti;
- individuati i sistemi applicativi a supporto dell'operatività.

Il Manuale è aggiornato costantemente dalla Funzione Antiriciclaggio di Gruppo, che è altresì incaricata di redigerlo e trasmetterlo al Consiglio di Amministrazione di Gruppo; in ogni caso, il Manuale è revisionato sulla base delle modifiche intervenute nella Policy Antiriciclaggio di Gruppo

2 GLOSSARIO

Alto Dirigente/Alta Dirigenza - Nei termini di cui al presente documento, si fa riferimento ai soggetti titolari di poteri di amministrazione o direzione ovvero di loro delegati o, comunque, di soggetti che svolgono una funzione equivalente ([1])

Antiriciclaggio (AML - Anti Money Laundering) - Misure di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose.

ARCHIVIO STANDARDIZZATO – modalità di conservazione e messa a disposizione dei documenti, dei dati e delle informazioni, corrispondente all'ex Archivio Unico Informatico, scelta effettuata ex art. 6, comma 1, lett. b) delle Disposizioni di Banca d'Italia del 24 marzo 2020 "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".

AV – Adeguata Verifica della Clientela.

CSF - Comitato di Sicurezza Finanziaria istituito con decreto legge 12 ottobre 2001, n. 369, convertito, con modificazioni, dalla legge 14 dicembre 2001, n. 431, e disciplinato con il decreto legislativo 22 giugno 2007, n. 109, in ottemperanza agli obblighi internazionali assunti dall'Italia nella strategia di contrasto al riciclaggio, al finanziamento del terrorismo e della proliferazione delle armi di distruzione di massa ed all'attività di Paesi che minacciano la pace e la sicurezza internazionale, anche al fine di dare attuazione alle misure di congelamento disposte dalle Nazioni unite e dall'Unione europea.

Dati identificativi - il nome e il cognome, il luogo e la data di nascita, la residenza anagrafica e il domicilio, ove diverso dalla residenza anagrafica, e, ove assegnato, il codice fiscale o, nel caso di soggetti diversi da persona fisica, la denominazione, la sede legale e, ove assegnato[2], il codice fiscale.

Decreto Antiriciclaggio - Decreto legislativo 21 novembre 2007, n. 231 e s.m.i..

---

[1] Per tali si intendono l'Amministratore Delegato, il Direttore generale della società bancaria controllata e/o i Vicedirettori generali competenti

[2] Si fa riferimento ai casi di clienti privi di un codice fiscale rilasciato dall'Agenzia delle Entrate (in quanto, ad es., cittadini non italiani, residenti all'estero)

Disposizioni in materia di adeguata verifica - Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo - Banca d'Italia (30 luglio 2019).

Disposizioni in materia di organizzazione, procedure e controlli interni - 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 - Banca d'Italia (26 marzo 2019).

Disposizioni S.AR.A. - Disposizioni per l'invio dei dati aggregati – Banca d'Italia UIF (25 agosto 2020).

Provvedimento del 24 marzo 2020 - "*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*".

Esecutore - Il soggetto delegato ad operare in nome e per conto del cliente, o a cui siano comunque conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del cliente.

Finanziamento del terrorismo - Qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione , al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto previsto dalle leggi penali ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette.

Funzioni aziendali di controllo - Funzione di controllo di conformità (Compliance); Funzione Antiriciclaggio (confluita nella Funzione Compliance); Funzione di gestione del rischio (Risk Management); Funzione di revisione interna (Internal Audit).

Funzione Antiriciclaggio – Funzione accentrata sulla Capogruppo, incardinata nella Funzione *Compliance.*

GAFI - Gruppo di Azione Finanziaria Internazionale / Financial Action Task Force (FATF).

Gruppo Bancario Igea (o il Gruppo) - Il Gruppo bancario di cui all'art. 60 del D.Lgs. n. 385/1993 composto dalla Capogruppo, dalla Società bancaria controllata e dalla Società finanziaria controllata.

Manuale Antiriciclaggio - Manuale Antiriciclaggio e Antiterrorismo.

Paesi terzi ad alto rischio - Paesi non appartenenti all'Unione europea i cui ordinamenti presentano carenze strategiche nei rispettivi regimi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo, per come individuati dalla Commissione europea nell'esercizio dei poteri di cui agli articoli 9 e 64 della Direttiva (UE) 2015/849.

PEP - *Persone Esposte Politicamente* - Persone fisiche di cui all'art. 1, comma 2, lett. dd), del Decreto antiriciclaggio.

Referente – Referente antiriciclaggio presso le Entità Controllate, gerarchicamente subordinato alla Funzione della Capogruppo.

Regolamento UE 2015/847 - Regolamento del Parlamento Europeo e del Consiglio riguardante i dati informativi che accompagnano i trasferimenti di fondi del 20 maggio 2015.

Rischi di riciclaggio e di finanziamento del terrorismo - Rischi derivanti dalla violazione di previsioni di legge, regolamentari e di autoregolamentazione funzionali alla prevenzione dell'uso del sistema finanziario per finalità di riciclaggio, di finanziamento del terrorismo o di finanziamento dei programmi di proliferazione delle armi di distruzione di massa, nonché il rischio di coinvolgimento in episodi di riciclaggio e di finanziamento del terrorismo o di finanziamento dei programmi di proliferazione delle armi di distruzione di massa.

Trasferimento di fondi - Operazione effettuata almeno parzialmente per via elettronica per conto di un ordinante da un prestatore di servizi di pagamento, allo scopo di mettere i fondi a disposizione del beneficiario mediante un prestatore di servizi di pagamento, indipendentemente dal fatto che l'ordinante e il beneficiario siano il medesimo soggetto e che il prestatore di servizi di pagamento dell'ordinante e quello del beneficiario coincidano, fra cui: a) bonifico, quale definito all'articolo 2, punto 1), del regolamento (UE) n. 260/2012; b) addebito diretto, quale definito all'articolo 2, punto 2), del regolamento (UE) n. 260/2012; c) rimessa di denaro, quale definita all'articolo 4, punto 13),

della direttiva 2007/64/CE, nazionale o transfrontaliera; d) trasferimento effettuato utilizzando una carta di pagamento, uno strumento di moneta elettronica o un telefono cellulare o ogni altro dispositivo digitale o informatico prepagato o postpagato con caratteristiche simili.

SOS - Segnalazione di Operazioni Sospette.

Strutture operative - L'insieme delle strutture produttive (di Linea e di Rete) della Banca che effettuano controlli di linea.

UIF - Unità di Informazione Finanziaria.

3 ADEGUATA VERIFICA DELLA CLIENTELA

3.1 Obblighi di adeguata verifica alla clientela

Il presente paragrafo illustra le disposizioni finalizzate ad ottemperare all'obbligo di adeguata verifica della clientela e delle controparti di cui al Titolo II, Capo I del D.lgs. 231/2007 e s.m.i. (di seguito "Decreto").

L'**adeguata verifica della clientela (AV),** cardine della prevenzione del rischio riciclaggio, consiste nell'acquisire tutte le informazioni necessarie a garantire una conoscenza del cliente e delle sue caratteristiche, al fine di individuare, nel successivo e costante monitoraggio dell'operatività, eventuali elementi di anomalia che potrebbero essere alla base di eventuali segnalazioni alle autorità di vigilanza competenti. L'adeguata verifica deve essere rapportata e commisurata al cosiddetto principio dell'**"approccio basato sul rischio"** (risk based approach), di cui parla l'art. 17, comma 3, del Decreto.

Gli obblighi normativi in materia di Adeguata Verifica si articolano in un processo composto dal succedersi di diverse attività che saranno illustrate e meglio specificate oltre.

- **Soggetti coinvolti**
  - Funzione Antiriciclaggio
  - Alto dirigente
  - Strutture Operative (incluse le filiali)
- **Presidi informatici**

Il Gruppo si è dotato in particolare dei seguenti presidi informatici per l'ausilio degli adempimenti AML/CFT:

- **G.I.AN.O.S.:** tool di ausilio per le fasi di adeguata verifica della clientela, profilatura di rischio e monitoraggio dell'operatività della clientela.
- ***Fastcheck* ("Liste negative") – (WorldCheck):** Banca dati che consente di verificare il profilo reputazionale di un soggetto, il coinvolgimento dei soggetti in organizzazioni terroristiche o in procedimenti/indagini penali, nonché la sussistenza di informazioni pubblicamente disponibili in ragione dell'eventuale notorietà del soggetto e per la ricerca delle Persone politicamente esposte.
- **S.C.I.P.A.F.I.:** Portale web del Sistema Pubblico di Prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo e dei pagamenti dilazionati o differiti, con specifico riferimento al Furto d'Identità. Il Sistema consente il riscontro dei dati contenuti nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento e su quello dell'Agenzia delle Entrate.
- **Cedacri FEU (Front End Unico):** ambiente sul quale è resa disponibile documentazione e contrattualistica relativa all'apertura dei rapporti di conto corrente.

- **Piattaforma Digitale Smile:** applicativo in uso per Igea Digital Bank in fase di identificazione della clientela. La piattaforma, tramite integrazione nei sistemi Cedacri, consente la trasmissione automatica dei dati in Anagrafe.
- ***t-Notice*:** servizio elettronico di recapito certificato ("Raccomandata elettronica" e *FEA -Firma Elettronica Avanzata)* utilizzato dal Distretto prestiti al lavoro per la raccolta della documentazione contrattuale a distanza.

3.1.3 Adeguata verifica semplificata

L'adeguata verifica semplificata consiste nella **riduzione dell'estensione e della frequenza degli adempimenti descritti per l'adeguata verifica ordinaria**. Le disposizioni di legge e di vigilanza consentono al Gruppo di adottare tale regime soltanto in presenza di un basso rischio di riciclaggio, tenuto conto dei fattori previsti dal D.Lgs. 231/2007 e dal Provvedimento dalla Banca d'Italia del 30 luglio 2019, e purché siano formalizzate policy sufficientemente dettagliate sull'argomento.

L'applicazione di questa tipologia di misure è prevista solo per determinate categorie di soggetti o prodotti.

Le categorie di soggetti rientranti nella previsione sono:

- società ammesse alla quotazione su un mercato regolamentato e sottoposte ad obblighi di comunicazione che impongono l'obbligo di assicurare un'adeguata trasparenza della titolarità effettiva;
- pubbliche amministrazioni ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea;
- intermediari bancari e finanziari elencati all'art. 3, comma 2 del Decreto antiriciclaggio e intermediari bancari e finanziari comunitari o con sede in un Paese terzo con un efficace regime di contrasto al riciclaggio e finanziamento al terrorismo.

Si riporta, di seguito, una tabella dei soggetti rientranti nelle categorie sopra enunciate:

- una banca;
- Poste Italiane S.p.A.;
- un istituto di moneta elettronica (IMEL);
- un istituto di pagamento (IP);
- una società di intermediazione mobiliare (SIM);
- una società di gestione del risparmio (SGR);
- una società di investimento a capitale variabile (SICAV);
- una società che svolge il servizio di riscossione dei tributi;
- un intermediario finanziario iscritto nell'albo previsto dall'articolo 106 del TUB;
- una succursale insediata in Italia dei soggetti indicati alle lettere precedenti aventi sede legale in uno Stato estero;
- Cassa depositi e prestiti S.p.A.;
- un soggetto disciplinati dagli articoli 111 e 112 del TUB (operatori del microcredito e confidi);
- un ente creditizio o finanziario comunitario soggetto alla direttiva;
- un ente creditizio o finanziario situato in uno Stato extracomunitario, che imponga obblighi equivalenti a quelli previsti dalla direttiva e preveda il controllo del rispetto di tali obblighi;
- una società o un altro organismo quotato i cui strumenti finanziari sono ammessi alla negoziazione su un mercato regolamentato ai sensi della direttiva 2004/39/CE in uno o più Stati membri, ovvero una società o un altro organismo quotato di Stato estero soggetto ad obblighi di comunicazione conformi alla normativa comunitaria;
- un ufficio della pubblica amministrazione ovvero una istituzione o un organismo che svolge funzioni pubbliche conformemente al trattato sull'Unione europea, ai trattati sulle Comunità europee o al diritto comunitario derivato.

- Sono soggetti agli obblighi semplificati di adeguata verifica della clientela a titolo esemplificativo anche le istituzioni scolastiche (quali Unità locali del Ministero dell'Istruzione dell'Università e della ricerca),

Le categorie di prodotti rientranti nella previsione sono:

- contratti di assicurazione vita rientranti nei rami di cui all'articolo 2, comma 1, del CAP, nel caso in cui il premio annuale non ecceda i 1.000 euro o il cui premio unico non sia di importo superiore a 2.500 euro;
- forme pensionistiche complementari disciplinate dal decreto legislativo 5 dicembre 2005, n. 252, a condizione che esse non prevedano clausole di riscatto diverse da quelle di cui all'articolo 14 del medesimo decreto e che non possano servire da garanzia per un prestito al di fuori delle ipotesi previste dalla legge;
- regimi di previdenza o sistemi analoghi che versano prestazioni pensionistiche ai dipendenti, in cui i contributi sono versati tramite detrazione dalla retribuzione e che non permettono ai beneficiari di trasferire i propri diritti;
- prodotti o servizi finanziari che offrono servizi opportunamente definiti e circoscritti a determinate tipologie di clientela, volti a favorire l'inclusione finanziaria;
- prodotti in cui i rischi di riciclaggio o di finanziamento del terrorismo sono mitigati da fattori, quali limiti di spesa o trasparenza della titolarità.

È onere delle Strutture operative verificare, in sede di apertura dei rapporti, la sussistenza dei requisiti per l'applicazione di misure semplificate di adeguata verifica. Le funzioni di controllo effettuano periodicamente controlli di II e III livello per accertare che tali requisiti sussistano.

La riduzione dell'intensità delle verifiche e degli adempimenti caratteristici dell'adeguata verifica semplificata, al ricorrere dei presupposti indicati, si sostanzia prevalentemente in quanto segue:

- acquisire, prima dell'apertura del rapporto continuativo, il set minimo di dati identificativi del cliente, dell'esecutore e del titolare effettivo volto a consentire la verifica dell'abbinamento degli stessi rispetto alle liste di evidenza presenti nella procedura FastCheck, e rinviare fino a un massimo di trenta giorni il completamento del set informativo nonché l'effettiva acquisizione della copia dei documenti;
- ridurre la documentazione da raccogliere. In particolare, è possibile acquisire una dichiarazione di conferma dei dati inerenti al titolare effettivo del cliente persona giuridica, sotto la responsabilità del cliente stesso, qualora il medesimo sia una Pubblica Amministrazione, un intermediario finanziario o bancario – indicati nella tabella precedente - o una società ammessa alla quotazione su un mercato regolamentato;
- ridurre la frequenza dell'aggiornamento dei dati raccolti per l'adeguata verifica prevedendone l'intervento solo al ricorrere dell'apertura di un nuovo rapporto e/o all'innalzamento del profilo di rischio del cliente;
- ridurre la frequenza e la profondità delle analisi funzionali al monitoraggio del rapporto, prevedendo l'attivazione del controllo dell'operatività al di sopra di una determinata soglia, qualora vi sia coerenza rispetto allo scopo e natura del rapporto.

Resta inteso che in presenza di un qualsivoglia sospetto del coinvolgimento in attività di riciclaggio o di finanziamento del terrorismo, dovranno essere applicate le misure di adeguata verifica rafforzata indipendentemente da qualsiasi deroga, esenzione o soglia applicabile.

3.1.1 Adeguata verifica della clientela

L'adeguata verifica è svolta dalle Società del Gruppo nei seguenti casi:

- in sede di instaurazione di ogni nuovo rapporto continuativo[3], anche in relazione a clienti già acquisiti e lungo tutta la durata del rapporto stesso, secondo le modalità nel prosieguo definite;

[3] Si rinvia all'**Allegato 5 – Elenco rapporti continuativi da sottoporre ad adeguata verifica,** nel quale sono elencati i rapporti continuativi. Con riferimento ai conti correnti aventi la funzione di "Conto dedicato ai sensi della Legge 124/2017" di cui venga richiesta l'apertura da parte di un Notaio, si rinvia all'Allegato 7 del presente Manuale ("Conto corrente dedicato- Notai") nonché alla Circolare interna n. 2/2017 ("Conto dedicato Notai").

- quando viene eseguita un'operazione occasionale che 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 consista in un trasferimento di fondi superiore a 1.000 euro. A norma dell'art. 17, co 6 del decreto Antiriciclaggio si deve procedere all'adeguata verifica, per tutte le operazioni occasionali effettuate a titolo di servizio di pagamento o di emissione e distribuzione di moneta elettronica tramite agenti in attività finanziaria o "soggetti convenzionati e agenti", a prescindere dall'importo della singola operazione. Rientrano tra le operazioni occasionali anche le ipotesi in cui le banche – ovvero 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 tra soggetti diversi per un importo complessivo pari o superiore a 15.000 euro;
- quando vi è sospetto di riciclaggio o di finanziamento al terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile;
- quando sorgano dubbi sulla completezza, attendibilità o veridicità delle informazioni o della documentazione acquisita.

Laddove non sia possibile ottemperare agli obblighi di adeguata verifica, le Società del Gruppo non istaurano il rapporto continuativo ovvero non eseguono l'operazione ovvero si astengono dal proseguire il rapporto se l'impossibilità si verifica per un rapporto continuativo in essere e valutano, al ricorrere dei presupposti inerenti e conseguenti, l'opportunità di trasmettere una segnalazione di operazione sospetta.

In relazione ai clienti già acquisiti viene svolta nuovamente l'adeguata verifica nei termini declinati nel seguito. Qualora il cliente sia già stato identificato in relazione ad altro rapporto, sarà possibile, ai soli fini dell'identificazione, far riferimento alle informazioni medesime purché siano aggiornate e adeguate in relazione al profilo di rischio del cliente ed alla caratteristica del nuovo rapporto da avviare. Dovrà dunque essere raccolto un nuovo questionario in cui indicare i riferimenti al nuovo rapporto (natura, scopo, prevalente attività svolta, *etc*.).

Gli obblighi di adeguata verifica sono calibrati a seconda del rischio di riciclaggio del cliente su tre livelli:

- Adeguata verifica ordinaria;
- Adeguata verifica rafforzata: quando sussista un elevato rischio di riciclaggio risultante da specifiche previsioni normative oppure da autonoma valutazione;
- Adeguata verifica semplificata: in presenza di un basso rischio di riciclaggio, l'adeguata verifica può essere svolta in maniera semplificata, riducendo l'estensione e la frequenza degli adempimenti previsti.

