LINEE GUIDA DI CONFORMITÀ IN MATERIA DI ANTIRICICLAGGIO E CONTRASTO AL FINANZIAMENTO DEL TERRORISMO

INTRODUZIONE

Lo scopo delle presenti Linee Guida per le misure di Antiriciclaggio (AML), Lotta al Finanziamento del Terrorismo (CFT) e Sanzioni è quello di garantire che **UAB Criptomy** (Azienda) disponga di linee guida interne per prevenire l'uso della propria attività per il Riciclaggio di Denaro e il Finanziamento del Terrorismo e di linee guida interne per l'attuazione delle sanzioni internazionali.

Le presenti Linee guida sono state adottate per garantire la conformità della Società alle norme e ai regolamenti stabiliti dalla Legge della Repubblica di Lituania sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo (Legge) e da altre leggi applicabili, tra cui le seguenti:

- Requisiti tecnici per il processo di identificazione del cliente per l'autenticazione dell'identificazione a distanza tramite dispositivi elettronici per la trasmissione diretta di video approvati dal Direttore del Servizio di investigazione sulla criminalità finanziaria sotto il Ministero degli Affari Interni della Repubblica di Lituania il 30 novembre 2016 con la Risoluzione n. V-314 "Per i requisiti tecnici del processo di identificazione del cliente per l'autenticazione dell'identificazione a distanza tramite dispositivi elettronici per la trasmissione diretta di video" (di seguito - Requisiti tecnici).[1]

- Risoluzione n. V-240 del 5 dicembre 2014 del Direttore del Servizio di investigazione sul crimine finanziario sotto il Ministero degli Affari Interni della Repubblica di Lituania "Sull'approvazione dell'elenco dei criteri per il riciclaggio di denaro e l'identificazione di operazioni o transazioni monetarie sospette o insolite".[2]

- Risoluzione n. V-5 del 10 gennaio 2020 del Direttore del Servizio di investigazione sul crimine finanziario sotto il Ministero degli Affari Interni della Repubblica di Lituania "Sull'approvazione delle linee guida per gli operatori di portafogli di valuta virtuale e gli operatori di cambio di valuta virtuale per prevenire il riciclaggio di denaro e/o il finanziamento del terrorismo".[3]

- Risoluzione n. V-273 del 20 ottobre 2016 del Direttore del Servizio di investigazione sui crimini finanziari sotto il Ministero degli Affari Interni della Repubblica di Lituania "Sull'approvazione delle linee guida per la supervisione dei crimini finanziari per l'attuazione delle sanzioni finanziarie internazionali nel campo dei regolamenti del Ministero degli Affari Interni della Repubblica di Lituania".[4]

- il Ministro dell'Interno della Repubblica di Lituania 2017 16 ottobre con ordinanza n. 1V-701 "Sulla sospensione di transazioni o operazioni monetarie sospette e sulla presentazione di informazioni su transazioni o operazioni monetarie sospette al Servizio di investigazione sulla criminalità finanziaria ai sensi della descrizione della procedura del Ministero dell'Interno della Repubblica di Lituania e sulle informazioni su transazioni o operazioni in contanti pari o superiori a 15.000 euro o sulla presentazione dell'importo corrispondente in valuta estera".

[1] https://www.e-tar.lt/portal/lt/legalAct/e45f4270b70011e6aae49c0b9525cbbb/asr
[2] https://www.e-tar.lt/portal/lt/legalAct/a664b2107ecd11e4bc68a1493830b8b9
[3] https://www.e-tar.lt/portal/lt/legalAct/570a231035e011ea829bc2bea81c1194
[4] https://www.e-tar.lt/portal/lt/legalAct/01d5d4e0974411e69ad4c8713b612d0f

valuta al Servizio di Investigazione sulla Criminalità Finanziaria in base all'approvazione della descrizione della procedura del Ministero dell'Interno della Repubblica di Lituania".[5]

- Direttore del Servizio di investigazione sui reati finanziari 2015 21 maggio con ordinanza n. V-129 "Sull'approvazione dei moduli informativi, degli schemi di presentazione e delle raccomandazioni per il completamento delle informazioni fornite in conformità ai requisiti della legge sulla prevenzione del riciclaggio di denaro e del finanziamento del terrorismo della Repubblica di Lituania".[6]

Le presenti linee guida sono soggette a revisione da parte del Consiglio di amministrazione almeno una volta all'anno. La proposta di revisione e il riesame delle presenti Linee guida possono essere programmati con maggiore frequenza su decisione del Responsabile della segnalazione del riciclaggio di denaro (MLRO) della Società o del Responsabile del controllo interno.