Si riporta, di seguito, una tabella riassuntiva dei criteri generali, soggettivi e oggettivi, individuati dall'art. 17 co. 3 del Decreto Antiriciclaggio, di cui deve essere tenuto conto nel graduare l'entità delle misure sopra indicate:

a)	con riferimento al cliente: 1) natura giuridica; 2) prevalente attività svolta; 3) comportamento tenuto al momento del compimento dell'operazione o dell'instaurazione del rapporto continuativo o della prestazione professionale; 4) area geografica di residenza o sede del cliente o della controparte;
b)	con riferimento all'operazione, rapporto continuativo o prestazione professionale[4]: 1) tipologia dell'operazione, rapporto continuativo o prestazione professionale posti in essere; 2) modalità di svolgimento dell'operazione, rapporto continuativo o prestazione professionale; 3) ammontare; 4) frequenza delle operazioni e durata del rapporto continuativo o della prestazione professionale;

[4] Si rinvia all'**Allegato 6 – Criteri di valutazione concernenti i rapporti continuativi e le operazioni occasionali** per la trattazione sintetica di alcuni esempi.

5) ragionevolezza dell'operazione, del rapporto continuativo o della prestazione professionale in rapporto all'attività svolta dal cliente;
6) area geografica di destinazione del prodotto, oggetto dell'operazione o del rapporto continuativo.

3.1.1.1 Fasi operative dell'adeguata verifica ordinaria

Il processo di adeguata verifica ordinaria si articola secondo le seguenti fasi

1. **identificazione del cliente e dell'esecutore:** l'attività si sostanzia nell'acquisizione dei dati identificativi del cliente e dell'esecutore.
   - Nel caso in cui il cliente sia una **persona fisica,** l'identificazione, salvo eccezioni tassativamente individuate dalla normativa interna, avviene in sua presenza, raccogliendo i dati dallo stesso forniti, previa esibizione di un documento d'identità (o altro documento di riconoscimento equipollente ai sensi della normativa vigente, vedi **Allegato 1 - Elenco documenti idonei per identificazione**) e del codice fiscale ove assegnato, dei quali viene acquisita copia in formato cartaceo o elettronico. Limitatamente alla Capogruppo, la documentazione e contrattualistica relativa all'apertura dei conti correnti viene inviata alla società C-Global che provvede alla scannerizzazione di tutta la documentazione che viene resa disponibile in ambiente Cedacri FEU (Front End Unico). Per i rapporti diversi dai conti correnti (a titolo esemplificativo dossier titoli, libretti nominativi, etc.) la documentazione viene trattenuta in Filiale, in appositi fascicoli custoditi in armadi provvisti di serratura (ad eccezione del questionario di adeguata verifica che viene acquisito e storicizzato in formato digitale tramite la citata società C-Global). Attraverso le medesime modalità viene effettuata l'identificazione degli eventuali cointestatari e/o esecutori: rispetto a questi ultimi devono essere acquisite informazioni aggiuntive e documenti attestanti la sussistenza e l'ampiezza del potere di rappresentanza (vedi **Allegato 1 - Elenco documenti idonei per identificazione**).
   - Qualora il cliente sia una **persona non fisica,** è previsto che l'identificazione avvenga in presenza dell'esecutore, effettuando l'acquisizione di denominazione, sede legale e, ove assegnato, il codice fiscale, nonché di informazioni su tipologia, forma giuridica, fini perseguiti e/o attività svolta e, se esistenti, gli estremi dell'iscrizione nel registro delle imprese e negli albi tenuti dalle eventuali autorità di vigilanza di settore. La documentazione da acquisire, relativamente al cliente diverso da persona fisica è, salvo casi particolari trattati **nell'Allegato 1 – Elenco documenti idonei per identificazione**, la seguente:
     a) Atto costitutivo;
     b) Statuto;
     c) Visura camerale aggiornata (Infonet/Cerved) anche al fine di acquisire contezza circa il tipo di attività svolta e il relativo ambito territoriale (in caso di società di diritto estero, documento equivalente rilasciato dagli organi territoriali competenti, corrispondente al registro delle imprese e/o tribunale). Per le società neo costituite in corso di iscrizione nel Registro delle imprese è ammessa l'acquisizione dell'atto costitutivo corredata dalla richiesta di iscrizione depositata, fermo restando che la concreta operatività del cliente può essere garantita solo una volta completato il censimento con il numero di iscrizione;
     d) se presenti, procure ad operare;
     e) evidenze circa l'esistenza di eventuali patti parasociali, verbali assembleari o scritture per comprendere l'assetto societario ed il titolare effettivo.

Dovranno essere acquisite anche le informazioni relative **all'esecutore** o agli esecutori con le modalità sopra specificate (acquisendo copia della documentazione attestante la sussistenza di poteri, quali Atto Costitutivo, Statuto, Visura CCIAA aggiornata, eventuali Delibere Assembleari, etc.).
Alla raccolta di questo set di informazioni si accompagna in questa fase l'avvaloramento da parte dell'operatore nella procedura Anagrafe, funzione Inserimento/Variazione NDG dei campi relativi a:

- dati identificativi (cfr. le "Definizioni");

- Codice Professione e TAE (tipo di attività economica), presente nella sezione Altri dati, per i soggetti privati con codice SAE 600 (escluse le cointestazioni). Il TAE incide sul calcolo del profilo di rischio della clientela privata ai fini dell'adeguata verifica (non è necessario nel caso di cliente studente, casalinga, disoccupato e pensionato).
- il codice ATECO 2007, presente nella sezione Altri dati, nel caso di persone giuridiche.

NB: A seguito delle modifiche introdotte dalla Legge di Bilancio 2018 (Legge 205/2017 art.1 comma 45 che ha apportato modifiche al DPR 605/73 art. 6 comma 2), le Banche, Intermediari finanziari e società fiduciarie, negli atti o negozi riguardanti l'apertura o la chiusura di qualsiasi rapporto continuativo, non sono più obbligati ad indicare il codice fiscale dei soggetti non residenti ai quali tale codice non sia già stato attribuito, essendo sufficiente, in questi casi, la sola indicazione dei dati di cui all'art. 4 del DPR 605/73 (ossia, dei dati necessari per la presentazione della domanda di attribuzione del codice fiscale), con l'eccezione del domicilio fiscale, in luogo del quale va indicato il domicilio o sede legale all'estero.

Tramite l'inserimento dei dati il sistema elabora il Modulo per l'Identificazione e l'Adeguata Verifica della Clientela, che fornisce la base per la profilatura della clientela in ambito AML (vedi **Allegato 3 - modulo per l'identificazione e l'adeguata verifica della clientela**).

In conformità al Decreto e fermo quanto previsto dal paragrafo precedente, l'obbligo di identificazione si considera assolto, anche senza la loro presenza fisica, per i clienti:

1) i cui dati identificativi risultino da atti pubblici, da scritture private autenticate o da certificati qualificati utilizzati per la generazione di una firma digitale associata a documenti informatici, ai sensi dell'articolo 24 del decreto legislativo 7 marzo 2005, n. 82;
2) in possesso di un'identità digitale, di livello massimo di sicurezza, nell'ambito del Sistema di cui all'articolo 64 del decreto legislativo 7 marzo 2005, n. 82 (ad esempio, lo SPID – Sistema Pubblico di Identità Digitale), e della relativa normativa di attuazione, ovvero di un'identità digitale di livello massimo di sicurezza o di un certificato per la generazione di firma digitale, rilasciati 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;
3) i cui dati identificativi risultino da dichiarazione della rappresentanza diplomatica e dell'autorità consolare italiana, come indicata nell'articolo 6 del decreto legislativo 26 maggio 1997, n. 153;
4) che siano già stati identificati dal destinatario in relazione ad un altro rapporto continuativo in essere, purché le informazioni esistenti siano aggiornate e adeguate rispetto allo specifico profilo di rischio del cliente e alle caratteristiche del nuovo rapporto che si intende avviare;
5) i cui dati identificativi siano acquisiti secondo le modalità individuate per l'operatività a distanza[5], Vedi *infra* (par. 3.1.1.2).

All'interno di questa fase avviene, inoltre, un controllo preliminare su eventuali fattori di rischio in capo al soggetto suscettibili di innalzarne il profilo di rischio: è stato adottato un sistema di verifiche integrato negli applicativi Cedacri che viene innescato automaticamente al censimento di un nuovo soggetto (oltre che all'aggiornamento dell'adeguata verifica e alla variazione di taluni dati anagrafici -intestazione, natura giuridica, data di nascita, comune di nascita, provincia di nascita, codice fiscale e partita IVA, data iscrizione legale per le società-, oltre che settimanalmente in modalità massiva) in modo tale da riscontrare la presenza dello stesso nelle "Liste negative" World-Check (PEP, PEP Italiani, PEP Locali, Crime, Crime Financial, Sanzionati OFAC , ONU, UE, Terroristi, Individual). La certificazione circa la effettiva coincidenza dei clienti banca con i soggetti presenti nelle suddette Liste, sarà effettuata dalla Rete. Si rinvia ai

[5] Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo - Banca d'Italia (30 luglio 2019) – Parte II, sez VIII.

paragrafi sull'Adeguata Verifica Rafforzata per la disamina delle procedure da seguire, nei casi in cui la certificazione risulta positiva.
Infine, si precisa che nel caso in cui il soggetto sia già censito nell'Anagrafe Generale si dovrà verificare la sussistenza o il passato intrattenimento di rapporti presso altre Filiali e contattare per iscritto i relativi Responsabili al fine di acquisire informazioni utili ai fini antiriciclaggio. Nello specifico caso in cui il soggetto già censito nell'Anagrafe Generale rechi lo status anagrafico "F. Antiriciclaggio", saranno da richiedere alla Funzione Antiriciclaggio i motivi circa l'applicazione di tale status e l'autorizzazione all'accensione del nuovo rapporto.

Peraltro, il decreto-legge n.76/2020 "Semplificazione" (convertito nella legge n. 120/2020) ha apportato le seguenti modifiche al decreto antiriciclaggio con particolare riferimento all'identificazione a mezzo di strumenti digitali.
Per quanto riguarda gli estremi del documento di identificazione", la lettera a) del comma 1 dell'art. 18 del decreto antiriciclaggio (Contenuto degli obblighi di adeguata verifica), è stata sostituita con la seguente: "l'identificazione del cliente e la verifica della sua identità sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente. Le medesime misure si attuano nei confronti dell'esecutore, anche in relazione alla verifica dell'esistenza e dell'ampiezza del potere di rappresentanza in forza del quale opera in nome e per conto del cliente".
Il predetto D.L. n. 76/2020 anche con riferimento alle modalità di adempimento degli obblighi di adeguata verifica (art. 19), ha apportato delle modifiche:

il numero 2 della lett. a) viene sostituito da "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;".

Infine, viene previsto che "per i clienti che, previa identificazione elettronica basata su credenziali che assicurano i requisiti previsti dall'articolo 4 del Regolamento Delegato (UE) 2018/389 della Commissione del 27 novembre 2017, dispongono un bonifico verso un conto di pagamento intestato al soggetto tenuto all'obbligo di identificazione. Tale modalità di identificazione e verifica dell'identità può essere utilizzata solo con riferimento a rapporti relativi a carte di pagamento e dispositivi analoghi, nonché a strumenti di pagamento basati su dispositivi di telecomunicazione, digitali o informatici, con esclusione dei casi in cui tali carte, dispositivi o strumenti sono utilizzabili per generare l'informazione necessaria a effettuare direttamente un bonifico o un addebito diretto verso e da un conto di pagamento.

Sarà, pertanto, possibile procedere all'identificazione del cliente ed esecutore, o del titolare effettivo se effettuata in presenza di questi - mediante processi di identificazione elettronica ovvero di autenticazione informatica.

2. **identificazione del titolare effettivo:** Il cliente persona non fisica è tenuto a fornire i dati identificativi della persona individuata quale titolare effettivo ai sensi del Decreto Antiriciclaggio. Nello stesso Decreto è definito quale titolare effettivo "*la persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l'operazione è eseguita*". Si avranno perciò in via principale due casistiche di titolarità effettiva:
   a) il soggetto per conto del quale il cliente effettua un'operazione occasionale;
   b) la persona fisica o le persone fisiche che, in ultima istanza, possiedono o controllano l'entità giuridica o ne risultano beneficiari secondo i criteri individuati dall'art. 20 del Decreto Antiriciclaggio (nel caso in cui il cliente sia una persona non fisica).

Si rinvia a quanto descritto all'interno dell'**Allegato 2 - Definizione e Casistiche Titolare effettivo** per una trattazione specifica sull'individuazione del titolare effettivo a seconda della tipologia di clientela.

L'identificazione del Titolare Effettivo avviene anche senza la necessaria presenza dello stesso, ma contestualmente all'identificazione del cliente e sulla base dei dati e delle informazioni fornite dall'esecutore sotto la propria responsabilità (che permane anche circa l'obbligo di comunicare eventuali variazioni della titolarità effettiva). Qualora, a seconda della tipologia di soggetto, siano disponibili pubblici registri, elenchi, atti o documenti pubblici (ad esempio, archivi camerali, statuti, bilanci), l'identificazione del titolare effettivo deve essere riscontrata anche attraverso l'acquisizione dei dati reperibili su tali fonti.
Le verifiche effettuate ai fini dell'identificazione del titolare effettivo sono conservate per consentire la comprensione del percorso conoscitivo effettuato. Qualora, ai medesi fini, venga utilizzato il c.d. "criterio residuale", le Società del Gruppo tengono traccia delle ragioni che abbiano indotto all'applicazione di tale criterio, conservando i documenti utilizzati e lasciando traccia del percorso argomentativo utilizzato.

3. **verifica dei dati del cliente, dell'esecutore e del Titolare Effettivo:** l'attività consiste nell'effettuare una verifica circa la veridicità dei dati forniti e/o raccolti relativi al cliente, all'esecutore e al titolare effettivo mediante riscontro con quelli desumibili da fonti affidabili ed indipendenti, di cui va acquisita e conservata copia in formato cartaceo o elettronico.
   - Per quanto attiene al **cliente persona fisica ed all'esecutore** si procede a:
     - accertare l'autenticità e la validità del documento d'identità o di altro documento di riconoscimento equipollente acquisito e, per l'esecutore, accertare altresì l'esistenza e l'ampiezza del potere di rappresentanza in forza del quale egli opera in nome e per conto del cliente;
     - per i **minori** in mancanza della carta di identità o del passaporto[6], acquisire certificato di nascita (o foto autenticata) o eventuale provvedimento del giudice tutelare;
     - per i **soggetti non comunitari**, accertare l'autenticità e la validità del passaporto, del permesso di soggiorno, del titolo di viaggio per stranieri rilasciato dalla Questura o di altro documento da considerarsi equivalente ai sensi della normativa italiana;
     - Per gli **apolidi**, in mancanza dei documenti di cui sopra, i dati identificativi possono essere verificati attraverso il titolo di viaggio per apolidi (rilasciato ai sensi della Convenzione sullo Statuto degli Apolidi del 28.9.1954);
     - Per i titolari dello status di "**rifugiato**" o dello status di "**protezione sussidiaria**" i dati identificativi possono essere verificati anche attraverso i documenti di viaggio rilasciati dalla Questura (come previsto dall'articolo 24 del D. Lgs. 19 novembre 2007, n. 251);
     - in caso di incertezze o incongruenze, effettuare ulteriori controlli (ad es. consultazione sistema pubblico per la prevenzione del furto di identità).

   - In presenza di un cliente persona non fisica si procede a:
     - riscontrare i dati identificativi del cliente con informazioni desumibili da fonti affidabili e indipendenti, di cui si acquisiscono - in via autonoma o per il tramite del cliente - e conservano copie in formato cartaceo o elettronico;
     - con riferimento all'esecutore, accertare l'esistenza e l'ampiezza del potere di rappresentanza in forza del quale egli opera in nome e per conto del cliente;
     - con riferimento alla titolarità effettiva, adottare misure proporzionate al rischio al fine di ricostruirne, con ragionevole attendibilità, l'assetto proprietario e di controllo.

   Oltre al registro delle imprese italiano, rientrano tra le fonti affidabili e indipendenti per il riscontro dei dati identificativi del cliente diverso da persona fisica e del titolare effettivo:

   - gli albi ed elenchi di soggetti autorizzati, gli atti costitutivi, gli statuti, i bilanci o documenti equivalenti, le comunicazioni rese al pubblico in conformità alla normativa di settore (quali prospetti, comunicazioni di partecipazioni rilevanti o informazioni privilegiate);

[6] La carta di identità e il passaporto fino a 3 anni hanno validità triennale, dai 3 ai 18 anni hanno validità quinquennale.

- i registri dei titolari effettivi istituiti in altri paesi comunitari in attuazione degli articoli 30 e 31 della direttiva antiriciclaggio;
- le informazioni provenienti da organismi e autorità pubbliche, anche di altri paesi comunitari; tali informazioni possono essere acquisite anche attraverso i siti web.

In presenza di documentazione in lingua straniera devono essere adottati standard di diligenza professionale idonei ad accertarne l'autenticità e il reale contenuto (anche attraverso una traduzione giurata dell'originale). Nello specifico caso di soggetti provenienti da Paesi non comunitari la verifica va effettuata specificatamente attraverso il passaporto, il permesso di soggiorno o il titolo di viaggio per stranieri rilasciato dalla Questura.

In merito alle tempistiche dell'esecuzione di questa fase dell'adeguata verifica, il Decreto Antiriciclaggio impone che la stessa avvenga al momento dell'instaurazione del rapporto ovvero dell'esecuzione dell'operazione occasionale.
Per quanto attiene alla verifica circa la titolarità effettiva di clienti che non siano persone fisiche, volta ad individuare con ragionevole certezza il titolare effettivo ed accertarne i dati, deve essere conservata traccia delle verifiche effettuate.

4. **acquisizione e valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo[7] o delle operazioni occasionali**: l'attività si sostanzia nell'acquisizione di ulteriori informazioni circa lo scopo e la natura del rapporto o dell'operazione occasionale, nell'ottica dell'approccio basato sul rischio ed in modo tale da rendere il sistema di profilatura il più efficace possibile, oltre che gettare le basi per un monitoraggio più efficace circa l'operatività.
   Dovranno essere obbligatoriamente raccolte informazioni circa le finalità relative all'accensione del rapporto, l'attività lavorativa ed economica svolta, le relazioni intercorrenti tra il cliente e gli eventuali esecutori nonché tra il cliente ed il titolare effettivo del rapporto; secondo un approccio basato sul rischio, saranno da raccogliere ulteriori dati che possono riguardare, a titolo esemplificativo e non esaustivo:
   - l'origine dei fondi utilizzati nel rapporto;
   - la situazione economica (es., fonti di reddito) e patrimoniale del cliente (bilanci, dichiarazioni IVA e dei redditi, documenti e dichiarazioni provenienti dal datore di lavoro, da intermediari finanziari o altri soggetti), le relazioni d'affari e i rapporti con altri destinatari delle "Disposizioni di Adeguata verifica" pubblicate dalla Banca d'Italia;
   - la situazione lavorativa, economica e patrimoniale del titolare effettivo nonché, ove sia nota e conoscibile, di familiari e conviventi.