Le presenti Linee guida sono accettate e approvate con delibera del Consiglio di amministrazione della Società.

DEFINIZIONI

Per **Proprietario Beneficiario** si intende una persona fisica che, sfruttando la propria influenza, effettua una transazione, un atto, un'azione, un'operazione o un passo o esercita in altro modo il controllo su una transazione, un atto, un'azione, un'operazione o un passo o su un'altra persona e nel cui interesse o a beneficio della quale o per conto della quale viene effettuata una transazione o un atto, un'azione, un'operazione o un passo. Nel caso di una persona giuridica, il Proprietario Beneficiario è una persona fisica la cui partecipazione diretta o indiretta, o la somma di tutte le partecipazioni dirette e indirette nella persona giuridica, supera il 25%, comprese le partecipazioni sotto forma di azioni o altre forme al portatore.

Per **rapporto commerciale** si intende un rapporto che si instaura in seguito alla stipula di un contratto a lungo termine da parte della Società nell'ambito di attività economiche o professionali finalizzate alla fornitura di un servizio o alla sua distribuzione in altro modo o che non si basa su un contratto a lungo termine, ma per il quale si può ragionevolmente prevedere una certa durata al momento dell'instaurazione del contatto e durante il quale la Società effettua ripetutamente transazioni distinte nel corso di attività economiche o professionali durante la fornitura di un servizio.

Per **azienda** si intende una persona giuridica con i seguenti dati:

- nome dell'azienda: UAB Criptomy;
- Paese di registrazione: Lituania;
- numero di registrazione: 306127858;
- indirizzo: Vilnius, Eišiškių Sodų 18-oji g. 11;
- email: info@criptomy.exchange, contact@criptomy.exchange

Per **Portafoglio di Valuta Virtuale Custode** si intende l'indirizzo o gli indirizzi di Valuta Virtuale generati con la chiave pubblica[7] per la conservazione e la gestione delle Valute Virtuali affidate alla Società ma che rimangono di sua proprietà.

[5] https://e-tar.lt/portal/lt/legalAct/143ad320b24011e7afdadfc0e4460de4
[6] https://www.e-tar.lt/portal/lt/legalAct/e1f42fa0006d11e588da8908dfa91cac

Per **Portafoglio di Valuta Virtuale Custode** si intende l'indirizzo o gli indirizzi di Valuta Virtuale generati con la chiave pubblica[7] per la conservazione e la gestione delle Valute Virtuali affidate alla Società ma che rimangono di sua proprietà.

Per **Cliente** si intende una persona fisica o giuridica che intrattiene un rapporto commerciale con la Società.

Per dipendente si intende il dipendente della Società e qualsiasi altra persona coinvolta nell'applicazione delle presenti Linee guida nella Società.

Linee guida - il presente documento comprensivo di tutti gli allegati di cui sopra. Le Linee guida comprendono, tra l'altro, la procedura di controllo interno della Società relativa alle Linee guida e la politica di valutazione del rischio della Società relativa all'approccio basato sul rischio per i rischi di riciclaggio e di finanziamento del terrorismo.

Per Consiglio di amministrazione si intende il consiglio di amministrazione della Società. Se la Società non ha un consiglio di amministrazione, il manager della Società sarà considerato come membro del consiglio di amministrazione e sarà responsabile dei compiti del consiglio di amministrazione nel contesto delle Linee guida.

MLRO significa Money Laundering Reporting Officer, nominato dalla Società come responsabile della ricezione delle segnalazioni interne e delle segnalazioni al Financial Crime Investigation Service (FCIS) e di altri compiti come sopra descritto.

Per **operazione monetaria** si intende qualsiasi pagamento, trasferimento o ricezione di denaro.

Per **riciclaggio di denaro** (ML) si intende l'occultamento delle origini dei fondi illeciti attraverso la loro introduzione nel sistema economico legale e in transazioni che appaiono legittime. Il processo di riciclaggio si articola in tre fasi:

- collocamento, che consiste nel collocare i proventi del crimine nel sistema finanziario;
- la stratificazione, che prevede la conversione dei proventi del crimine in un'altra forma e la creazione di complessi strati di transazioni finanziarie per nascondere la pista di controllo e la fonte e la proprietà dei fondi;
- integrazione, che prevede il reinserimento dei proventi riciclati nell'economia per creare la percezione di legittimità.

Per **Operazione Occasionale** si intende la transazione effettuata dalla Società nel corso di attività economiche o professionali ai fini della fornitura di un servizio o della vendita di beni o della loro distribuzione in altro modo al Cliente al di fuori del corso di un Rapporto Commerciale stabilito.

Per **PEP** si intende una persona fisica che svolge o ha svolto funzioni pubbliche di rilievo e nei confronti della quale permangono rischi correlati.

Le sanzioni sono uno strumento essenziale della politica estera che mira a sostenere il mantenimento o il ripristino della pace, della sicurezza internazionale, della democrazia e dello stato di diritto, seguendo le regole dell'umanità.

---

[7] Per **chiave pubblica** s'intende un codice di lettere, numeri e/o simboli destinato a identificare il cliente e a generare l'indirizzo di valuta virtuale del cliente.

diritti e del diritto internazionale o il raggiungimento di altri obiettivi della Carta delle Nazioni Unite o della Politica estera e di sicurezza comune dell'Unione Europea. Le sanzioni includono:

- Sanzioni internazionali imposte nei confronti di uno Stato, un territorio, un'unità territoriale, un regime, un'organizzazione, un'associazione, un gruppo o una persona da una risoluzione del Consiglio di Sicurezza delle Nazioni Unite, da una decisione del Consiglio dell'Unione Europea o da qualsiasi altra legislazione che imponga obblighi alla Lituania;
- Sanzioni del Governo della Repubblica di Lituania, che sono uno strumento di politica estera che può essere imposto in aggiunta agli obiettivi specificati nella clausola precedente al fine di proteggere la sicurezza o gli interessi della Lituania.

Le sanzioni internazionali possono vietare l'ingresso di un soggetto di una sanzione internazionale nello Stato, limitare il commercio internazionale e le transazioni internazionali e imporre altri divieti o obblighi.

L'oggetto delle sanzioni è una persona fisica o giuridica, un'entità o un organismo, designato nell'atto giuridico che impone o attua le sanzioni, nei confronti del quale si applicano le sanzioni.

Per **finanziamento del terrorismo** (TF) si intende il finanziamento e il sostegno di un atto di terrorismo e la sua commissione, nonché il finanziamento e il sostegno di viaggi a scopo di terrorismo ai sensi della legislazione applicabile.

Per **Paese terzo** si intende uno Stato che non è membro dello Spazio economico europeo (SEE).

Per **valuta virtuale** si intende un valore rappresentato in forma digitale, che è trasferibile, conservabile o negoziabile digitalmente e che le persone fisiche o giuridiche accettano come strumento di pagamento, ma che non ha corso legale in nessun paese o fondo ai fini dell'articolo 4, paragrafo 25, della direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e che abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pagg. 35-127) o un'operazione di pagamento ai fini dell'articolo 3, lettere k e l, della stessa direttiva.12.2015, pagg. 35-127) o un'operazione di pagamento ai fini dell'articolo 3, lettere k) e l), della stessa direttiva.

Per **indirizzo della Valuta Virtuale** si intende un indirizzo/conto generato da lettere, numeri e/o simboli nella blockchain, mediante il quale la blockchain assegna la Valuta Virtuale al proprietario o al destinatario.