   Le informazioni sono richieste al cliente (o all'esecutore) ovvero desunte dal rapporto, quando sia possibile secondo l'approccio basato sul rischio e possono essere ricavate informazioni univoche. Ove vengano fornite dal cliente che sia classificato ad alto rischio, dovranno essere compiute verifiche circa la compatibilità di tali dati con le informazioni già acquisite autonomamente o desumibili dal rapporto.

5. **controllo costante del rapporto**: tale fase ha come oggetto una valutazione complessiva dell'intera operatività del cliente ed è demandata alla Filiale di competenza. Il controllo costante si svolge durante tutta la durata del rapporto, con lo scopo di mantenere sempre aggiornato il profilo di rischio del cliente e rilevare eventuali anomalie in ambito antiriciclaggio sorte in un tempo successivo all'instaurazione dei rapporti. Le tempistiche circa lo svolgimento di tale fase dell'adeguata verifica sono stabilite in ragione del grado di rischio assegnato al cliente, fermo restando che il Questionario di adeguata verifica deve essere necessariamente aggiornato nel momento in cui si rilevi che le informazioni utilizzate per l'ultima adeguata verifica non siano più attuali (ad es. in fase di revisione di pratiche di fido, o aggiornamento dei poteri di rappresentanza, variazione del titolare effettivo).
   La periodicità stabilità è di:
   - 12 mesi per i profili di rischio alto;
   - 24 mesi per i profili di rischio medio;

[7] Si veda l'**Allegato 5 – Elenco rapporti continuativi da sottoporre ad adeguata verifica.**

- 48 mesi per i profili di rischio basso;
- 60 mesi per i profili di rischio irrilevante.

Deve essere svolto in modo tempestivo al verificarsi di un evento che porti il cliente ad un aumento del punteggio di rischio tale da collocarlo in fascia alta oppure media, qualora i dati e le informazioni siano stati aggiornati in un periodo antecedente rispetto alle tempistiche precedentemente indicate.

Sinteticamente, il monitoraggio del cliente comporta:

a) l'analisi, eseguita anche con il supporto della procedura informatica di ausilio G.I.An.O.S., delle transazioni concluse durante il corso del rapporto;
b) la verifica della compatibilità di tali transazioni con la conoscenza del proprio cliente, delle sue attività commerciali e del suo profilo di rischio, avendo riguardo all'origine dei fondi e tenendo aggiornati i documenti, i dati e le informazioni detenute;
c) l'aggiornamento dell'adeguata/rafforzata verifica dei clienti in ragione del profilo di rischio assegnato dall'applicativo G.I.AN.O.S..

Di seguito, si riportano i moduli dell'applicativo GIANOS utilizzati allo scopo di valutare nel continuo l'operatività della clientela:

1. modulo Inattesi, per la valutazione delle operazioni anomale estratte in automatico dalla procedura;
2. modulo Gestione Profili di Rischio, dedicato alla generazione dei profili di rischio di riciclaggio per tutti i clienti della banca ai quali sarà, pertanto, attribuita una delle seguenti fasce di rischio: Alta, Media, Bassa, Irrilevante.
3. modulo Evidenze Usura, di ausilio agli intermediari nel monitoraggio del fenomeno;
4. modulo Know Your Customer (KYC), con funzioni dedicate all'approfondimento della conoscenza del cliente. In occasione dell'acquisizione del questionario di Adeguata verifica su clienti classificati in fascia di rischio Media o Alta, all'interno della funzione "Workflow Autorizzativo", presente nel modulo KYC viene aperta una pratica che deve essere valutata e quindi, "approvata" o "non approvata"; qualora il soggetto sia classificato in fascia di rischio Media, il Responsabile della dipendenza presso la quale è radicato il cliente può lavorare la pratica in autonomia mentre nel processo di valutazione dei clienti classificati in fascia di rischio Alta è coinvolta anche la Funzione Antiriciclaggio che riceve, a mezzo mail, la valutazione espressa dal Responsabile della dipendenza ed esprime una propria autonoma valutazione. Il questionario di adeguata verifica potrà quindi essere stampato e sottoposto alla firma del cliente solo al termine del processo di valutazione sopra descritto.

Per quanto riguarda le estrazioni periodiche relative ai moduli 1, 2 e 3, la Funzione Antiriciclaggio, al fine di fornire un ausilio alle strutture operative interessate, provvede mensilmente a comunicare l'avvenuta elaborazione ed i termini di lavorazione delle pratiche, fornendo nel contempo alcune istruzioni operative in ordine alle modalità di lavorazione ed alla natura delle informazioni che devono risultare dal testo di valutazione inserito dai Responsabili. Nel processo deve essere coinvolto qualunque dipendente che abbia contatto con la clientela (ad esempio, addetti all'istruttoria, al monitoraggio ed alla gestione dei clienti affidati).

3.1.1.2 Operatività "a distanza" (cliente non fisicamente presente)

Per operatività a distanza si intende quella svolta senza la presenza fisica del cliente. Si specifica che tale modalità di identificazione è svolta unicamente per l'apertura dello specifico prodotto "Conto corrente on line" (denominato "*conto IU*"), per il collocamento dei prodotti TFS e CQS attraverso la rete distributiva e per l'identificazione dei clienti della Igea Digital Bank.

Al ricorrere di simili circostanze si applicheranno misure ad hoc al fine di procedere all'identificazione del cliente. Le misure comprendono anche la consultazione di sistemi pubblici per la prevenzione del furto di identità, in considerazione dell'aumento del rischio del verificarsi del fenomeno di riciclaggio.

Per quanto riguarda il prodotto "Conto corrente on line" (destinato alla sola clientela classificata come "Consumatore") venduto dalla Unità Operativa Sviluppo Canali Digitali, per effettuare l'identificazione a distanza del cliente deve essere osservata la procedura che prevede le seguenti attività:

1. acquisizione in copia di due documenti di identità (ai sensi del D.P.R 445/2000) in corso di validità e della tessera sanitaria, ottenuti sia mediante caricamento, da parte del cliente, sul portale della Banca, sia mediante successivo inoltro a mezzo posta, unitamente al contratto sottoscritto; le fotocopie cartacee allegate al contratto devono recare anche la firma in originale del cliente per consentire un ulteriore riscontro tra le suddette firme e quelle apposte sui documenti;
2. verifica della esistenza/validità del documento di identità e della tessera sanitaria mediante accesso al portale web S.C.I.P.A.F.I. (Sistema Pubblico di Prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo e dei pagamenti dilazionati o differiti, con specifico riferimento al Furto d'Identità). Il Sistema consente il riscontro dei dati contenuti nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento e su quello dell'Agenzia delle Entrate.

Per la vendita di prodotti TFS e CQS, in capo alla Direzione Crediti al Lavoro, l'identificazione dei clienti acquisiti tramite le reti terze avviene attraverso l'invio (a mezzo posta elettronica) della copia datata e sottoscritta di un documento di riconoscimento in corso di validità, della tessera sanitaria o del Codice fiscale e del certificato INPS e attraverso la compilazione del Modulo di adeguata verifica della clientela, adempimento effettuato con l'assistenza telefonica di un addetto alla vendita della Banca. Il modulo così compilato viene restituito attraverso il servizio di Raccomandata elettronica "*t Notice*".

Per quanto attiene invece Igea Digital Bank, in caso di apertura di rapporti è utilizzata la Piattaforma Digitale Smile e sono state definite due diverse modalità di identificazione a distanza della clientela, in relazione alla tipologia di prodotto da sottoscrivere e al canale di vendita ed in considerazione dei relativi presidi dei rischi di frode ed operativi:

- Acquisizione di modulistica firmata digitalmente[8];
- Acquisizione del documento di identità e bonifico effettuato dal medesimo intestatario di conto corrente presso altra banca.

Inoltre, a supporto e rafforzamento di tali modalità di identificazione della clientela, sono state predisposte altre misure per garantire una maggiore sicurezza, quali:

- spedizione carta Bancomat all'indirizzo indicato dal cliente come domicilio;
- attivazione carta Bancomat tramite chiamata alla Banca previo riconoscimento del cliente attraverso domande identificative quali: nome e cognome, numero cellulare, numero carta d'identità, numero bancomat.

Nel caso di imprese, per i Titolari Effettivi, gli obblighi di Adeguata Verifica sono rispettati al momento della richiesta di apertura del Conto Corrente. L'identificazione del/i Titolare/i effettivo/i avviene senza che sia necessaria la loro presenza fisica, contestualmente all'identificazione del Cliente e sulla base dei dati identificativi da questi forniti. I dati identificativi sono annotati in piattaforma e riportati nel Modulo Adeguata Verifica che è firmato digitalmente dal Cliente e costituisce parte integrante del dossier documentale.

I questionari di adeguata verifica sono salvati su apposita repository sulla Piattaforma Digitale Smile e tutti i contratti sottoscritti sono inviati in conservazione all'Archivio.

La Funzione Antiriciclaggio è chiamata a verificare nel continuo la rispondenza delle suindicate modalità di identificazione a distanza alle migliori prassi operative adottate dal sistema, al fine di garantire il costante presidio dei

[8] L'identificazione della clientela, in sede di rilascio della Firma Digitale Certificata, può avvenire in 2 diverse modalità:
- *De Visu*: tramite riconoscimento diretto effettuato dall'incaricato alla registrazione dell'Ente Certificatore (InfoCert)
- WEB ID: tramite riconoscimento effettuato da un incaricato alla registrazione via webcam dell'Ente Certificatore (InfoCert)

rischi connessi al processo in argomento. L'Unità Internal Audit provvede a verificare, nell'ambito delle proprie attività ispettive in loco e/o a distanza, il rispetto delle disposizioni operative in materia di identificazione del titolare effettivo.

In conclusione, si indicano di seguito, le principali attività di verifica ulteriori rispetto a quelle previste per l'identificazione in presenza (indicati al punto 3 del paragrafo 3.1.1.1), finalizzate a verificare la veridicità dei dati forniti dal cliente:

i) contatto telefonico su utenza fissa (welcome call);

ii) invio di comunicazioni a un domicilio fisico con ricevuta di ritorno;

iii) bonifico effettuato dal cliente attraverso un intermediario bancario e finanziario con sede in Italia o in un paese comunitario;

iv) richiesta di invio (su posta elettronica certificata o altro strumento idoneo) di documentazione controfirmata, anche con l'utilizzo di sistemi di firma digitale;

v) verifica su residenza, domicilio, attività svolta, tramite richieste di informazioni ai competenti uffici;

vi) incontri in loco, effettuati avvalendosi di personale proprio o di terzi.

Simili misure devono essere modulate secondo un approccio basato sul rischio. Nell'impossibilità di ottenere i dati e le informazioni o di verificarne l'attendibilità o all'emergere di falsità o incoerenza delle informazioni fornite a distanza, vige l'obbligo di astenersi dal compiere l'operazione o avviare il rapporto continuativo ovvero porre fine al rapporto già in essere e valutare l'invio di una segnalazione di operazione sospetta.

3.1.2 Adeguata verifica rafforzata

L'adeguata verifica rafforzata consiste nell'adozione di misure caratterizzate da maggiore profondità, estensione e frequenza, nelle diverse fasi dell'adeguata verifica. L'adeguata verifica "rafforzata" è eseguita in presenza di soggetti ad "**alto rischio**" e ogni qualvolta vi siano dubbi circa la sussistenza di un elevato rischio di riciclaggio o di finanziamento al terrorismo: comporta l'acquisizione di informazioni aggiuntive sul cliente, sul titolare effettivo, su scopo e natura del rapporto e, se del caso, di singole operazioni se queste risultano non in linea con le caratteristiche del cliente e/o la movimentazione del rapporto. La graduazione nell'approfondimento delle analisi e della tipologia di dati da acquisire dipende in modo imprescindibile dalla conoscenza del cliente e della sua operatività: ***si sottolinea l'importanza di una compilazione il più possibile esaustiva del "Giudizio finale" nella Scheda d'Ausilio nel quale esporre gli aspetti significativi inerenti il cliente e la sua operatività e le valutazioni svolte in relazione alla presenza o meno di un effettivo "rischio riciclaggio".***

- L'adeguata verifica rafforzata si sostanzia nell'adozione di misure caratterizzate da maggiore profondità, estensione e frequenza, nelle diverse aree dell'adeguata verifica. A titolo esemplificativo, possono essere acquisite informazioni ulteriori rispetto ai dati identificativi ordinariamente previsti (ad esempio, quelli relativi a familiari/conviventi/società/soggetti in affari con il cliente); possono essere acquisite ulteriori informazioni sull'esecutore e il titolare effettivo; per le operazioni occasionali, possono essere acquisite informazioni sulla natura e lo scopo delle stesse; possono essere effettuate verifiche più incisive delle informazioni acquisite in merito al cliente, all'esecutore e al titolare effettivo ovvero possono essere svolte indagini più approfondite sulla natura e/o scopo del rapporto; possono essere aumentate l'intensità e la frequenza del monitoraggio nel controllo continuo.

In sintesi, le misure di adeguata verifica, atte ad acquisire maggiori informazioni sul cliente e sul titolare effettivo, sulla natura e lo scopo del rapporto, possono consistere:

- nell'acquisizione di una maggiore quantità di informazioni relative al cliente ed al titolare effettivo o all'assetto proprietario del cliente, al rapporto continuativo relativamente al numero, all'entità e alla frequenza delle operazioni attese e alle ragioni per cui il cliente chiede un determinato servizio, nonché alla destinazione dei fondi e alla natura dell'attività svolta dal cliente e dal titolare effettivo approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto;

- nell'acquisizione di una migliore qualità delle informazioni;
- in una maggiore frequenza degli aggiornamenti delle informazioni acquisite, attraverso controlli più frequenti sul rapporto e sulle singole operazioni.

Le attività di adeguata verifica rafforzata sono svolte con modalità operative che mirano ad acquisire una conoscenza il più approfondita del profilo soggettivo e oggettivo del cliente, tale ad escludere con ragionevole certezza il ricorrere di ipotesi di riciclaggio o finanziamento del terrorismo, o, in alternativa, a determinare la decisione di trasmettere una segnalazione di operazione sospetta all'UIF.

3.1.2.1 Fasi operative dell'adeguata verifica rafforzata

L'adeguata verifica rafforzata viene applicata in presenza di un rischio più elevato di riciclaggio o di finanziamento al terrorismo (si veda l'**Allegato 4 – Fattori di rischio elevato)** e, comunque, deve essere sempre applicata qualora ricorrano i seguenti casi:

- clientela non fisicamente presente: al ricorrere della fattispecie va accertata l'identità del cliente con le modalità supplementari previste *supra* (par. 3.1.1.2), certificando la documentazione fornita;
- clienti e titolari effettivi residenti in Paesi terzi ad alto rischio;
- clienti la cui struttura partecipativa veda la presenza di strutture qualificabili come veicoli di interposizione patrimoniale (i.e. Trust, Fiduciarie, fondazioni e altri soggetti che possano beneficiare dell'anonimato);
- società che hanno emesso strumenti al portatore (soprattutto se emessi in Paesi terzi ad alto rischio);
- clienti che svolgono attività economica caratterizzata da elevato uso del contante (i.e. compro oro, cambio valute, gioco e scommesse, etc.);
- clienti che svolgono attività economica riconducibile a settori particolarmente esposti a rischi di corruzione (appalti pubblici, sanità, edilizia, commercio di armi, difesa, industria bellica, industria estrattiva, raccolta e smaltimento rifiuti, produzione di energie rinnovabili);
- clientela classificata come Persona Esposta Politicamente;
- rapporti di c/c con intermediari creditizi finanziari con sede in Stati extracomunitari diversi dai paesi terzi ad alto rischio;
- operazioni con importi insolitamente rilevanti ovvero rispetto a cui sussistano dubbi circa la finalità delle stesse;
- soggetti presenti in black list per sospetto o fatti di terrorismo;
- soggetti interessati da accertamenti disposti dall'Autorità Giudiziaria[9] nell'ambito di procedimenti penali o per l'applicazione di misure di prevenzione;
- soggetti certificati "positivi" in *FastCheck* o in capo ai quali siano emerse notizie di stampa negativa (da altre fonti aperte e comunque apprese a livello di Gruppo) tali da integrare gli "Indici reputazionali negativi" previsti dall'Allegato 2, lettera *a,* n. 3 delle "*Disposizioni di Adeguata verifica*".

Nei casi per i quali è prevista l'applicazione di un regime di verifica rafforzata e comunque per tutti i soggetti collocati in fascia Alta di rischio di riciclaggio, è fatto obbligo di acquisire un *set* di informazioni più esteso rispetto a quello previsto per i soggetti sottoposti ad adeguata verifica. Più specificamente, dovrà essere acquisito ed archiviato in un fascicolo dedicato, salvato anche in formato elettronico, un corredo informativo che dovrà comprendere, minimalmente:

- copia di bilanci (forniti dal cliente e/o estratti dalla procedura Ribes);
- dichiarazioni dei redditi;

[9] Il procedimento circa la gestione degli accertamenti dell'Autorità Giudiziaria è contenuto nella Circolare "Direzione Generale 13/2017 del 14/09/2017 – Antiriciclaggio – Accertamenti dell'Autorità Giudiziaria". È previsto che alla ricezione di una richiesta di accertamento penale venga inserita, a cura dell'Unità Infrastrutture e Sicurezza, una notizia nell'Anagrafe Generale (status anagrafico A "Flag Antiriciclaggio"). La Funzione *Compliance* e Antiriciclaggio, ricevuta la comunicazione a mezzo e-mail sulla ricezione del provvedimento effettua un controllo sulla correttezza dell'attribuzione dello status.

- il numero, l'entità e la frequenza delle operazioni attese, per poter individuare eventuali scostamenti che potrebbero determinare elementi di sospetto;
- le ragioni per cui il cliente chiede un determinato prodotto o servizio, specie se le sue necessità finanziarie potrebbero essere soddisfatte al meglio in altro modo o in un altro paese;
- l'assetto proprietario e di controllo del cliente. In questo ambito è inclusa l'acquisizione e la valutazione di informazioni sulla reputazione del cliente e del titolare effettivo;
- consistenza patrimoniale;
- origine del patrimonio e dei fondi utilizzati nel rapporto;
- la destinazione dei fondi;
- visura camerale aggiornata (estratta da procedura Ribes);
- copia di fatture (relative alle operazioni rilevanti registrate sui rapporti);
- ogni utile informazione sull'attività svolta dal cliente;
- la presenza di relazioni familiari o di tipo giuridico e/o economico con altri clienti dell'Istituto (in tal caso la verifica dovrà essere estesa, con le medesime modalità, anche a tali soggetti);
- evidenza di accertamenti da parte dell'Autorità Giudiziaria nell'ambito di procedimenti penali o per l'applicazione di misure di prevenzione;
- notizie negative sul cliente apprese da organi di stampa o da altre fonti aperte o comunque apprese dall'Istituto;
- la natura dell'attività svolta dal cliente e dal titolare effettivo;
- valutazione comparative con l'operatività di soggetti con similari caratteristiche (professionali, di settore economico, di area geografica).