PRINCIPI DI STRUTTURA E GESTIONE DELLA SOCIETÀ

La struttura organizzativa della Società deve corrispondere alle sue dimensioni e alla natura, alla portata e al livello di complessità delle sue attività e dei servizi forniti, compresa la propensione al rischio e i rischi correlati, e deve essere strutturata secondo il principio delle **tre linee di difesa.** La struttura organizzativa della Società deve corrispondere alla completa comprensione dei rischi potenziali e alla loro gestione. Le catene di reporting e di subordinazione dell'Azienda devono essere garantite in modo tale che tutti i Dipendenti conoscano il proprio posto nella struttura organizzativa e sappiano quali sono i loro compiti lavorativi.

Il Consiglio di amministrazione

Il Consiglio di gestione è portatore della cultura del rispetto dei requisiti di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo, garantendo che i membri del Consiglio di gestione e i dipendenti della Società operino in un ambiente in cui siano pienamente consapevoli dei requisiti di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo e degli obblighi associati a tali requisiti, e che le considerazioni sui rischi rilevanti siano prese in considerazione in misura adeguata nei processi decisionali della Società.

I membri del Consiglio di amministrazione hanno la responsabilità ultima delle misure adottate per prevenire l'uso dei servizi della Società per il riciclaggio di denaro o il finanziamento del terrorismo. Essi forniscono la supervisione e sono responsabili di:

- stabilire e mantenere i processi, le procedure, i rischi e i processi di controllo AML[8] ;
- adottare le presenti Linee guida e altre linee guida e istruzioni interne;
- determinare le linee guida della Società per le misure antiriciclaggio;
- nominare un MLRO e assicurarsi che l'MLRO abbia i poteri, le risorse e le competenze necessarie per svolgere il proprio incarico;
- stanziare risorse sufficienti per garantire l'effettiva attuazione delle Linee guida e degli altri documenti correlati e per mantenere l'organizzazione;
- garantire che tutti i dipendenti interessati completino la formazione annuale in materia di antiriciclaggio.

La prima linea di difesa: i dipendenti

La prima linea di difesa ha la funzione di applicare le misure di due diligence al momento del rapporto commerciale e di applicare le misure di due diligence durante il rapporto commerciale. La prima linea di difesa comprende le unità strutturali e i Dipendenti della Società alle cui attività sono associati i rischi e che devono identificare e valutare tali rischi, le loro caratteristiche specifiche e la loro portata e che gestiscono tali rischi attraverso le loro attività ordinarie, principalmente attraverso l'applicazione delle misure di due diligence. I rischi derivanti dalle attività e dalla fornitura di servizi della Società appartengono alla prima linea di difesa. Sono i gestori (proprietari) di questi rischi e ne sono responsabili.

[8] Ai fini della semplificazione delle presenti Linee guida, il termine "antiriciclaggio" comprende anche la prevenzione del finanziamento del terrorismo e l'attuazione delle sanzioni.

I Dipendenti della Società devono agire con la lungimiranza e la competenza che ci si aspetta da loro e secondo i requisiti stabiliti per le loro posizioni, procedendo dagli interessi e dagli obiettivi della Società, e garantire che il sistema finanziario e lo spazio economico del Paese non siano utilizzati per il riciclaggio di denaro e il finanziamento del terrorismo. La Società adotta misure per valutare l'idoneità dei Dipendenti prima che inizino a lavorare con la relativa formazione.

Per i suddetti motivi, i Dipendenti sono tenuti a:

- rispettare tutti i requisiti indicati nelle Linee guida e negli altri documenti correlati;
- raccogliere le informazioni richieste sui clienti in base alla loro funzione e alle loro responsabilità;
- segnalare senza indugio all'MLRO informazioni, situazioni, attività, transazioni o tentativi di transazione insoliti per qualsiasi tipo di servizio o rapporto con il cliente, indipendentemente dall'importo e dal fatto che la transazione sia stata completata o meno;
- non informare o rendere altrimenti noto ai Clienti se il Cliente o altri Clienti sono o possono essere oggetto di una segnalazione o se una segnalazione è stata o può essere presentata;
- completare l'adeguata formazione antiriciclaggio richiesta per la posizione del Dipendente.

La seconda linea di difesa - Gestione del rischio e conformità, MLRO

La seconda linea di difesa è costituita dalle funzioni di gestione del rischio e di conformità. Queste funzioni possono anche essere svolte dalla stessa persona o unità strutturale a seconda delle dimensioni della Società e della natura, dell'ambito e del livello di complessità delle loro attività e dei servizi forniti, compresa la propensione al rischio e i rischi derivanti dalle attività della Società.

L'obiettivo della **funzione di compliance** è quello di garantire che la Società sia conforme alla legislazione, alle linee guida e ad altri documenti in vigore e di valutare il possibile effetto di eventuali modifiche del contesto legale o normativo sulle attività della Società e sul quadro di compliance. Il compito della compliance è quello di aiutare la prima linea di difesa, in quanto detentrice del rischio, a definire i luoghi in cui i rischi si manifestano (ad esempio, l'analisi delle transazioni sospette e insolite, per le quali i dipendenti addetti alla compliance possiedono le competenze professionali e le qualità personali richieste, ecc. La seconda linea di difesa non si impegna ad assumere rischi.

La politica del rischio viene attuata e il quadro di gestione del rischio è controllato dalla **funzione di gestione del rischio**. L'esecutore della funzione di gestione del rischio assicura che tutti i rischi siano identificati, valutati, misurati, monitorati e gestiti, e ne informa le unità appropriate della Società. L'esecutore della funzione di gestione del rischio ai fini dell'antiriciclaggio svolge principalmente la supervisione sul rispetto della propensione al rischio, la supervisione sulla tolleranza al rischio, la supervisione sull'identificazione delle variazioni dei rischi, esegue la panoramica dei rischi associati e svolge altri compiti relativi alla gestione del rischio.

Il Consiglio di amministrazione ha nominato un **MLRO** per svolgere le funzioni di seconda linea di difesa. Questa persona non è coinvolta operativamente nelle aree che l'MLRO monitorerà e verificherà ed è quindi indipendente in relazione a queste. Nell'ambito dell'attuale struttura antiriciclaggio della Società, è l'MLRO a prendere le decisioni chiave in merito alle singole questioni antiriciclaggio, come l'approvazione delle PEP, l'accettazione o il rifiuto degli utenti ad alto rischio.

ecc. Il responsabile antiriciclaggio nominato dalla Società è il funzionario senior della Società e una persona che possiede tutte le conoscenze e il background lavorativo necessari.

L'MLRO è responsabile delle seguenti attività:

- produrre e, quando necessario, aggiornare le Linee guida della Società;
- monitorare e verificare costantemente che la Società soddisfi i requisiti prescritti dalle presenti Linee guida e dai documenti correlati, nonché le leggi e i regolamenti esterni;
- fornire al personale della Società e ai membri del Consiglio di amministrazione consulenza e supporto in merito alle norme relative al riciclaggio di denaro e al finanziamento del terrorismo;
- informare e formare i membri del Consiglio di amministrazione e le persone interessate sulle norme relative al riciclaggio di denaro e al finanziamento del terrorismo;
- indagare e registrare dati sufficienti sulle notifiche interne ricevute e decidere se l'attività può essere giustificata o se è sospetta;
- depositare le relazioni pertinenti presso le autorità di regolamentazione competenti in conformità alla legislazione applicabile;
- verificare e valutare regolarmente se le procedure e le linee guida dell'Azienda per prevenire l'uso dell'attività per il riciclaggio di denaro o il finanziamento del terrorismo sono adeguate allo scopo ed efficaci.