Per quanto attiene alle evidenze negative, queste vengono riscontrate mediante le "*Liste negative*" della procedura *FastCheck* utilizzata dal Gruppo ed integrata nel *Front End Unico (FEU).* La certificazione circa la effettiva coincidenza (oppure l'omonimia) dei clienti della banca con i soggetti estratti dalla procedura sarà effettuata dalla Rete, ed in caso di riscontro positivo (cioè in presenza di effettiva coincidenza dei soggetti) deve essere fatta richiesta alla Funzione Antiriciclaggio di un'autorizzazione all'instaurazione dei rapporti, allegando le informazioni utili al fine di valutare il rischio di riciclaggio connesso all'apertura del rapporto (a titolo esemplificativo, si citano le informazioni su natura e scopo dell'instaurando rapporto e sull'origine dei fondi, oltre a un'accurata descrizione della notizia riferita al potenziale cliente corredata dagli esiti dei primi approfondimenti svolti e dall'invio dell'eventuale documentazione reperita a sostegno delle ricerche svolte). Qualora l'autorizzazione venga concessa, la dipendenza dovrà indicare l'operatore che materialmente eseguirà l'accensione del rapporto; la Funzione *Compliance* e Antiriciclaggio richiederà all'Ufficio Organizzazione la temporanea attribuzione al suddetto operatore, di uno specifico profilo necessario per l'accensione del rapporto.

Tutta la clientela collocata in fascia Alta di rischio di riciclaggio (mediante la profilatura mensile eseguita dall'applicativo G.I.An.O.S.) dovrà essere sottoposta ad una adeguata verifica rafforzata da parte del Responsabile dell'Unità Operativa presso la quale il cliente intrattiene i propri rapporti (qualora il cliente intrattenga rapporti con più dipendenze, la procedura in automatico "assegnerà" la valutazione sulla base di criteri definiti dall'Outsourcer (tipologia di rapporti, data di accensione, etc.); eventuali variazioni nell'assegnazione dell'Unità competente per la valutazione, dovranno essere concordate con la Funzione Antiriciclaggio.

Sulla base della richiamata profilatura mensile, ciascuna Dipendenza/Filiale dovrà eseguire la verifica su tutti i soggetti classificati in fascia Alta di rischio di riciclaggio per i quali non risulti presente, in procedura G.I.An.O.S., una valutazione

in corso di validità; tale valutazione avrà una validità di 15 mesi. La valutazione circa l'operatività del cliente è esplicitata tramite la compilazione della Scheda di Ausilio richiamabile mediante il Modulo "*Gestione Profili di Rischio*" di G.I.An.O.S.. Nella propria attività, il valutatore potrà avvalersi dell'ausilio di altri dipendenti del Gruppo (ad esempio il Gestore della posizione, l'addetto titoli, etc.) per l'acquisizione di informazioni il più possibile complete. Lo stesso valutatore potrà, ove lo ritenga opportuno, condividere informazioni rilevanti, anche tramite scambio di mail e documentazione, con la Funzione Antiriciclaggio.

In esito alle attività di verifica, dovrà essere espressa una valutazione di coerenza (o meno) tra l'operatività del cliente ed il proprio profilo soggettivo, con l'indicazione in ordine alla volontà di procedere (o meno) ad una segnalazione di operazione sospetta e se si intenda (o meno) procedere con l'estinzione dei rapporti intestati e/o riconducibili al cliente.

La valutazione complessiva sull'operatività è espressa, come detto, all'interno della Scheda D'Ausilio alla Valutazione, composta di diverse sezioni, alcune già parzialmente alimentate dalla procedura, che dovranno essere implementate dall'operatore con le informazioni acquisite anche per il tramite del cliente stesso. Al riguardo si evidenzia la necessità di acquisire informazioni il più possibile dettagliate (e documentate) in ordine al profilo patrimoniale e reddituale dei clienti. Nell'ultima sezione della Scheda di Ausilio, denominata "*Valutazione finale*", l'operatore dovrà inserire un giudizio sulla rischiosità dell'operatività analizzata in termini di coerenza, compatibilità con il profilo economico finanziario. Il giudizio potrà essere motivato in forma descrittiva nell'apposito campo.

3.1.2.2 Clientela residente in Paesi terzi ad alto rischio

La prima ipotesi di applicazione delle misure di adeguata verifica rafforzata prevista dalla legge (art. 25 co. 4-bis del Decreto Antiriciclaggio) è relativa ai soggetti residenti in Paesi classificati ad alto rischio di riciclaggio o finanziamento del terrorismo (le società del Gruppo si avvalgono della classificazione dei Paesi terzi effettuata e periodicamente aggiornata da G.I.An.O.S.). Nello specifico, sono così definiti i "*paesi non appartenenti all'Unione europea i cui ordinamenti presentano carenze strategiche nei rispettivi regimi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo, per come individuati dalla Commissione europea nell'esercizio dei poteri di cui agli articoli 9 e 64 della direttiva*" (cfr. la lett. bb dell'art. 1, comma 2 del Decreto Antiriciclaggio ([10]). L'elenco dei Paesi terzi ad alto rischio è pubblicato nell'area della intranet aziendale dedicata all'Antiriciclaggio ed è periodicamente aggiornato a cura della Funzione AML.

Gli intermediari devono astenersi dall'instaurare rapporti continuativi o dall'eseguire operazioni o devono porre fine ai rapporti già in essere di cui siano, direttamente o indirettamente, parte società fiduciarie, trust, società anonime o controllate attraverso azioni al portatore aventi sede nei Paesi terzi ad alto rischio. Tali misure si applicano anche nei confronti delle ulteriori entità giuridiche aventi sede in tali Paesi qualora non sia possibile identificare il titolare effettivo dell'operazione/rapporto e verificarne l'identità.

L'eventuale apertura del rapporto o esecuzione di operazioni deve essere espressamente autorizzata per iscritto da un Alto Dirigente, sulla base di una relazione a questo sottoposta per il tramite della Funzione *Compliance* e Antiriciclaggio, redatta dal Responsabile della dipendenza alla quale è attribuito il cliente, che deve comprendere almeno:

- motivazione per cui il cliente intende aprire rapporti bancari in Italia;
- valutazione circa i rischi di riciclaggio /benefici sottesi all'apertura del rapporto, evidenza del canale di presentazione/entrata in rapporto del potenziale cliente con la Banca;
- documentazione che attesti la situazione patrimoniale e reddituale del cliente, es. le ultime dichiarazioni dei redditi ufficialmente presentate, gli ultimi bilanci ufficiali o relazioni semestrali approvati, atti pubblici di compravendita, altre informazioni tratte da fonti aperte purché attendibili e riscontrabili;

[10] Si rappresenta per completezza che l'Allegato 2 alle Disposizioni di Adeguata verifica della clientela (lettera *c*, n. 1) menziona tra i "*fattori di elevato rischio geografici*" i "*paesi terzi che fonti autorevoli e indipendenti ritengono carenti di efficaci presidi di prevenzione del riciclaggio*", ivi citando espressamente "*l'elenco pubblicato dal GAFI dei paesi a rischio elevato e non collaborativi*".

- verifica che il cliente non sia presente in liste pregiudizievoli, non abbia precedenti segnalazioni a suo carico o a carico di soggetti collegati, indagini fiscali o penali a suo carico o a carico di soggetti collegati, etc.

La relazione così redatta, corredata dal parere della Funzione Antiriciclaggio, dovrà essere sottoposta all'attenzione di un Alto Dirigente che potrà autorizzare o declinare la richiesta di accensione di un rapporto continuativo, la prosecuzione dello stesso ovvero l'esecuzione di una operazione. Alla clientela rientrante nella categoria in oggetto dovrà essere necessariamente attribuita una fascia di rischio "alta" e dovrà essere sottoposta ad un costante monitoraggio dei rapporti ad essa collegati, secondo le modalità di adeguata verifica rafforzata.

3.1.2.3 Trust

Il "trust" è un istituto giuridico, di origine anglosassone, e ricorre allorché con un atto tra vivi o *mortis causa* un *settlor*/disponente trasferisce ad un altro soggetto (il "trustee") beni o diritti con l'obbligo di amministrarli nell'interesse di un beneficiario/i oppure per il perseguimento di uno scopo determinato (trust di scopo), sotto l'eventuale vigilanza di un terzo ("*protector*"/guardiano), secondo le regole dettate dal disponente nell'atto istitutivo di trust dalla legge regolatrice dello stesso (Stato di istituzione del trust).

Le indicazioni riportate in seguito dovranno essere seguite sia nel caso in cui sia direttamente il trust a richiedere l'instaurazione di rapporti con la Banca che nel caso in cui il trust partecipi nel capitale del cliente, a prescindere dalla quota di partecipazione.

Con riferimento a tale catena di controllo, il titolare effettivo di un trust va individuato nei seguenti soggetti:

- Il trustee o i trustees;
- il costituente o i costituenti (disponente o settlor);
- Il guardiano i guardiani;
- I beneficiari o classi di beneficiari di un trust ove identificati nell'atto costitutivo, ovvero altre persone fisiche che esercitano il controllo sul trust o qualunque altra persona fisica che esercita, in ultima istanza, il controllo sul trust attraverso la proprietà diretta o indiretta o attraverso altri mezzi.

Il soggetto abilitato a richiedere l'apertura di rapporti per conto del trust è il trustee, quale amministratore e responsabile della gestione dello stesso, con le modalità che sono previste nel regolamento del trust.

Nell'apertura a gestione dei rapporti si seguiranno le seguenti modalità:

1) Il cliente tramite il trustee chiede di aprire rapporti intestati al trust;
2) La filiale, acquisita la documentazione, tra cui l'atto di costituzione (dev'essere copia dell'atto costitutivo e dei successivi atti modificativi) e il relativo regolamento recante tra l'altro eventuali limitazioni dei poteri del trustee, inoltra una relazione alla Funzione *Compliance* e Antiriciclaggio, nella quale deve essere indicato se il cliente sia stato presentato da soggetto favorevolmente conosciuto, lo scopo del Trust e del rapporto, l'origine dei fondi con i quali verrà creata la provvista sul rapporto e la natura della movimentazione attesa, eventuali anomalie rilevate (anche facendo riferimento agli indicatori di anomalia come individuati nella Comunicazione divulgata in proposito dall'UIF il 2 dicembre 2013). Tale relazione deve essere corredata della documentazione acquisita;
3) La Funzione *Compliance* e Antiriciclaggio, esaminata la relazione e la documentazione, autorizza (o meno) l'accensione del rapporto;
4) Nel caso di esito positivo, la Filiale provvede poi all'adeguata verifica ed all'apertura dei rapporti. Per l'individuazione del titolare effettivo si procede verificando i criteri indicati nell'**Allegato 2**.

N.B. Nei casi di coincidenza fra disponente/beneficiario è necessario monitorare con particolare cura la costituzione e l'operato dell'istituto in parola in quanto la finalità potrebbe essere quella di creare uno schermo (interposizione fittizia) fra il disponente ed il relativo patrimonio.

3.1.2.4 Fiduciarie

Le società fiduciarie non iscritte nella sezione separata dell'albo ex art. 106 TUB (SAE 273 "Società Fiduciarie di Amministrazione") sono sottoposte agli obblighi di adeguata verifica.

Qualora una delle suindicate Fiduciarie intenda accendere uno o più rapporti presso il ns. Istituto, la Filiale avrà cura di richiedere, per ogni rapporto acceso, se la Fiduciaria opera:

a) in nome e per conto proprio;

b) su mandato di un fiduciante (o di una cointestazione di fiducianti);

c) su mandato di una pluralità di fiducianti con apertura di un Conto Omnibus.

Caso a)

Nel caso di rapporto proprio della Fiduciaria, la Filiale deve individuare il titolare effettivo della Fiduciaria stessa, che dovrà essere collegato, in procedura Anagrafe Generale, sul singolo rapporto, mediante la nuova facoltà "**B**" (InfoCli/Anagrafe/Rapporto/Facoltà).

Caso b)

In presenza di un conto riconducibile ad un fiduciante (o ad una cointestazione di fiducianti), la Filiale deve:

- richiedere alla Fiduciaria una dichiarazione attestante l'identità del fiduciante, nonché copia della documentazione necessaria ai fini del censimento in Anagrafe Generale. Tale documentazione dovrà essere trasmessa dalla Fiduciaria alla Funzione *Compliance* e Antiriciclaggio, a mezzo PEC al seguente indirizzo: funzione_antiriciclaggio@postacert.cedacri.it; la Funzione *Compliance* e Antiriciclaggio avrà cura di inoltrare copia della documentazione al Responsabile della Filiale di pertinenza;
- avvalorare, per il rapporto fiduciario, il **dato aggiuntivo di rapporto 2087** (InfoCli/Anagrafe/Rapporto/Dati aggiuntivi) con l'NDG del fiduciante. Nel caso su un unico rapporto ci siano più fiducianti, è necessario creare una cointestazione con tutti i nominativi comunicati e inserire l'NDG della SCO (cointestazione) nel Dato Aggiuntivo suddetto;
- avvalorare con "S" il dato aggiuntivo di Ndg 2069 "Presente titolare effettivo" per indicare che, pur in assenza di titolari effettivi (in rete J), non deve esserne richiesto il censimento obbligatorio.

Caso c)

In presenza di conti correnti Omnibus, la Filiale:

- deve avvalorare il Dato Aggiuntivo 9013 a livello di rapporto (Infocli/Anagrafe/Rapporto/Dati aggiuntivi) con S per indicare che il conto è omnibus;
- deve avvalorare con "S" il dato aggiuntivo di NDG 2069 "Presente titolare effettivo" per indicare che, pur in assenza di titolari effettivi (in rete J), non deve esserne richiesto il censimento obbligatorio;
- per ogni singola operazione sul rapporto omnibus:

- deve censire in anagrafe generale il fiduciante dell'operazione, comunicato per iscritto dal rappresentante della Fiduciaria, sulla base dei documenti forniti;
- deve avvalorare il campo "**NDG Titolare Effettivo Operazione**" nella mappa di registrazione dati per l'antiriciclaggio (ARRE) in procedura Nuovo sportello, con l'NDG del fiduciante dell'operazione. L'NDG dichiarato può essere sia di persona fisica sia di persona giuridica; in quest'ultimo caso i soggetti censiti come titolari effettivi della persona giuridica verranno caricati automaticamente nell'Archivio Unico Informatico.

- non deve avvalorare il dato aggiuntivo di rapporto 2087.

Al fine di garantire il rispetto dell'operatività sopra citata, la Filiale deve apporre un **blocco totale** sul rapporto Omnibus. Tale blocco potrà essere rimosso dal Responsabile della Filiale previa verifica della avvenuta ricezione dell'indicazione del titolare effettivo da parte della Fiduciaria.

È fatto assoluto divieto di accendere dossier titoli Omnibus o collegare dossier titoli riconducibili a singoli fiduciani a rapporti di conto corrente Omnibus.

Si precisa infine che:

- per la gestione dei fiduciani in procedura anagrafe è necessario assegnare un apposito profilo di sicurezza da richiedere a mezzo mail all'Unità Organizzazione, previa autorizzazione della Funzione *Compliance* e Antiriciclaggio;
- la stampa dell'adeguata verifica non riporta nel campo "titolare effettivo" i dati del fiduciante essendo questi secretati, seppur risultino visualizzati, al momento della compilazione del questionario, dal collega dotato del profilo di sicurezza suddetto.

3.1.2.5 Persone Politicamente Esposte

I soggetti rientranti nella categoria delle Persone Esposte Politicamente (PEP) devono essere sottoposti a misure rafforzate di adeguata verifica ai sensi dell'art. 25 co. 4 del Decreto Antiriciclaggio, in considerazione della loro maggiore esposizione al rischio di fenomeni corruttivi/collusivi, siano essi residenti in altri Stati comunitari o in Stati extracomunitari (PEP non residenti) o residenti nel territorio nazionale (PEP residenti). Ai sensi dell'art. 1 lettera dd) del Decreto Antiriciclaggio rientrano nella definizione di PEP i cittadini che occupano o hanno cessato di occupare da meno di un anno le seguenti cariche pubbliche:

a) Presidente della Repubblica, Presidente del Consiglio, Ministro, Vice-Ministro e Sottosegretario, Presidente di Regione, assessore regionale, Sindaco di capoluogo di provincia o città metropolitana, Sindaco di comune con popolazione non inferiore a 15.000 abitanti nonché' cariche analoghe in Stati esteri;
b) deputato, senatore, parlamentare europeo, consigliere regionale nonché' cariche analoghe in Stati esteri;
c) membro degli organi direttivi centrali di partiti politici;
d) giudice della Corte Costituzionale, magistrato della Corte di Cassazione o della Corte dei conti, consigliere di Stato e altri componenti del Consiglio di Giustizia Amministrativa per la Regione siciliana nonché' cariche analoghe in Stati esteri;
e) membro degli organi direttivi delle banche centrali e delle autorità indipendenti;
f) ambasciatore, incaricato d'affari ovvero cariche equivalenti in Stati esteri, ufficiale di grado apicale delle forze armate ovvero cariche analoghe in Stati esteri;
g) componente degli organi di amministrazione, direzione o controllo delle imprese controllate, anche indirettamente, dallo Stato italiano o da uno Stato estero ovvero partecipate, in misura prevalente o totalitaria, dalle Regioni, da comuni capoluoghi di provincia e città metropolitane e da comuni con popolazione complessivamente non inferiore a 15.000 abitanti;
h) direttore generale di ASL e di azienda ospedaliera, di azienda ospedaliera universitaria e degli altri enti del servizio sanitario nazionale;
i) direttore, vicedirettore e membro dell'organo di gestione o soggetto svolgenti funzioni equivalenti in organizzazioni internazionali.

Sono da considerarsi PEP anche i loro familiari, intesi quali *"i genitori, il coniuge o la persona legata in unione civile o convivenza di fatto o istituti assimilabili alla persona politicamente esposta, i figli e i loro coniugi nonché le persone legate ai figli in unione civile o convivenza di fatto o istituti assimilabili"* e coloro che con i predetti soggetti intrattengono notoriamente stretti legami, ossia *"le persone fisiche che, ai sensi del presente decreto detengono, congiuntamente alla persona politicamente esposta, la titolarità effettiva di enti giuridici, trust e istituti giuridici affini ovvero che intrattengono con la persona politicamente esposta stretti rapporti d'affari"* e *"le persone fisiche che detengono solo formalmente il controllo totalitario di un'entità notoriamente costituita, di fatto, nell'interesse e a beneficio di una persona politicamente esposta"*.

Il Sistema Informativo Cedacri è stato implementato per acquisire periodicamente un flusso costante da una banca dati aggiornata in tempo reale al fine di individuare l'appartenenza di un cliente alle liste in questione.

In via preliminare dovranno essere perciò stabilite procedure adeguate basate sul rischio, al fine di determinare se il cliente sia o meno una persona politicamente esposta.