L'MLRO riferisce al Consiglio di amministrazione con cadenza trimestrale. Tale relazione deve essere redatta per iscritto e deve includere almeno i seguenti elementi:

- numero di clienti in tutte le classificazioni di rischio
- numero di riscontri positivi di persone in relazione agli elenchi di sanzioni e alle misure applicate;
- numero di clienti o rappresentanti dei clienti identificati come PEP o persone con un legame con una PEP;
- numero di notifiche interne su attività o transazioni sospette;
- numero di segnalazioni pertinenti segnalate al Financial Crime Investigation Service (FCIS);
- numero e contenuto di una richiesta di informazioni al FCIS nell'ambito di un'indagine;
- la conferma dell'aggiornamento della valutazione del rischio di riciclaggio di denaro e di finanziamento del terrorismo;
- conferma che le presenti Linee guida e gli altri documenti correlati sono aggiornati;
- la conferma che il personale addetto alle misure antiriciclaggio è sufficiente;
- tutte le eventuali inadeguatezze individuate dalla funzione di controllo sono state affrontate;
- elenco dei corsi di formazione obbligatori tenuti per il personale in materia di misure antiriciclaggio.

La terza linea di difesa: l'audit interno

La terza linea di difesa è costituita da una funzione di revisione interna indipendente ed efficace. La funzione di revisione interna può essere svolta da un Preposto al controllo interno. Può trattarsi di uno o più dipendenti, dell'unità strutturale della Società con le relative funzioni o di una terza parte che fornisce il servizio in questione alla Società. Il Preposto al controllo interno non può ricoprire la posizione di MLRO e/o di membro del Consiglio di amministrazione della Società o altre posizioni che includano la stesura e/o la modifica dei regolamenti interni e delle linee guida della Società in materia di Antiriciclaggio e Finanziamento del Terrorismo.

I dipendenti, l'unità strutturale dell'Azienda o una terza parte che svolge la funzione di audit interno devono disporre delle competenze, degli strumenti e dell'accesso alle informazioni pertinenti necessari in tutte le unità strutturali dell'Azienda. I metodi di revisione interna devono essere conformi alle dimensioni dell'Azienda, alla natura, all'ambito e al livello di complessità delle attività e dei servizi forniti, compresa la propensione al rischio e i rischi derivanti dalle attività dell'Azienda.

La decisione di condurre un audit interno viene presa con una delibera del Consiglio di amministrazione. Il Consiglio di amministrazione deve valutare la necessità di condurre un audit interno almeno una volta all'anno.

PRINCIPI DI ATTUAZIONE DELLE MISURE DI DUE DILIGENCE DEL CLIENTE

Le misure di due diligence del cliente (CDD) sono necessarie per verificare l'identità di un cliente nuovo o esistente e per effettuare un monitoraggio continuo basato sul rischio del rapporto commerciale con il cliente. Le misure di CDD consistono in 3 livelli, tra cui misure di due diligence semplificate e rafforzate, come specificato di seguito.

Principi fondamentali

Le misure di CDD vengono adottate ed eseguite nella misura necessaria in considerazione del profilo di rischio del Cliente e di altre circostanze nei seguenti casi:

- al momento dell'avvio della Relazione d'affari e durante il monitoraggio continuo della Relazione d'affari;
- all'atto dell'esecuzione o della mediazione di Operazioni occasionali al di fuori del Rapporto commerciale, qualora il valore della/e transazione/i sia pari o superiore a 700 euro (o un importo equivalente in altre attività) entro 24 ore;
- al momento dell'esecuzione o della mediazione di Operazioni occasionali al di fuori del rapporto commerciale, il cui valore ammonti a 10.000 euro o più (o a un importo equivalente in altri beni) nell'arco di un mese;
- in seguito alla verifica delle informazioni raccolte durante l'applicazione delle misure di due diligence o in caso di dubbi sulla sufficienza o sulla veridicità dei documenti o dei dati raccolti in precedenza durante l'aggiornamento dei dati pertinenti;
- in caso di sospetto di riciclaggio di denaro o di finanziamento del terrorismo, indipendentemente da eventuali deroghe, eccezioni o limiti previsti dalle presenti Linee guida e dalla legislazione applicabile.

La Società non stabilisce o mantiene la Relazione d'affari e non esegue la transazione se:

- la Società non è in grado di adottare ed eseguire nessuna delle misure CDD richieste;
- la Società abbia il sospetto che i servizi o la transazione della Società vengano utilizzati per il riciclaggio di denaro o il finanziamento del terrorismo;
- il livello di rischio del Cliente o della transazione non è conforme alla propensione al rischio della Società.

Nel caso in cui riceva informazioni in lingua straniera nell'ambito dell'implementazione della CDD, la Società può richiedere la traduzione dei documenti in un'altra lingua adatta alla Società. L'uso di traduzioni dovrebbe essere evitato in situazioni in cui i documenti originali sono preparati in una lingua adatta alla Società.

Il raggiungimento della CDD è un processo che inizia con l'attuazione delle misure di CDD. Al termine di tale processo, al Cliente viene assegnato un livello di rischio individuale documentato che costituisce la base per le misure di follow-up e che viene seguito e aggiornato quando necessario.

La Società ha applicato adeguatamente le misure di CDD se ha la convinzione interna di aver rispettato l'obbligo di applicare le misure di due diligence. Il principio di ragionevolezza viene osservato nella considerazione della convinzione interna. Ciò significa che la Società deve, al momento dell'applicazione delle misure di CDD, acquisire la conoscenza, la comprensione e l'affermazione di aver raccolto informazioni sufficienti sul Cliente, sulle attività del Cliente, sullo scopo del Rapporto d'affari e delle transazioni eseguite nell'ambito del Rapporto d'affari, sull'origine dei fondi, ecc. Tale livello di asserzione deve consentire di identificare transazioni complicate, di valore elevato e insolite e schemi di transazione che non hanno uno scopo economico o legittimo ragionevole o ovvio o che non sono caratteristici delle caratteristiche specifiche dell'attività in questione.

La Società deve applicare la CDD non solo ai Clienti persone fisiche, ma anche alle persone giuridiche. Tutti i controagenti e i partner della Società sono controllati manualmente dal responsabile MLRO con l'aiuto di fonti affidabili e indipendenti.

I servizi offerti

L'attività economica principale della Società è costituita dai servizi di valuta virtuale. Per questo motivo, la Società offre ai propri Clienti i seguenti tipi di transazione:

- fornire il servizio di operatore di cambio di Valuta Virtuale, che consente al Cliente di scambiare, acquistare e vendere Valuta Virtuale.

La Società fornirà i suddetti servizi solo nel corso di un rapporto commerciale consolidato.

La verifica delle informazioni utilizzate per l'identificazione del Cliente

Per verifica delle informazioni per l'identificazione del Cliente si intende l'utilizzo di dati provenienti da una fonte affidabile e indipendente per confermare che i dati sono veri e corretti, confermando anche, se necessario, che i dati direttamente collegati al Cliente sono veri e corretti. Ciò significa, tra l'altro, che lo scopo della verifica delle informazioni è quello di ottenere la certezza che il Cliente che intende instaurare il rapporto commerciale sia la persona che dichiara di essere.

La fonte affidabile e indipendente (deve esistere cumulativamente) è la verifica delle informazioni ottenute nel corso dell'identificazione:

- che proviene da due fonti diverse;
- che sono stati emessi da (documenti d'identità) o ricevuti da una terza parte o da un luogo che non ha interessi o legami con il Cliente o la Società, vale a dire che è neutrale (ad esempio, le informazioni ottenute da Internet non sono tali, in quanto spesso provengono dal Cliente stesso o la loro affidabilità e indipendenza non può essere verificata);
- la cui affidabilità e indipendenza possono essere determinate senza ostacoli oggettivi e l'affidabilità e l'indipendenza sono comprensibili anche a una terza parte non coinvolta nella Relazione d'Affari; e
- i dati inclusi o ottenuti tramite i quali sono aggiornati e pertinenti e la Società può ottenere rassicurazioni in merito (e in alcuni casi le rassicurazioni possono essere ottenute anche sulla base delle due clausole precedenti).