Qualora si sia in presenza di un soggetto PEP in base a tali verifiche, occorre raccogliere informazioni più approfondite in merito a:

- origine dei fondi utilizzati nel rapporto (ad es. acquisendo atto di successione qualora l'origine dei fondi impiegata nel rapporto sia "eredità");
- situazione economica (fonti di reddito) e patrimoniale del cliente (ad es., acquisendo dichiarazione dei redditi, bilanci, dichiarazioni e attestati provenienti da altri soggetti obbligati);
- situazione lavorativa, economica e patrimoniale di familiari rientranti nella nozione di PEPs;
- eventuali relazioni d'affari rilevanti ai fini della normativa (ad. es., partecipazioni societarie).

Al termine della fase di raccolta delle informazioni sarà onere del Responsabile della Filiale ottenere l'autorizzazione dell'Alto Dirigente per l'avvio o la prosecuzione di un rapporto continuativo con tali clienti. Si precisa a tale ultimo proposito che l'autorizzazione in parola riguarda ciascun nuovo rapporto riferito ad un cliente PEP, anche qualora si tratti di clienti già acquisiti e autorizzati in precedenza. La richiesta deve essere inoltrata alla Funzione *Compliance* e Antiriciclaggio corroborata da una relazione sul cliente, sulla natura e sullo scopo del rapporto che si intende aprire, nonché ogni altra informazione utile per una compiuta valutazione da parte dell'Organo deliberante (allegando eventualmente documentazione a supporto). La decisione in merito sarà comunicata all'addetto dal Responsabile di Filiale, una volta ottenuto riscontro circa l'avvenuta autorizzazione all'accensione del rapporto e/o all'esecuzione dell'operazione.

Poiché l'accensione di rapporti intestati ad un PEP necessita dell'attribuzione di uno specifico profilo operativo, la Filiale deve comunicare a mezzo mail alla Funzione *Compliance* e Antiriciclaggio il nome e la matricola dell'addetto che procederà all'accensione del rapporto e la Funzione *Compliance*, verificata l'avvenuta acquisizione dell'autorizzazione da parte dell'Alto Dirigente, richiederà all'Ufficio Organizzazione la temporanea attribuzione del citato profilo.

La certificazione, da parte della Filiale, della qualifica di PEP (mediante la procedura FastCheck) relativa ad un cliente, determina l'automatica attribuzione al soggetto di un punteggio ulteriore nell'ambito del diagnostico G.I.An.O.S. che determinerà la collocazione del cliente in fascia "Alta" di rischio che consentirà di sottoporre il rapporto ad un controllo costante e rafforzato.

Si evidenzia che la qualifica di PEP potrebbe non rilevare per i rapporti nei quali il soggetto intervenga in veste di organo della Pubblica Amministrazione, così come previsto all'art. 24, comma 5, lett. c), del Decreto Antiriciclaggio.

3.1.2.6 Rapporti di C/C con intermediari finanziari con sede in Paesi terzi ad alto rischio

Ai sensi dell'art. 25 co. 2 del Decreto Antiriciclaggio l'accensione di conti di corrispondenza transfrontalieri rappresenta un'ipotesi per la quale è prevista l'applicazione di misure rafforzate di adeguata verifica. Si tratta dell'apertura di conti con enti corrispondenti di Paesi terzi. Al ricorrere di tale fattispecie le Società del Gruppo dovranno:

- raccogliere informazioni sull'ente corrispondente per comprendere la natura delle attività, la reputazione e la qualità della vigilanza cui è soggetto;
- valutare la qualità dei controlli in materia di contrasto al riciclaggio o al finanziamento del terrorismo cui l'ente corrispondente è soggetto;
- richiedere l'autorizzazione all'Alto Dirigente/ dell'Alta Dirigenza per l'apertura del rapporto di corrispondenza;
- definire, per iscritto, un accordo con l'ente corrispondente e i relativi obblighi per l'adempimento dell'adeguata verifica della clientela. L'accordo deve anche prevedere: i) le modalità attraverso le quali poter monitorare il rapporto di corrispondenza per accertare se la controparte adempia agli obblighi di adeguata verifica della clientela ed effettui gli altri controlli previsti dalla disciplina antiriciclaggio; ii) l'obbligo per la controparte di fornire, su

richiesta, informazioni su determinate transazioni o determinati clienti della controparte; iii) la possibilità di effettuare sopralluoghi e verifiche a campione per accertare l'efficacia delle politiche e delle procedure antiriciclaggio della controparte; iv) l'obbligo per la controparte di comunicare adeguatamente l'esistenza di relazioni della controparte con altri intermediari ("corrispondenti indiretti") che possano utilizzare i conti aperti con Società del Gruppo, in particolare per quanto riguarda l'area geografica di operatività dei corrispondenti indiretti e la disponibilità di questi ultimi a impartire istruzioni trasparenti in modo che siano note tutte le parti coinvolte nelle operazioni; v) l'obbligo per la controparte di impartire le istruzioni al corrispondente indiretto;

- assicurarsi che l'ente corrispondente abbia verificato l'identità dei clienti, che abbia assolto agli obblighi di adeguata verifica della clientela, che sia in grado fornire, a richiesta, i dati del cliente e del titolare effettivo mediante la compilazione e sottoscrizione di un questionario predisposto dalla Banca. Dovrà essere valutata la completezza delle informazioni e della documentazione fornite, considerando eventuali lacune ai fini di una rivalutazione del profilo di rischio del rispondente. Sarà, altresì, da acquisire espressa attestazione del rispondente circa l'inesistenza di impedimento normativi o contrattuali alla tempestiva trasmissione delle informazioni richieste;
- acquisire presso il rispondente, informazioni idonee a comprendere pienamente la natura delle attività da esso svolte, anche con riferimento ai servizi prestati ai clienti in relazione ai quali vengono utilizzati il conto o i conti accesi presso la banca.

Nei casi di rapporti continuativi e operazioni che coinvolgono Paesi terzi ad alto rischio, occorre anche:

a) acquisire informazioni aggiuntive in merito allo scopo e alla natura del rapporto continuativo o della prestazione professionale;
b) acquisire informazioni sull'origine dei fondi e sulla situazione economico-patrimoniale del cliente e del titolare effettivo;
c) acquisire informazioni sulle motivazioni delle operazioni previste o eseguite;
d) acquisire l'autorizzazione dell'Alta Dirigenza prima di avviare o proseguire o intrattenere un rapporto continuativo o effettuare un'operazione che coinvolga Paesi terzi ad alto rischio;
e) assicurare un controllo costante e rafforzato del rapporto continuativo, aumentando la frequenza e l'intensità dei controlli effettuati e individuando schemi operativi da sottoporre ad approfondimento.

3.1.2.7 Operazioni con importi insolitamente rilevanti ovvero rispetto a cui sussistano dubbi circa la finalità delle stesse

Le Disposizioni di Banca d'Italia in materia di adeguata verifica impongono obblighi di adeguata verifica rafforzata della clientela circa operazioni caratterizzate da importi insolitamente elevati o anomale rispetto alla consueta operatività del cliente ovvero per operazioni rispetto alle quali sussistono dubbi circa la finalità cui le medesime sono, in concreto, preordinate.

Al riguardo, un utile strumento per individuare comportamenti sospetti è rappresentato dagli Indicatori di anomalia emanati ed aggiornati periodicamente dalla Banca d'Italia nonché dagli schemi rappresentativi di comportamenti anomali pubblicati nel tempo dalla UIF.

Le Società del Gruppo devono adottare *"misure adeguate per comprendere contesto e finalità di queste operazioni e determinarne la coerenza con il profilo economico del cliente"* e porre in essere *"un più frequente controllo costante del rapporto continuativo e delle ulteriori operazioni eseguite."*[11]

[11] Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo – Banca d'Italia (30 luglio 2019) – Parte IV, sez VI.

Per intercettare tali operazioni le Società del Gruppo si avvalgono di appositi applicativi informatici (ad es.: il modulo "G.I.An.O.S. Inattesi"); la Funzione *Compliance* e Antiriciclaggio verifica periodicamente la correttezza dei parametri impostati attivandosi con l'outsourcer informatico per l'eventuale rimodulazione.

3.1.2.8 Soggetti presenti in black list per sospetto o fatti di terrorismo

Un'ulteriore ipotesi di misure rafforzate di adeguata verifica ricorre nel momento in cui, in sede di apertura del rapporto o in presenza di un rapporto già aperto ovvero a fronte di una richiesta di operazione occasionale, emerga una coincidenza dei nominativi di clienti o di soggetti che hanno richiesto l'apertura di un rapporto o l'effettuazione di un'operazione occasionale, con nominativi presenti nelle cd. Black List. In questo caso, la Rete verifica la presenza di eventuali casi di omonimia o "falsi positivi" (ossia casi in cui il soggetto sotto attenzione non coincida con il nominativo estratto dalla lista), conservando traccia e archiviando la relativa documentazione acquisita e procedendo con il consueto *iter* di apertura dei rapporti ; di contro, qualora si accerti la coincidenza tra il cliente e i soggetti presenti nelle Black List, la Dipendenza deve immediatamente informare la Funzione *Compliance* e Antiriciclaggio che procederà a disporre l'immediato blocco del rapporto (ove già in essere) e delle eventuali somme depositate sullo stesso ovvero comunicherà alla Dipendenza il divieto assoluto di accendere un nuovo rapporto o eseguire l'operazione occasionale. Nel contempo, la Funzione *Compliance* e Antiriciclaggio dovrà valutare se inviare una Segnalazione di Operazione Sospetta alla U.I.F., anche nell'ottica della confisca dei fondi e delle risorse economiche da parte del Ministero dell'Economia e delle Finanze ex art. 4 del D.Lgs. 231/2007. La Funzione *Compliance* e Antiriciclaggio informa l'Alta Direzione di quanto emerso e delle azioni intraprese.

In ogni caso, la Funzione *Compliance* e Antiriciclaggio avvia le procedure da seguire con le Autorità previste dalle disposizioni per il congelamento dei Fondi (si veda in merito il capitolo 5).

3.2 Adeguata verifica della clientela da parte di terzi

La normativa antiriciclaggio prevede la possibilità di affidare a terzi qualificati l'effettuazione degli obblighi di identificazione e adeguata verifica della clientela, secondo modalità che variano in ragione del soggetto incaricato. In particolare, l'obbligo di identificazione e adeguata verifica in assenza del cliente si ritiene assolto mediante il rilascio di un'idonea attestazione da parte di uno dei seguenti soggetti, con i quali i clienti abbiano rapporti continuativi e in relazione ai quali siano stati già identificati:

- 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;
- gli intermediari bancari e finanziari comunitari;
- 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.

L'attestazione deve espressamente confermare il corretto adempimento degli obblighi antiriciclaggio da parte dell'attestante, in relazione alle varie attività effettuate. Il contenuto dell'attestazione varia a seconda dello specifico obbligo di adeguata verifica cui essa è diretta; in base a tale criterio, essa deve contenere:

- i dati identificativi del cliente, dell'esecutore e del titolare effettivo ai fini dell'adempimento dell'obbligo di identificazione;
- l'indicazione delle tipologie delle fonti utilizzate per l'accertamento e per la verifica dell'identità;
- le informazioni sulla natura e sullo scopo del rapporto da aprire e dell'operazione occasionale da eseguire ai fini dell'adempimento del relativo obbligo.

Copia dei documenti e delle informazioni acquisite deve essere resa disponibile in sede di verifica da parte dell'intermediario responsabile ovvero inviata tempestivamente da parte dei terzi su richiesta dell'intermediario responsabile dell'adeguata verifica.

L'attestazione può essere resa in forma cartacea o informatica e in via autonoma ovvero in connessione con specifiche operazioni e può consistere, oltre che in un bonifico qualificato, anche nell'invio, per mezzo di sistemi informatici, dei dati identificativi del cliente da parte dell'intermediario che abbia provveduto all'identificazione mediante contatto diretto.

Permane comunque l'obbligo di procedere all'identificazione diretta, qualora si abbia motivo di ritenere che l'identificazione indiretta o a distanza non sia attendibile o non consenta l'acquisizione delle informazioni necessarie.

La Banca d'Italia prevede la possibilità che soggetti terzi possano effettuare solo l'identificazione del cliente, dell'esecutore e del titolare effettivo, inclusa l'acquisizione di copia dei documenti di identità. Essi sono:
1) i mediatori creditizi e gli agenti in attività finanziaria, salvo se non previsto diversamente dalla legge;

2) i "soggetti convenzionati e agenti", con le modalità previste dall'articolo 44 del decreto antiriciclaggio;

3) i collaboratori esterni che, in virtù di apposita convenzione, operano in nome e per conto dei destinatari nel proporre alla clientela la sottoscrizione di contratti, riconducibili alla loro attività istituzionale, relativi al credito al consumo ovvero al *leasing*, al *factoring*, al microcredito, al credito agrario e peschereccio.

La convenzione specifica gli obblighi da assolvere in materia di identificazione e le modalità e i tempi di adempimento, ivi inclusi i tempi di trasmissione delle informazioni al destinatario, nonché la responsabilità del collaboratore per il non corretto svolgimento dell'attività assegnatagli.

Collaboratori esterni

L'articolo 27 comma 5 del Decreto Antiriciclaggio prevede che *"nel caso di rapporti continuativi relativi all'erogazione di credito al consumo, di leasing o di altre tipologie operative indicate dalla Banca d'Italia, l'identificazione può essere effettuata da collaboratori esterni legati all'intermediario da apposita convenzione".*

Tali collaboratori operano sulla base di un'apposita convenzione, che deve specificare gli obblighi da assolvere in materia di identificazione e le modalità e i tempi di adempimento, ivi inclusi i tempi di trasmissione delle informazioni all'intermediario, nonché la responsabilità del collaboratore per il non corretto svolgimento dell'attività assegnatagli.

3.3 Obblighi della clientela (art.22)

I clienti hanno l'obbligo di fornire per iscritto e sotto la propria responsabilità tutte le informazioni necessarie e aggiornate per consentire alle Società del Gruppo di adempiere agli obblighi di adeguata verifica della clientela ed ai fini dell'identificazione del titolare effettivo. Per le imprese dotate di personalità giuridica sono gli amministratori che hanno l'obbligo di acquisire, a seguito di espressa richiesta rivolta ai soci, le informazioni; per le persone giuridiche private (fondazioni, enti e associazioni con personalità giuridica) tale compito è in capo ai fondatori ove in vita ovvero ai soggetti cui è attribuita la rappresentanza e l'amministrazione dell'ente.

Le informazioni devono essere conservate per un periodo non inferiore ai 5 anni dalla cessazione del ruolo amministrativo e le rendono prontamente disponibili alle autorità di vigilanza.

Per quanto attiene ai trust espressi sono individuati nei fiduciari (trustee, ossia l'amministratore del trust), nonché le persone che esercitano diritti, poteri e facoltà equivalenti in istituti giuridici affini, purché stabiliti o residenti sul territorio della Repubblica italiana, i soggetti deputati ad ottenere e detenere informazioni adeguate, accurate e aggiornate sulla titolarità effettiva del trust, o dell'istituto giuridico affine, così come individuata a seconda dei criteri riportati nell'**Allegato 2** - **Definizione e Casistiche Titolare effettivo**.

Tale obbligo non esonera le Società del Gruppo dal verificare la veridicità della documentazione ricevuta utilizzando sistemi informatici di controllo interni e/o messi a disposizione dalle autorità di settore (es. visure camerali).

3.4 Obbligo di astensione (art. 42)

Nei casi di impossibilità oggettiva (ossia qualora dalle informazioni comunicate dal cliente o dalle evidenze della banca risulti che non è possibile concludere il processo di adeguata verifica e la profilatura del cliente in base al rischio) di

effettuare l'adeguata verifica *(ad esempio perché il cliente si rifiuta di fornire tutte le informazioni necessarie, oppure il cliente continua a fornire documentazione palesemente falsa)*, è obbligatorio astenersi dall'instaurare il rapporto, eseguire l'operazione ovvero proseguire il rapporto.

In tali casi e in base alle circostanze deve essere valutata la possibilità di inserire una segnalazione di operazione sospetta (si veda *infra* cap. 9).

Qualora il Gruppo non sia in grado di adempiere oggettivamente agli obblighi di AV, non instaura rapporti continuativi, né esegue operazioni e, se del caso, procede all'estinzione del rapporto continuativo già in essere, inoltre valuta se effettuare una segnalazione di operazione sospetta

4 LIMITAZIONE ALL'USO DEL CONTANTE (ART.49)

L'art. 49 comma 1 del D. Lgs.231/07 e s.m.i. prevede che:

"È vietato il trasferimento di denaro contante e di titoli al portatore in euro o in valuta estera, effettuato a qualsiasi titolo tra soggetti diversi, siano esse persone fisiche o giuridiche, quando il valore oggetto di trasferimento, è complessivamente pari o superiore a 3.000 euro. Il trasferimento superiore al predetto limite, quale ne sia la causa o il titolo, è vietato anche quando è effettuato con più pagamenti inferiori alla soglia che appaiono artificiosamente frazionati […]".

Il trasferimento di contante per importi pari o superiore a €. 3.000,00 può aver luogo per il tramite di banche, istituti di moneta elettronica (IMEL) e Poste Italiane S.p.A., previa consegna della somma in contanti, con disposizione accettata per iscritto dall'intermediario stesso. Il beneficiario ha diritto di ottenere il pagamento nella provincia del proprio domicilio, a decorrere dal terzo giorno lavorativo successivo a quello dell'accettazione.

Il d. lgs. 124/2019 ha introdotto il comma 3 bis all'art. 49 del decreto antiriciclaggio: "A decorrere dal 1° luglio 2020 e fino al 31 dicembre 2021, il divieto di cui al comma 1 e la soglia di cui al comma 3 sono riferiti alla cifra di 2000 euro. A decorrere dal 1° gennaio 2022, il predetto divieto e la predetta soglia sono riferiti alla cifra di 1.000 euro".

Si rammentano in aggiunta le limitazioni previste per assegni bancari, circolari e postali, individuate sempre dall'art 49 del Decreto, commi 5, 6 e 7:

"Gli assegni bancari e postali emessi per importi pari o superiori a 1.000 euro devono recare l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità. Gli assegni bancari e postali emessi all'ordine del traente possono essere girati unicamente per l'incasso a una banca o a Poste Italiane S.p.A. Gli assegni circolari, vaglia postali e cambiari sono emessi con l'indicazione del nome o della ragione sociale del beneficiario e la clausola di non trasferibilità".

4.1 Operazioni di versamento di contanti o valori provenienti da altri Stati

Le Disposizioni in materia di adeguata verifica della clientela individuano quale fattore di rischio elevato il versamento di contante o valori provenienti dall'estero, in particolare quando l'importo dell'operazione è pari o superiore a 10.000 euro. In questo ambito, deve essere richiesta al cliente copia della dichiarazione di trasferimento di contante prevista dall'articolo 3 del decreto legislativo 19 novembre 2008, n. 195, e deve essere approfondito l'eventuale comportamento di rifiuto o riluttanza del cliente a fornire la documentazione.[12]

[12] Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo – Banca d'Italia (30 luglio 2019) – Allegato 2, lettera *b,* n. 4.

4.2 Operatività con banconote di grosso taglio

In presenza di operazioni in contante frequenti e ingiustificate, caratterizzate dall'utilizzo di banconote in euro di grosso taglio le Disposizioni in materia di adeguata verifica della clientela impongono che vengano condotti approfondimenti, anche con il cliente, per verificare le ragioni alla base di una simile operatività[13]. L'eventuale presenza di biglietti danneggiati o contraffatti deve essere considerato un ulteriore elemento di rischio.

All'occorrenza di una simile fattispecie deve essere fatto compilare l'apposito questionario G.I.An.O.S. relativo alle operazioni in contanti.

4.3 Obbligo di comunicazione al Ministero dell'Economia e delle Finanze delle infrazioni

L' art. 51 del Decreto Antiriciclaggio obbliga gli intermediari che abbiano notizia delle infrazioni agli obblighi riportati in materia di violazioni circa le limitazioni all'uso del contante, di riferirne entro trenta giorni al Ministero dell'Economia e delle Finanze, salvo che la stessa non sia già stata oggetto di segnalazione ai sensi dell'art. 35 dello stesso Decreto.

Nel caso l'infrazione riguardi assegni bancari e circolari, libretti al portatore o titoli similari la comunicazione deve essere effettuata dalla banca che li accetta in versamento e da quella che ne effettua l'estinzione.

Al realizzarsi dell'illecito, il Responsabile della struttura operativa provvederà personalmente a segnalare senza indugio, alla Funzione *Compliance* e Antiriciclaggio, gli estremi dell'operazione mediante l'apposito modulo, debitamente compilato e corredato di due fotocopie del titolo. La documentazione completa dovrà essere trasmessa in busta chiusa accompagnata dal modulo di trasmissione valori; copia della stessa sarà conservata in apposito dossier in Filiale. Il Responsabile della Filiale avrà cura di accertare l'avvenuta ricezione, da parte del ricevente, della documentazione inviata.

4.3.1 Funzione Antiriciclaggio: verifica ed inoltro segnalazione al MEF

La Funzione *Compliance* e Antiriciclaggio, non appena ricevuta la suddetta documentazione, provvederà ad inoltrare la prevista comunicazione al Ministero dell'Economia e delle Finanze - Ragioneria Territoriale dello Stato (competente per Territorio), mediante l'utilizzo della procedura informatizzata, denominata "SIAR – Segnalazioni Infrazioni Antiriciclaggio".

Tale procedura facilita e velocizza l'invio delle previste segnalazioni delle infrazioni relative agli illeciti in materia di antiriciclaggio (trasferimento tra privati di denaro contante o titoli al portatore oltre i limiti previsti, traenza di assegni bancari privi della clausola di non trasferibilità per importi superiori ai limiti previsti, presenza di libretti al portatore recanti un saldo creditore superiore ai limiti previsti).

Per inviare la comunicazione con tutti gli estremi relativi alla infrazione e ai soggetti coinvolti, la Funzione Antiriciclaggio dovrà accedere ad una sezione riservata del portale istituzionale www.siar.mef.gov.it mediante l'utilizzo di credenziali rilasciate dal MEF al Responsabile della *Compliance* e Antiriciclaggio. L'accesso potrà avvenire mediante uno dei due percorsi alternativi di seguito indicati:

- Sistema delle Ragionerie > RGS sul territorio > SIAR;
- Attività istituzionali > Vigilanza e Controllo di Finanza pubblica > SIAR.

L'intero processo dovrà essere completato con la massima sollecitudine e comunque inderogabilmente entro e non oltre 30 giorni dal momento in cui l'Istituto ha avuto notizia dell'infrazione.

[13] Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo - Banca d'Italia (30 luglio 2019) – Parte IV, sez. II.

4.4 Acquisto di beni e di prestazioni di servizi legati al turismo

Il Decreto Legge "Semplificazioni"[14] ha innalzato il limite circa il trasferimento di denaro tra soggetti diversi a 15 mila euro per quanto riguarda l'acquisto di beni e di prestazioni di servizi legati al turismo, effettuati presso attività legate al turismo - commercio al dettaglio ed assimilate e agenzie di viaggi e turismo, da persone fisiche di cittadinanza diversa da quella italiana e comunque diversa da quella di uno dei paesi dell'Unione europea ovvero dello Spazio economico europeo, che abbiano residenza fuori dal territorio dello Stato, a condizione che il cedente del bene o il prestatore del servizio provveda ai seguenti adempimenti, disciplinati dall'Agenzia delle Entrate con provvedimento 45160/2012 del 23/03/2012:

a) all'atto dell'effettuazione dell'operazione acquisisca fotocopia del passaporto del cessionario e/o del committente e apposita autocertificazione dello stesso cessionario e/o del committente[15] di non essere cittadino italiano né cittadino di uno dei Paesi dell'Unione europea ovvero dello Spazio economico europeo e che ha la residenza fuori del territorio dello Stato;
b) nel primo giorno feriale successivo a quello di effettuazione dell'operazione versi il denaro contante incassato in un conto corrente intestato allo stesso cedente o prestatore presso un intermediario finanziario, consegnando a quest'ultimo fotocopia dei documenti di cui alla lettera a) e della fattura o della ricevuta o dello scontrino fiscale emesso.

5 MISURE DI PREVENZIONE DEL TERRORISMO

Il contrasto del finanziamento al terrorismo rappresenta un adempimento che reca alcune peculiari problematiche legate soprattutto all'intercettazione delle operazioni che possono sottendere al fenomeno.

Un aspetto da sottolineare è che, a differenza delle fattispecie di riciclaggio, nel contesto del finanziamento al terrorismo la fonte del denaro impiegato allo scopo non è necessariamente illecita, ma può anche essere lecita. Da un punto di vista oggettivo sarà perciò necessario per l'operatore fare attenzione agli specifici indicatori di anomalia emanati da UIF sul tema[16].

Da un punto di vista soggettivo, è necessario che l'operatore compia verifiche sui soggetti coinvolti nella movimentazione; a tal fine, il Gruppo dispone di sistemi per intercettare un soggetto designato Terrorista, tramite il riscontro di abbinamenti di singoli soggetti con le *black list* del terrorismo in *World-Check* (attraverso il riscontro dei nominativi sulla procedura *FastCheck*- "Liste negative"), da effettuare non solo per il cliente, ma anche qualora si nutra sospetto circa le controparti delle operazioni. In presenza di un sospetto di operatività collegata al fenomeno, sarà fondamentale un'acquisizione di informazioni approfondite e aggiornate sul profilo del cliente, verificando anche

---

1.1.1.1 [14] D. L. 2 marzo 2012, n. 16 - "Disposizioni urgenti in materia di semplificazioni tributarie, di efficientamento e potenziamento delle procedure di accertamento" (convertito con modificazioni dalla L. 26 aprile 2012, n. 44 (in SO n. 85, relativo alla G.U. 28/04/2012, n. 99 Provvedimento pubblicato sulla G.U. n.52 del 2-3-2012 è entrato in vigore lo stesso giorno).

[15] La certificazione deve essere fatta ai sensi dell'articolo 47 del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445. L'art. 47 del DPR 445/2000 - Dichiarazioni sostitutive dell'atto di notorietà, al comma 1 prevede che: "L'atto di notorietà concernente stati, qualità personali o fatti che siano a diretta conoscenza dell'interessato è sostituito da dichiarazione resa e sottoscritta dal medesimo con la osservanza delle modalità di cui all'articolo 38" (il quale prevede, al comma 3 che: "Le istanze e le dichiarazioni sostitutive di atto di notorietà da produrre agli organi della amministrazione pubblica o ai gestori o esercenti di pubblici servizi sono sottoscritte dall'interessato in presenza del dipendente addetto ovvero sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore. La copia fotostatica del documento è inserita nel fascicolo …").

[16] Parimenti sono stati elaborati indicatori di anomalia concernenti il fenomeno della proliferazione di armi di distruzione di massa, circa le attività legate all'ideazione e realizzazione di programmi volti a sviluppare strumenti bellici di natura nucleare, chimica o batteriologica, ulteriore minaccia per la sicurezza internazionale.

l'eventuale sottoposizione dello stesso a procedimenti penali per reati in materia di terrorismo, valutando anche l'eventuale presenza di notizie di stampa negativa, anche in capo ad altri soggetti eventualmente coinvolti.

Nei casi di appartenenza alle *black list* del terrorismo o di sospetto di operatività volta al finanziamento del terrorismo l'operatore dovrà procedere ad effettuare una segnalazione di operazione sospetta **con la massima tempestività**; la Funzione *Compliance* e Antiriciclaggio oltre a valutare l'inoltro alla UIF della segnalazione, dovrà porre in essere le misure previste per il congelamento dei fondi e/o delle risorse economiche in collaborazione con la Struttura operativa interessata.

I fondi e le risorse economiche sottoposti a congelamento non possono essere oggetto di alcun atto di trasferimento, disposizione o utilizzo; la custodia, l'amministrazione e la gestione delle risorse economiche in attesa di accertamento compete all'Agenzia del Demanio.

La Funzione *Compliance* e Antiriciclaggio comunica tempestivamente a tutte le Strutture operative di non dar più seguito ad alcuna operazione o aprire nuovi rapporti continuativi che riguardano i soggetti interessati dalle misure di congelamento e trasmette al Responsabile SOS le informazioni necessarie alla segnalazione alla UIF.

Le Società del Gruppo, attraverso la Funzione *Compliance* e Antiriciclaggio, devono adempiere ai seguenti obblighi di comunicazione: comunicare alla UIF, entro trenta giorni dall'entrata in vigore dei regolamenti comunitari, delle decisioni degli organismi internazionali e dell'Unione Europea ai sensi dell'art. 4 – ter del d.lgs. 109/2007 e dei decreti di cui ai citati articoli 4 e 4 – bis, le misure di congelamento di fondi e risorse economiche applicate, indicando i soggetti coinvolti nonché l'entità e la natura dei fondi e delle risorse economiche congelate e comunicare alla UIF le operazioni, i rapporti, nonché ogni altra informazione disponibile riconducibile ai soggetti designati nonché a quelli in via di designazione anche sulla base delle indicazioni fornite dal Comitato di Sicurezza Finanziaria.

Limitatamente alle misure aventi ad oggetto risorse economiche, le comunicazioni in questione sono effettuate anche al Nucleo speciale di polizia valutaria della Guardia di Finanza.

6 PROFILATURA DELLA CLIENTELA

Ai sensi dell'art.15 comma 2 del D. Lgs. 231/2007 e delle Disposizioni in materia di adeguata verifica[17], il Gruppo utilizza una procedura informatica per l'elaborazione del profilo di rischio riciclaggio di ogni cliente, individuata in G.I.An.O.S. della società OASI.

G.I.An.O.S. attribuisce a ciascun cliente, un profilo di rischio che identifica un corrispondente rischio di riciclaggio e di finanziamento del terrorismo: il calcolo del profilo è attivato in fase di acquisizione del flusso contenente i dati di adeguata verifica, ogni qualvolta venga aperto un nuovo rapporto o lo stesso venga aggiornato; è altresì prevista, per tutta la base clienti, una revisione mensile del profilo di rischio.

Il modello di profilatura prevede le seguenti quattro fasce di rischio, come definite in dettaglio nella Policy Antiriciclaggio, che tengono conto delle caratteristiche soggettive e oggettive dei soggetti:

A. Irrilevante (fino a 5 punti)
B. Bassa (da 6 a 12 punti)
C. Media (da 13 a 24 punti)
D. Alta (da 25 a 99 punti)

La fascia di rischio assegnata al cliente determina la frequenza dei controlli e l'estensione della verifica da effettuare; in particolare: ad un profilo di rischio Irrilevante, Basso e Medio, corrispondono misure ordinarie di adeguata verifica (eventualmente graduate); ad un profilo di rischio Alto, corrispondono misure rafforzate di adeguata verifica.

Per i soggetti collocati in fascia di rischio Media o Alta, al momento dell'acquisizione di un questionario di adeguata verifica viene innescato un workflow valutativo che determina la creazione, all'interno del modulo G.I.An.O.S. "Know

[17] Disposizioni in materia di adeguata verifica della clientela della Banca d'Italia, Parte I, Sezione III.

Your Customer", di una pratica mediante la quale deve essere inserita una valutazione di coerenza (o meno) circa la complessiva operatività posta in essere dal cliente con il nostro istituto.

- La *Compliance* e Antiriciclaggio è coinvolta nel processo valutativo (cosiddetto "workflow autorizzativo") per i clienti collocati in fascia Alta di rischio di riciclaggio. In tale caso, il Responsabile della dipendenza che deve acquisire il questionario di adeguata verifica formalizza la propria valutazione sul cliente, trasmettendola a mezzo e-mail alla *Compliance* e Antiriciclaggio che esprime le proprie considerazioni, approvando la pratica o richiedendo al Responsabile ulteriori approfondimenti. Per i soggetti collocati in fascia Media di rischio di riciclaggio, il Responsabile della Filiale valuta in autonomia la posizione in esame.

Secondo quanto previsto nella Sezione III delle Disposizioni in materia di adeguata verifica *"Per i destinatari appartenenti ad un gruppo, quando la profilatura del cliente non è accentrata, essa viene effettuata dalle singole società anche sulla base delle informazioni utilizzate dalle altre società del gruppo. Ciascuna società assume, per uno stesso cliente, il profilo di rischio più elevato tra quelli assegnati da tutte le società del gruppo".*

L'allineamento del profilo di rischio di clienti condivisi da diverse Società del gruppo, prima che ciò avvenga automaticamente con il funzionamento a pieno regime di un automatismo previsto dai sistemi Cedacri, deve essere effettuato manualmente attraverso un intervento della Funzione *Compliance* e Antiriciclaggio.

7 AUTOVALUTAZIONE DEL RISCHIO DI RICICLAGGIO

La Funzione *Compliance* e Antiriciclaggio ha il compito di valutare con cadenza almeno annuale, mediante attività di *risk assessment* (cd. esercizio di autovalutazione), l'idoneità del complessivo impianto organizzativo ed operativo del Gruppo ai fini della mitigazione del rischio di riciclaggio e finanziamento del terrorismo. La metodologia per l'effettuazione dell'esercizio di autovalutazione è descritta analiticamente nel Documento di Autovalutazione Annuale consultabile presso la funzione.

All'esito di tale esercizio, la Funzione sottopone detti esiti, unitamente agli interventi correttivi individuati a rischio di riciclaggio, al Consiglio di Amministrazione, all'Amministratore Delegato ed al Collegio sindacale per gli adempimenti di propria competenza.

Gli esiti dell'autovalutazione sono trasmessi a Banca d'Italia, unitamente alla Relazione annuale della Funzione, entro il 30 aprile dell'anno successivo rispetto a quello oggetto di valutazione.

8 OBBLIGHI DI CONSERVAZIONE E SEGNALETICI

Secondo quanto previsto dall'articolo 31 del Decreto antiriciclaggio le Società del Gruppo hanno l'obbligo, di:

a) conservare i documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo e a consentire lo svolgimento delle analisi effettuate, nell'ambito delle rispettive attribuzioni, dall'UIF o da altra Autorità competente (art. 31 D.Lgs. 231/2007);
b) prevedere le modalità con le quali i documenti, i dati e le informazioni devono essere conservati al fine, tra l'altro, di consentirne l'accessibilità completa e tempestiva da parte delle Autorità competenti (art. 32 D.Lgs. 231/2007 e s.mi.).

Gli obblighi sussistono:

- in sede di accensione, variazione e chiusura di conti, depositi e altri rapporti continuativi;
- per ogni operazione che comporti la trasmissione o la movimentazione di mezzi di pagamento o il trasferimento tra soggetti diversi di contante o titoli al portatore di importo (in euro o valuta estera) pari o superiore a €.15.000,00, indipendentemente dal fatto che si tratti di un'operazione unica o di più operazioni che appaiono tra loro collegate per realizzare un'operazione frazionata.

Al comma 3 dell'art. 31 del Decreto antiriciclaggio è previsto che *"i documenti, i dati e le informazioni acquisiti sono conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale".*

Il provvedimento della Banca d'Italia del 24/03/2020 ha rinnovato la materia e prevede due ordini di adempimenti:

a) obblighi di **conservazione**: riguardante documenti, dati e informazioni da conservarsi ai sensi del Decreto Antiriciclaggio, indipendentemente dalle soglie;
b) obblighi di **messa a disposizione:** riguardante anch'esso documenti, dati e informazioni, ma nei limiti e nelle forme standardizzate indicati negli allegati dello stesso Provvedimento.

8.1 Messa a disposizione dei dati

Le Società del Gruppo sono destinatarie degli obblighi di cui alle «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» emanate da Banca d'Italia in data 24 marzo 2020.

Per quanto riguarda lo strumento di conservazione e messa disposizione dei dati è stato scelto di continuare ad utilizzare dal 1° gennaio 2021 il sistema degli "archivi standardizzati" ex AUI, con le seguenti principali novità:

- abbassamento da 15.000 a 5.000 euro della soglia per le registrazioni nell'archivio standardizzato;
- eliminazione dell'analisi frazionamenti;
- eliminazione dei soggetti "a verifica semplificata" e adozione dell'approccio basato sul rischio;
- obbligatorietà del titolare effettivo su tutti i rapporti intestati a persone giuridiche;
- obbligatorietà dell'esecutore;
- per quanto riguarda pe le operazioni eseguite sulla base di ordini di pagamento o di accreditamento, va indicato rispettivamente il numero di rapporto del beneficiario o dell'ordinante o l'IBAN .

I sistemi informatizzati utilizzati tramite gli applicativi Cedacri garantiscono i requisiti di accessibilità completa e tempestiva, integrità, non alterabilità e storicità di documenti, dati e informazioni oggetto dell'obbligo.

Si riportano di seguito i dati da rendere disponibili alle autorità a norma dell'art. 5 delle citate Disposizioni di Banca d'Italia:

- <u>Con riferimento ai rapporti continuativi</u>:
  - i documenti acquisiti in occasione dell'adeguata verifica del cliente, dell'esecutore e del titolare effettivo;
  - il punto operativo di instaurazione del rapporto, la data di instaurazione e la data di chiusura del rapporto;
  - il numero del rapporto e il settore di attività economica (e eventuali variazioni).
- <u>Con riferimento alle operazioni di importo ≥ Euro 5.000:</u>
  - i documenti acquisiti in occasione dell'adeguata verifica del cliente, dell'esecutore e del titolare effettivo;
  - la data di effettuazione;
  - l'importo;
  - il segno monetario;
  - la causale dell'operazione;
  - il mezzo di pagamento utilizzato;
  - la causale analitica che codifica la tipologia dell'operazione;
  - l'importo espresso in euro, con l'indicazione della valuta utilizzata e l'evidenza della parte eseguita in contanti;
  - la codifica interna, il Comune e il CAB del punto operativo dell'intermediario presso il quale è stata disposta l'operazione;
  - il numero dell'eventuale rapporto continuativo e il settore di attività economica del cliente intestatario dell'eventuale rapporto.
- Per le operazioni di accreditamento/addebito, sono previsti specifici dati e informazioni da rendere disponibili alle autorità.

Circa gli obblighi di messa a disposizione previsti dall'art. 6 delle citate Disposizioni, le Società del Gruppo, in allineamento a quanto previsto dalla Policy Antiriciclaggio di Gruppo, adottano quale modalità di messa a disposizione, la prosecuzione della tenuta del sistema standardizzato ex Archivio Unico Informatico.

8.2 Registrazione di rapporti in archivio standardizzato

Nelle ipotesi di accensione, variazione ed estinzione dei rapporti le registrazioni di dati e informazioni sono effettuate in automatico dalla procedura informatica il giorno successivo all'operazione.

8.3 Registrazione di operazioni in archivio standardizzato

Le operazioni sono inserite direttamente negli Archivi Standardizzati (ex transitori Pre – AUI) tramite l'applicativo "3270", utilizzato anche dalla Funzione *Compliance* e Antiriciclaggio al fine di effettuare il monitoraggio delle operazioni che presentino anomalie e la loro sistemazione.

Sugli Archivi Transitori (Pre – A.U.I.) le operazioni sono registrate utilizzando il medesimo formato ministeriale previsto per l'Archivio Definitivo (A.U.I.) agevolando la verifica della correttezza (o meno) del corredo informativo (attributi) contenuto nelle registrazioni transitorie, prima della loro scrittura nell'A.U.I.; è possibile inserire registrazioni direttamente in Pre – A.U.I., senza dover ricorrere al data entry di sportello (in caso di omessa registrazione di una transazione) ed anche modificare i soggetti (ordinante, esecutore, titolare effettivo) collegati alla registrazione.

Nell'ambito delle verifiche della Funzione *Compliance* e Antiriciclaggio è compreso il monitoraggio e la sistemazione di eventuali operazioni che presentino anomalie effettive o potenziali. Tali registrazioni vengono evidenziate come "incomplete" nella procedura "Gestione nuovi transitori (Pre-A.U.I.)" presente nell'applicativo "3270" e possono essere riconducibili ad incompletezza/incongruenza nella registrazione o nell'anagrafica dei soggetti coinvolti. La funzione *Compliance* e Antiriciclaggio analizza il "codice errore" evidenziato dalla procedura ed in esito all'attività di analisi provvede a:

a. rettificare, ove necessario, gli elementi della registrazione incompleti e/o incongruenti;
b. forzare la registrazione in A.U.I. nel caso in cui l'anomalia evidenziata non rappresenti un errore ma sia riconducibile a scelte aziendali conformi alla normativa di riferimento;
c. annullare la registrazione ove la stessa risulti non dovuta e sia stata determinata da un errore operativo degli addetti.

La registrazione nell'Archivio definitivo (A.U.I.) avviene dopo il 21° giorno dal compimento dell'operazione. Tutti gli operatori di Filiale devono porre la massima attenzione nell'attribuzione delle esatte causali alle operazioni richieste dalla clientela, in quanto:

- sussiste un obbligo di esatta registrazione, ovvero di reale rappresentazione della movimentazione posta in essere;
- causali inidonee determinano la composizione di flussi informativi da rimettere periodicamente all'UIF inesatti.

In particolare, è necessario tenere presente che:

- non devono essere effettuate compensazioni tra operazioni di segno contrario poste in essere dallo stesso soggetto; quindi, con un solo atto possono essere effettuate anche più di una operazione, da annotare separatamente sull'archivio standardizzato in quanto di segno opposto (ad esempio, versamento di assegni e prelevamento di contanti con proprio assegno, entrambi d'ammontare pari o superiore a 5.000,00 euro);
- si ha una **"effettiva movimentazione"** anche nell'ipotesi di rinnovo titoli al portatore o nominativi (ad esempio, certificati di deposito, obbligazioni) per cassa, dovendo esso essere ricostruito come un incasso del vecchio titolo ed una sottoscrizione o un acquisto del nuovo titolo per contanti; gli interessi pagati in sede di rinnovo devono essere sommati all'ammontare dei titoli;
- si precisa che, per operazioni in **"contante reale"** si intendono esclusivamente quelle che riflettono una movimentazione fisica di banconote;
- per **"ordini di accreditamento o di pagamento"** si intendono le operazioni di "moneta scritturale" effettuate su conti correnti, che rappresentino un trasferimento di flussi finanziari tra soggetti diversi, ivi compresi quelli fra la banca e la clientela;
- devono essere registrati anche i trasferimenti di denaro contante o di titoli al portatore tra soggetti diversi in cui l'intermediario abbia agito da tramite e la consegna o il ritiro di titoli al portatore allo sportello.

8.4 Segnalazioni Antiriciclaggio aggregate (Flussi S.Ar.A.")

All'art. 33 del Decreto Antiriciclaggio è sancito l'obbligo di inoltrare mensilmente alla UIF *"dati aggregati concernenti la propria operatività, al fine di consentire l'effettuazione di analisi mirate a far emergere eventuali fenomeni di riciclaggio o di finanziamento del terrorismo nell'ambito di determinate zone territoriali"*. La trasmissione di tali comunicazioni avviene entro il ventesimo giorno del secondo mese successivo a quello di riferimento. La UIF individua le tipologie di dati e definisce le modalità di aggregazione e trasmissione. La stessa UIF verifica il rispetto dell'obbligo d'invio dei dati aggregati anche mediante accesso diretto all'archivio unico informatico.

Le operazioni da considerare sono quelle di importo pari o superiore ad Euro 5.000 (cfr. Disposizioni emanate dalla Banca d'Italia in data 25/08/2020, in vigore dal 01/01/2021).

Prima di essere inoltrati i dati devono essere aggregati secondo modalità che distinguono le operazioni per: causali sintetiche, con le quali vengono raggruppate varie tipologie di operazioni, CAB comune in cui le operazioni sono state poste in essere, tipo di valuta utilizzata, settorizzazione economica.

Per ogni aggregazione deve essere indicato l'importo totale e il numero delle operazioni, evidenziando, se presenti, le parti eseguite in contanti.

La trasmissione alla UIF dei dati aggregati concernenti l'operatività complessiva delle società del Gruppo è curata dalla Funzione *Compliance* e Antiriciclaggio ed avviene mensilmente, entro il secondo giorno del terzo mese successivo a quello di riferimento. L'invio dei dati avviene per via telematica tramite il Portale Infostat-UIF, previa adesione. Nel modulo di Adesione al sistema Infostat-UIF va indicato il Referente S.Ar.A. coincidente col **Responsabile AML**; possono essere abilitati dal Referente S.Ar.A. altri soggetti per le trasmissioni, ma il Referente mantiene la responsabilità e l'obbligo di verificare il corretto funzionamento. Attualmente il Referente ha delegato, per l'invio dei dati del Gruppo Igea, l'outsourcer Cedacri.

La UIF sottopone i dati inviati nelle segnalazioni S.Ar.A ad una serie di **controlli statistici**, tesi ad individuare dati statisticamente anomali e, nel qual caso, a notificarlo al segnalante, il quale deve procedere alle necessarie verifiche e:

- in caso di esito positivo: inviare il sostitutivo della segnalazione errata, seguendo le disposizioni attuative in vigore alla data di riferimento della segnalazione;
- in caso di esito negativo: procedere alla conferma dei dati tramite l'apposita funzione sul Portale Infostat-UIF.

Il termine entro cui fornire il riscontro è stabilito in 60 giorni dal quindicesimo giorno del mese di scadenza del termine di invio della segnalazione.

È cura della Funzione *Compliance* e Antiriciclaggio conservare in apposita cartella la documentazione relativa ai flussi trasmessi a UIF, comprensiva dei messaggi di ritorno che vengono inviati dal sistema del Portale Infostat-UIF.

8.5 Comunicazioni oggettive

L'obbligo di effettuare le c.d. "comunicazioni oggettive" è sancito dall'art. 47 del Decreto Antiriciclaggio attraverso la previsione secondo la quale *"i soggetti obbligati trasmettono alla UIF, con cadenza periodica, dati e informazioni individuati in base a criteri oggettivi, concernenti operazioni a rischio di riciclaggio o di finanziamento del terrorismo."* Gli obblighi di comunicazione sono relativi alle operazioni in contante di importo pari o superiore a 10.000 euro eseguite nel corso del mese solare dal medesimo soggetto, in qualità di cliente o di esecutore, anche se realizzate attraverso più operazioni singolarmente pari o superiori a 1.000 euro [18].

La corretta trasmissione della Comunicazione all'Autorità di Vigilanza da parte delle Società appartenenti al Gruppo è demandata alla Funzione *Compliance* e Antiriciclaggio, ed avviene tramite l'adozione di procedure informatiche messe a disposizione dall'outsourcer informatico di riferimento, oltre che l'utilizzo delle procedure segnaletiche messe a

[18] Cfr., il Provvedimento UIF "Istruzioni in materia di comunicazioni oggettive" del 28 marzo 2019.

disposizione da parte dell'Organo di Vigilanza. Sempre alla Funzione *Compliance* e Antiriciclaggio è demandata l'attuazione di verifiche periodiche sulla correttezza del flusso inoltrato all'UIF.

I dati sono elaborati tramite un applicativo predisposto dall'outsourcer Cedacri (delegato dal Gruppo per l'inoltro dei flussi relativi alle Comunicazioni Oggettive) che produce il file da inoltrare secondo il formato XML richiesto dalla normativa. La Funzione *Compliance* e Antiriciclaggio, esperite le opportune verifiche ed eventuali rettifiche relative a registrazioni evidenziate dalla procedura come "anomale", salva in una cartella numerata (pratica AT) i file (in formato ".csv") relativi alle registrazioni ricomprese nei flussi da inviare alla U.I.F. (uno relativo ai soggetti, uno relativo alle operazioni) e ne richiede l'inoltro mediante un comando della procedura; a seguito di tale richiesta, Cedacri provvede ad inserire nel portale Infostat-UIF, i flussi relativi al mese di osservazione; l'invio del flusso alla U.I.F. deve avvenire entro il 15 del secondo mese successivo al mese di osservazione (ad esempio, il flusso relativo al mese di gennaio deve essere inviato entro il 15 marzo). I dati inerenti alle comunicazioni oggettive sono conservati all'interno del sistema, ed in relazione ad essi si applica il termine generale di conservazione; nondimeno è cura della Funzione *Compliance* e Antiriciclaggio, come sopra indicato, conservare in apposita cartella la documentazione relativa ai flussi trasmessi a UIF, comprensiva dei messaggi di ritorno che vengono inviati dal sistema del Portale Infostat-UIF.

9 SEGNALAZIONE DI OPERAZIONI SOSPETTE (SOS)

L'art. 35 del decreto legislativo 21 novembre 2007, n. 231 impone ai *soggetti obbligati*", prima di compiere l'operazione, di portare a conoscenza della UIF, mediante l'invio di una segnalazione di operazione sospetta, le operazioni per le quali "*sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa*". In tale contesto, il presente capitolo ha l'obiettivo di descrivere i ruoli, le responsabilità e le attività del Gruppo finalizzate ad ottemperare all'obbligo di segnalazione delle operazioni sospette identificate, assicurandone il corretto adempimento, la riservatezza dell'identità del "segnalante", delle informazioni, dei riscontri ed i controlli interni, in conformità agli artt. 38 e seguenti.

Le Funzioni Aziendali coinvolte nel processo di valutazione delle operazioni sospette sono:

- Strutture operative;
- Responsabili di Filiale;
- Referente AML e *Compliance* presso la Controllata;
- Funzione *Compliance* e Antiriciclaggio;
- Responsabile SOS (Delegato Aziendale dell'Antiriciclaggio).

L'input per l'avvio dell'iter di segnalazione di operazioni sospette è demandato a ciascun dipendente nel momento in cui si trovi nella situazione sopra descritta di sapere, sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo.

9.1 Individuazione delle operazioni sospette

Il sospetto di riciclaggio/finanziamento al terrorismo è desunto dalle caratteristiche, dall'entità, dalla natura dell'operazione (ad esempio: interposizione di soggetti terzi; impiego di strumenti societari, associativi o fiduciari suscettibili di limitare la trasparenza della proprietà e della gestione; utilizzo del denaro contante o di strumenti al portatore) o da qualsivoglia altra circostanza conosciuta in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi a disposizione dei segnalanti, acquisiti nell'ambito dell'attività svolta ovvero a seguito del conferimento di un incarico (ad esempio: soggetti insediati in località caratterizzate da regimi fiscali o antiriciclaggio privilegiati; soggetti dei quali è noto il coinvolgimento in attività illecite, mancata coincidenza tra soggetto richiedente l'operazione e persona cui la stessa è riferita).

In tale fase di individuazione delle operazioni sospette, è di ausilio la consultazione degli "indicatori di anomalia" emanati da Banca d'Italia e periodicamente aggiornati, disponibili al seguente link:

https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/index.html?com.dotmarketing.htmlpage.language=102,

nonché i modelli e gli schemi di comportamenti anomali diffusi, tempo per tempo, dall'UIF (link: https://uif.bancaditalia.it/normativa/norm-indicatori-anomalia/index.html).

Le segnalazioni effettuate non costituiscono violazioni di obblighi di segretezza e non comportano responsabilità di alcun tipo, salvi i casi di dolo.

Si precisa che l'obbligo di segnalazione riguarda non solo le operazioni eseguite, ma anche quelle prive di importo, rifiutate o comunque non concluse o solamente tentate e l'obbligo permane per tutta la durata del rapporto, e non solamente nelle fasi di accensione o chiusura. Dovrà essere valutata anche l'operatività con altri intermediari nazionali ed esteri, soprattutto se aventi sede in Paesi non cooperativi.

9.1.1 Contenuto della segnalazione

La segnalazione di un'operazione sospetta deve essere molto dettagliata. Essa deve contenere:

- i consueti dati anagrafici sul soggetto segnalato, con aggiunta di qualsiasi informazione utile al fine di delineare il profilo soggettivo del cliente: ad es. professione del cliente, informazioni patrimoniali/reddituali.
- principali dati sul/i rapporto/i, con riferimento a data di accensione ed eventuale estinzione dello stesso, numero e tipologia di rapporto, deleghe o cointestazioni (comprensivi di legami tra il cliente e i soggetti delegati/cointestatari);
- una descrizione esaustiva dell'operazione, comprensiva di tutte le informazioni su eventuali segnalazioni collegate, genesi dell'operazione, descrizione dell'operatività del cliente e volumi complessivi della stessa;
- dettagli informativi sull'operazione, comprendente tutti i dati (numerazione assegni, conti di traenza, beneficiari ed eventuali legami conosciuti con gli stessi, girate, etc.) relativi alle operazioni di costituzione ed utilizzo dei fondi oggetto del sospetto;
- la descrizione particolareggiata dei motivi del sospetto, con riferimento sia agli elementi oggettivi delle operazioni, sia al profilo del cliente, corredata dalla descrizione di eventuali notizie di stampa negativa rilevate sullo stesso o comunque note al segnalatore in ragione del ruolo svolto o per informazioni negative in qualunque modo apprese. Eventualmente il riferimento ad un indicatore di anomalia qualora l'operazione abbia una configurazione che rientri all'interno di uno degli schemi emanati da Banca d'Italia sul tema;
- esito (ed eventuale documentazione a supporto) di approfondimenti svolti anche mediante interlocuzione con il cliente, circa le motivazioni sottostanti alle operazioni e/o ai comportamenti anomali rilevati, con l'indicazione delle motivazioni (eventualmente) addotte dal cliente.

9.2 Gestione Inattesi

A supporto dell'individuazione di situazioni di anomalia, il Gruppo si avvale del modulo G.I.An.O.S. relativo alla produzione mensile dei movimenti c.d. "Inattesi". Si tratta di estrazioni di operazioni che presentano profili di anomalia in base ad algoritmi concepiti in considerazione degli indicatori di anomalia emanati da Banca d'Italia. Si noti che tale modalità di rilevamento di operazioni potenzialmente sospette rappresenta solo un ausilio per il valutatore e non può in alcun modo sostituirsi alle attività di analisi e valutazione in capo a tutte le figure coinvolte nel processo in parola.

L'estrazione di operazioni qualificate quali "Inattesi" avviene tramite apposito modulo, che svolge funzioni di ausilio alla segnalazione di operazione sospetta, in quanto è finalizzato a selezionare, attraverso regole basate su parametri quantitativi e qualitativi, le operazioni anomale alle quali dedicare maggiori approfondimenti per valutarne il sospetto circa la connessione con operazioni di riciclaggio e di finanziamento al terrorismo.

Pertanto, il modulo, mensilmente, provvede a:

- analizzare le registrazioni antiriciclaggio presenti in archivio standardizzato con data contabile pari a due mesi precedenti a quello in corso (es.: a marzo sono analizzate le operazioni di gennaio);
- identificare i soggetti che nel periodo in questione hanno manifestato oggettive atipicità nell'operatività corrente rispetto alla movimentazione eseguita nei mesi precedenti.

All'interno di tale modulo è possibile, tramite la funzione "Pratiche extra-Gianos", procedere all'inserimento di nominativi, con o senza operazioni collegate, non estratti automaticamente dall'applicativo, ma per i quali si intende

effettuare una segnalazione di operazione sospetta. Il Gruppo attualmente non utilizza tale funzione e pertanto, le segnalazioni di operazioni sospette devono essere inoltrate alla Funzione *Compliance* e Antiriciclaggio secondo quanto indicato al successivo punto 9.4.

La valutazione di tutti gli inattesi deve essere eseguita entro il 10 del mese successivo a quello di elaborazione. Qualora in esito alla valutazione, il Responsabile ritenga di procedere alla segnalazione, dovrà essere osservato l'iter descritto *infra* al paragrafo 9.4.

9.3 Termini della segnalazione di operazione sospetta

Le segnalazioni devono essere effettuate senza ritardo, non appena si viene a conoscenza degli elementi di sospetto e, ove possibile, prima di eseguire l'operazione. Secondo quanto previsto dall'art. 35 co. 2 del Decreto Antiriciclaggio, i soggetti tenuti all'obbligo "*non compiono l'operazione fino al momento in cui non hanno provveduto ad effettuare la segnalazione di operazione sospetta. Sono fatti salvi i casi in cui l'operazione debba essere eseguita in quanto sussiste un obbligo di legge di ricevere l'atto ovvero nei casi in cui l'esecuzione dell'operazione non possa essere rinviata tenuto conto della normale operatività ovvero nei casi in cui il differimento dell'operazione possa ostacolare le indagini*".

L'iter di segnalazione segue il criterio generale di far transitare, senza ritardo, la segnalazione dell'operazione dal Responsabile della Dipendenza, dell'Ufficio, o di altra Unità organizzativa cui compete l'amministrazione e la gestione dei rapporti con la clientela, alla Funzione *Compliance* e Antiriciclaggio per le opportune valutazioni.

9.4 Modalità di segnalazione

Le strutture operative che intrattengono rapporti con la clientela, rappresentano gli organi deputati al primo impulso alla segnalazione di operazione sospetta, perché a diretto contatto con la clientela.

In presenza di operazioni sospette, il membro del personale (addetto o responsabile) che individua un sospetto nell'operatività di un cliente deve compilare il mod. 750/2016 di segnalazione, curandosi di allegare tutta la documentazione riferita all'operazione stessa. Nel caso l'operazione sia valutata da un Addetto, il mod. 750/2016 e la documentazione relativa deve essere consegnata al Responsabile; nel contempo, l'Addetto dovrà comunicare alla *Compliance* e Antiriciclaggio, a mezzo mail, l'avvenuta consegna al proprio Responsabile, della segnalazione, indicandone i dati essenziali. Sarà cura della *Compliance* e Antiriciclaggio monitorare l'iter della segnalazione in parola ed approfondire i motivi dell'archiviazione della stessa da parte del Responsabile, ove questa non pervenga alla *Compliance* e Antiriciclaggio entro un lasso di tempo ragionevole.

Il Responsabile provvede a:

- rilasciare all'addetto segnalante una copia del mod.750/2016 sottoscritta per ricevuta;
- eseguire un esame di congruità fra l'operazione eseguita o tentata (che può consistere anche nell'apertura di un rapporto) ed il profilo economico-finanziario del richiedente;
- valutare se effettuare o meno la segnalazione.

Qualora il Responsabile ritenga di procedere con la Segnalazione provvederà a:

- compilare un ulteriore mod.750/2016;
- redigere una relazione dettagliata sull'operazione sospetta che si sta segnalando, eventualmente corredando la stessa con evidenze documentali.

Qualora il Responsabile ritenga di non procedere con la Segnalazione, provvederà ad annotare il proprio giudizio sul modulo 750/2016 ricevuto dall'addetto che conserva, unitamente alla documentazione, in apposito dossier riservato presso la Filiale.

Le segnalazioni che il Responsabile intende effettuare devono essere trasmesse a mezzo posta elettronica certificata alla Funzione *Compliance* e Antiriciclaggio utilizzando l'indirizzo funzione_antiriciclaggio.bancafucino@postacert.cedacri.it, così come le segnalazioni che pervengano da altri uffici, ad esempio gli Uffici Centrali.

Specificatamente per la Controllata Igea Digital Bank, il controllo sulle operazioni è effettuato dall'operatore del contact center, il quale, in caso valuti di effettuare una segnalazione di operazione sospetta compila il mod. 750/2016 da inoltrarsi al Referente della Funzione *Compliance* e Antiriciclaggio, individuato all'interno della Direzione Generale, che provvederà all'invio della segnalazione alla Funzione *Compliance* e Antiriciclaggio accentrata presso la Capogruppo.

La Funzione *Compliance* e Antiriciclaggio compie un'istruttoria approfondita nel merito della segnalazione pervenuta, che sia in particolare comprensiva delle seguenti verifiche, delle quali dovrà essere conservata traccia in una cartella elettronica opportunamente predisposta ed il cui accesso sia limitato alla sola Funzione ed al Responsabile SOS:

- esame dell'accuratezza e completezza dei dati contenuti nella segnalazione di primo livello;
- ricerca, analisi e salvataggio delle schede anagrafiche relative al cliente oggetto di segnalazione, nonché dei soggetti ad esso collegati e di eventuali altri clienti coinvolti nell'operatività oggetto di segnalazione (es. controparti);
- acquisizione tramite l'applicativo G.I.AN.O.S. del profilo di rischio ("punteggio calcolato") del segnalato e dei collegati;
- qualora il soggetto sia a rischio "alto" per precedenti SOS, ricerca negli archivi interni della precedente segnalazione, analisi della stessa e valutazione del collegamento con la segnalazione in esame (attività da svolgere in merito anche alle eventuali ulteriori SOS precedenti, se più di una);
- estrazione di report sui soggetti segnalati e collegati (es. Cribis), rilievo di eventuali eventi pregiudizievoli e confronto con i dati presenti in archivi interni;
- verifica della presenza dei nominativi coinvolti nella segnalazione in banche dati (es. WorldCheck), nonché di notizie su provider esterni al fine di rilevare eventuali notizie di stampa negativa (es. ricerca Google), e conservazione delle evidenze, anche in caso di esito negativo;
- analisi dell'intera operatività dei rapporti collegati al segnalato ai fini di rilevare eventuali ulteriori anomalie da inserire nella segnalazione, con conseguente salvataggio di estratti conto o movimentazione sui rapporti in altro formato, con riferimento almeno agli ultimi 12 mesi.

La Funzione *Compliance* e Antiriciclaggio, sulla base della documentazione ricevuta ed esperiti gli approfondimenti ritenuti opportuni, effettua una propria valutazione in merito alla fondatezza della segnalazione e provvede ad inoltrare la stessa al Responsabile SOS per la valutazione finale e l'eventuale inoltro all'UIF.

L'esito della suddetta valutazione finale sarà comunicato all'Unità segnalante con un flusso di ritorno a mezzo mail al Responsabile della Dipendenza. Sarà compito della Funzione *Compliance* e Antiriciclaggio anche, in caso la SOS sia inoltrata alla UIF, alimentare il report delle Segnalazioni di Operazioni Sospette, effettuare le necessarie operazioni per garantire che il soggetto segnalato ed eventuali collegati coinvolti nell'operatività sospetta siano portati ad una fascia di rischio "alta". Infine, qualora la segnalazione di operazione sospetta abbia trovato origine in una pratica di "Inatteso" G.I.An.O.S., la Funzione *Compliance* e Antiriciclaggio provvederà a variarne opportunamente lo stato (05 – Inoltrata, 06 - Non inoltrata).

9.4.1 Segnalazioni urgenti

Qualora le caratteristiche di un'operazione ancora da compiere siano tali da far insorgere nell'operatore sospetti circa la natura della stessa, si dovrà sospenderne l'esecuzione e dovrà essere informata immediatamente la Funzione *Compliance* e Antiriciclaggio delle caratteristiche della stessa.

La Funzione *Compliance* e Antiriciclaggio ed il Responsabile SOS valuteranno la necessità di una segnalazione alla UIF, che anche su richiesta della DIA e del Nucleo Speciale di Polizia Valutaria della Guardia di Finanza, può sospendere l'operazione per un massimo di cinque giorni lavorativi.

La filiale dovrà nel frattempo astenersi dal compiere l'operazione, tranne che detta astensione non sia possibile, tenuto conto della normale operatività, o possa ostacolare le indagini.

9.4.2 Compiti del Responsabile SOS

Il Responsabile SOS è un soggetto in possesso di adeguati requisiti di indipendenza, autorevolezza e professionalità e svolge la propria attività con autonomia di giudizio e nel rispetto degli obblighi di riservatezza previsti dalla normativa di settore vigente, anche nei confronti degli esponenti e delle altre funzioni aziendali.

Il Responsabile SOS è persona specificatamente deputata alla segnalazione di operazioni sospette (e alle attività inerenti e conseguenti) con specifico incarico conferito con delibera dell'Organo con funzione di gestione e di supervisione strategica (competente anche per la revoca). L'attribuzione dell'incarico deve essere resa nota all'interno del Gruppo e presso l'intera rete distributiva e comunicato alla UIF con le modalità dalla medesima Autorità indicate.

Il Responsabile SOS non può detenere responsabilità dirette in aree operative né è gerarchicamente dipendente da soggetti appartenenti a queste aree.

Il Responsabile SOS deve effettuare la valutazione delle operazioni sospette di riciclaggio inserite in procedura ed inoltrate dai responsabili di unità operative decentrate (filiali e uffici) del Gruppo. Al Responsabile SOS è affidato anche il compito di trasmettere le segnalazioni, qualora le ritenga fondate, alla UIF tramite l'apposito portale "Infostat", esplicitando un grado di rischio della SOS (basso-medio basso-medio-medio alto-alto).

La segnalazione si compone di diverse parti:

- Descrizione dell'operatività sospetta: in questa parte dovrà essere riportata la descrizione circa l'operatività ritenuta sospetta sotto forma di descrizione testuale (in questa parte andranno riportate le informazioni di cui ai primi 4 punti del paragrafo *supra* 9.1.1);
- Motivo del sospetto: in questa parte, sempre di carattere descrittivo, dovranno essere enunciate chiaramente le motivazioni alla base delle quali si ritiene l'operatività sospetta (a titolo esemplificativo: può essere fatto riferimento ad un indicatore di anomalia ricorrente nella fattispecie, oppure alla presenza di indagini di magistratura in capo al soggetto; si veda l'ultimo punto di cui al paragrafo *supra* 9.1.1);
- Parte strutturata: oltre all'inserimento delle parti a carattere descrittivo di cui sopra, il sistema Infostat prevede l'inserimento di dati relativi a:
  - operazione/i: informazioni sulla/e operazione/i oggetto di segnalazione (ad es. tipologia di operazione, data/e, importo, causali, luogo dell'operazione);
  - soggetto/i: informazioni sui soggetti interessati dalle operazioni e relativi ruoli all'interno dell'operatività sospetta (ad es. dati anagrafici, durata della relazione col cliente, presenza di eventi pregiudizievoli);
  - rapporto/i: informazioni sul/i rapporto/i coinvolto/i nell'operazione sospetta (ad es. tipologia di rapporto, numero di rapporto, data di accensione, filiale di radicamento);
  - legami tra le entità inserite: di fondamentale importanza nel sistema Infostat è l'inserimento di appositi e coerenti legami tra le entità sopra descritte, al fine di ricostruire con precisione il quadro completo della segnalazione. Ad esempio, ad un bonifico in uscita dovranno essere collegati il soggetto che l'ha eseguito ed il soggetto controparte dell'operazione (legami operazione-soggetto), allo stesso bonifico dovranno collegarsi il rapporto di partenza dell'operazione ed il rapporto del beneficiario (legami operazione-rapporto), il soggetto che l'ha eseguito dovrà essere collegato al rapporto di partenza ed allo stesso modo la controparte a quello di arrivo (legame soggetto-rapporto).

Per una trattazione nel dettaglio utile al fine dell'inserimento delle segnalazioni di operazioni sospette sul portale Infostat-UIF, si rinvia all'apposito manuale disponibile sul sito di Banca d'Italia al seguente link:

https://uif.bancaditalia.it/adempimenti-operatori/segnalazioni-sos/manuale_sos.pdf

Particolare attenzione deve essere dedicata al fatto che le segnalazioni inoltrate alla UIF devono essere prive del nominativo del segnalante.

Nei casi in cui lo ritenga opportuno il Responsabile SOS può decidere di non dare corso alla segnalazione dell'operazione ritenuta sospetta; in tali casi dovrà essere conservata traccia di tutte le verifiche effettuate e delle motivazioni che hanno indotto a ritenere infondato il sospetto di riciclaggio/finanziamento al terrorismo alla base della segnalazione.

Al Responsabile SOS è demandata la tenuta di un Registro delle Segnalazioni di Operazioni Sospette il cui aggiornamento deve avvenire nel rispetto dei principi della riservatezza con riguardo ai soggetti che hanno avviato l'iter di segnalazione di operazione sospetta. All'interno del suddetto Registro sono contenute le informazioni essenziali relative alle segnalazioni stesse (di particolare importanza risulta la corretta e completa tenuta delle informazioni relative alla data dell'invio a UIF della segnalazione, al numero di protocollo UIF assegnato alla SOS, al ndg del cliente segnalato, ad una sintetica descrizione dell'operatività anomala. La tutela della riservatezza dell'identità del segnalante è sancita dall'art. 38 del Decreto Antiriciclaggio, al cui comma 1 si legge che *"I soggetti obbligati e gli organismi di autoregolamentazione adottano tutte le misure idonee ad assicurare la riservatezza dell'identità delle persone che effettuano la segnalazione".* I documenti, che contengono le generalità di tali soggetti, sono conservati e custoditi dal titolare dell'attività o legale rappresentante o loro delegato, o comunque sono sotto la loro diretta responsabilità.

È possibile che la UIF (anche attraverso messaggi disponibili nella sezione "scambi di informazioni" sul Portale Infostat-UIF), la Guardia di Finanza e la DIA richiedano ulteriori informazioni ai soggetti segnalanti, per il tramite dell'intermediario per fini di analisi e approfondimento investigativo della segnalazione, ed in casi simili garanzia alla riservatezza è data dal fatto che la trasmissione delle segnalazioni di operazioni sospette, le eventuali richieste di approfondimenti, gli scambi di informazioni tra UIF, Guardia di Finanza, DIA, Autorità di Vigilanza e ordini professionali, debbano avvenire per via telematica, con modalità atte ad assicurare la trasmissione dei dati ai soli soggetti interessati e l'integrità delle informazioni trasmesse. L'identità della persona fisica segnalante potrà essere resa nota in via residuale solamente con un provvedimento motivato dell'Autorità Giudiziaria, qualora sia ritenuto indispensabile ai fini dell'accertamento giudiziario.

È fatto inoltre divieto ai soggetti tenuti alla segnalazione *"di dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione, dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza ovvero della probabilità di indagini o approfondimenti in materia di riciclaggio o di finanziamento del terrorismo"* (art. 39 D. lgs. 231/07).

È previsto inoltre dall'art. 41 del Decreto Antiriciclaggio un flusso di ritorno sulle segnalazioni di operazioni sospette inoltrate, e cioè l'obbligo da parte della UIF di fornire un riscontro informativo sulle utilità delle singole segnalazioni e sull'esito delle stesse (compresa l'eventuale avvenuta archiviazione della stessa), considerando anche gli approfondimenti del caso che possono essere stati effettuati dagli organi investigativi.

Anche con riguardo ad un simile flusso di informazioni vige il divieto di comunicazione ai clienti o terzi.

La Capogruppo assicura, sulla base della complessiva struttura organizzativa e dei controlli adottata nell'ambito del Gruppo, che le società controllate consentano al Responsabile SOS l'accesso alle informazioni attinenti alle segnalazioni trasmesse e a quelle ritenute infondate, corredate della motivazione della decisione. Ai sensi dell'articolo 38 del Decreto Antiriciclaggio, tale accesso avviene con modalità volte a garantire la riservatezza dell'identità dei soggetti che partecipano alla procedura di segnalazione.

Il Responsabile SOS può acquisire informazioni dalle Società appartenenti al medesimo Gruppo e fornire, a sua volta, ai Referenti Antiriciclaggio individuati presso le altre entità eventuali informazioni rilevanti e di reciproca competenza ed interesse.

In ottemperanza a quanto previsto dal comma 5 dell'art 39 del Decreto Antiriciclaggio non è impedita la condivisione di informazioni relative alle segnalazioni di operazioni sospette tra intermediari bancari e finanziari nel caso relativi allo stesso cliente ed alla stessa operazione, a condizione che detti intermediari appartengano ad uno Stato membro o siano situati in un Paese terzo che impone obblighi equivalenti a quelli previsti dal Decreto Antiriciclaggio.

La comunicazione, in tal caso, avviene tramite il servizio di posta elettronica certificata in uso alla Funzione Compliance e Antiriciclaggio (funzione_antiriciclaggio.bancafucino@postacert.cedacri.it) avendo cura della riservatezza dei dati oggetto di trasmissione. Le informazioni scambiate possono essere utilizzate esclusivamente ai fini di prevenzione del riciclaggio o del finanziamento del terrorismo.

Il Responsabile SOS è obbligato alla corretta conservazione della documentazione relativa alle segnalazioni di operazioni sospette (comprensiva di eventuali richieste di informazioni in merito provenienti da UIF o dalle Autorità). In particolare,

sarà mantenuta in appositi armadi provvisti delle misure necessarie a limitarne l'accesso e la sicurezza, copia cartacea dei mod. 750/2016, delle segnalazioni inoltrate e dei messaggi inviati dal Portale Infostat-UIF in merito a diagnostico e consegna.

La documentazione relativa alla fase istruttoria della segnalazione sarà conservata in apposito fascicolo elettronico all'interno di una directory il cui accesso è limitato alla sola Funzione Antiriciclaggio.

10 FORMAZIONE

L'art. 16, co. 3 del decreto antiriciclaggio disciplina l'obbligo di formazione per il personale come segue:

"I *soggetti obbligati adottano misure proporzionate ai propri rischi, alla propria natura e alle proprie dimensioni, idonee a rendere note al proprio personale gli obblighi cui sono tenuti ai sensi del presente decreto, ivi compresi quelli in materia di protezione dei dati personali. A tal fine, i soggetti obbligati garantiscono lo svolgimento di programmi permanenti di formazione, finalizzati alla corretta applicazione delle disposizioni di cui al presente decreto, al riconoscimento di operazioni connesse al riciclaggio o al finanziamento del terrorismo e all'adozione dei comportamenti e delle procedure da adottare.*"

La formazione si rende perciò necessaria al fine di mantenere l'efficienza dei presidi e una piena consapevolezza della normativa antiriciclaggio, avuto particolare riguardo ai principi che la ispirano, nonché agli obblighi e alle responsabilità gravanti su tutti gli Operatori.

La Capogruppo adotta e realizza programmi di addestramento e di formazione del personale - avendo cura di farli recepire, nell'esercizio del proprio potere di indirizzo e coordinamento, alle Società Controllate - aventi ad oggetto gli obblighi previsti dalla normativa antiriciclaggio e finalizzati ad assicurare una specifica preparazione a tutti i dipendenti.

L'attività di formazione è svolta anche con l'ausilio di esponenti del mondo accademico, della magistratura e delle autorità investigative.

Con precipuo riferimento al personale più a diretto contatto con la clientela e di quello impiegato presso la Funzione *Compliance* e Antiriciclaggio, è necessario che sia pianificata una formazione specifica e continua garantendo l'aggiornamento sull'evoluzione dell'intero comparto normativo e regolamentare del settore.

La strutturazione di adeguati piani di formazione può avvenire sulla base di:

- una valutazione delle esigenze derivanti dall'entrata in vigore di specifiche novità legislative atte ad incidere sul comparto di riferimento;
- eventuali carenze riscontrate nel corso delle verifiche condotte dalla Funzioni di Controllo partitamente competenti.

L'attività di addestramento e formazione del personale è svolta quindi con continuità e sistematicità, nell'ambito di programmi organici. Annualmente viene sottoposta all'approvazione del Consiglio di Amministrazione una relazione in ordine alle attività di addestramento e formazione organizzate.

La Funzione *Compliance* e Antiriciclaggio supporta le Funzioni Aziendali competenti in materia di formazione del personale nella predisposizione di un adeguato piano di addestramento. Essa monitora l'effettiva esecuzione e partecipazione ai corsi programmati, evidenziando nelle relazioni destinate al Consiglio di Amministrazione, gli esiti delle attività poste in essere, ovvero eventuali scostamenti dalla programmazione o anomalie relative alla non partecipazione, individuando gli opportuni interventi correttivi da porre in essere.