Applicazione delle misure di due diligence semplificate (livello 1)

Le misure di due diligence semplificate (SDD) vengono applicate quando il profilo di rischio del cliente indica un basso livello di rischio di riciclaggio e di finanziamento del terrorismo.

Nell'applicare le misure SDD, la Società deve ottenere solo[9] i seguenti dati del Cliente che è una persona fisica:

- nome/i e cognome/i;
- numero personale;[10] o

nel caso del Cliente, che è una persona giuridica, i seguenti dati:

- nome o ragione sociale;
- forma giuridica;
- numero di registrazione, se tale numero è stato rilasciato;
- sede legale (indirizzo) e indirizzo di esercizio effettivo;
- nome/i, cognome/i e numero personale o data di nascita del rappresentante del Cliente; e

garantire che il primo pagamento sia effettuato tramite un conto presso un istituto di credito, qualora l'istituto di credito sia registrato nel SEE o in un Paese terzo che imponga requisiti equivalenti a quelli previsti dalla legge in materia e sia sottoposto alla vigilanza delle autorità competenti per il rispetto di tali requisiti.

Le misure di SDD possono essere eseguite solo se il monitoraggio continuo del rapporto commerciale con il cliente viene eseguito in conformità alle Linee guida e se esiste la possibilità di identificare operazioni e transazioni monetarie sospette.

Le misure di SDD non devono essere eseguite nelle circostanze in cui devono essere eseguite misure di due diligence rafforzate (come descritto di seguito).

---

9 Quando il Cliente è un'istituzione o un'agenzia statale o municipale o la Banca di Lituania, la Società può, nel corso dell'applicazione delle misure SDD, raccogliere solo i dati personali di tali entità e dei loro rappresentanti.

10 nel caso di uno straniero - la data di nascita (se disponibile - il numero personale o qualsiasi altra sequenza unica di simboli concessi a quella persona, destinati all'identificazione personale).

Qualora, nel corso del monitoraggio continuo delle relazioni commerciali del Cliente, si stabilisca che il rischio di riciclaggio e/o di frode finanziaria non è più basso, la Società deve applicare il livello pertinente di misure di CDD.

Applicazione delle misure standard di due diligence (livello 2)

Le misure di due diligence standard sono applicate a tutti i clienti per i quali è necessario applicare misure di CDD in conformità alle Linee guida. Le seguenti misure di due diligence standard devono essere applicate:

- l'identificazione del Cliente e la verifica delle informazioni presentate sulla base di informazioni ottenute da una fonte affidabile e indipendente;
- identificazione e verifica di un rappresentante del Cliente e del suo diritto di rappresentanza;
- l'identificazione del Titolare effettivo e, al fine di verificarne l'identità, l'adozione di misure che consentano alla Società di accertarsi di sapere chi è il Titolare effettivo e di comprendere la struttura proprietaria e di controllo del Cliente;
- comprensione della Relazione d'affari, della transazione o dell'operazione e, se del caso, raccolta di informazioni al riguardo;
- raccogliere informazioni sul fatto che il Cliente sia una PEP, un suo familiare o una persona nota come stretta collaboratrice;
- monitoraggio del rapporto commerciale.

Le misure di CDD sopra descritte devono essere applicate prima di instaurare un rapporto d'affari o di effettuare una transazione. Le istruzioni precise per l'applicazione delle misure di due diligence standard sono fornite nelle Linee guida.

Applicazione di misure di due diligence rafforzate (livello 3)

Oltre alle misure di due diligence standard, la Società applica misure di due diligence rafforzate (EDD) al fine di gestire e mitigare un rischio accertato di riciclaggio di denaro e di finanziamento del terrorismo nel caso in cui il rischio sia più elevato del normale.

L'azienda applica sempre misure di EDD, quando:

- il profilo di rischio del Cliente indica un elevato livello di rischio di riciclaggio e di frode;
- dopo l'identificazione del Cliente o la verifica delle informazioni trasmesse, sussistono dubbi sulla veridicità dei dati trasmessi, sull'autenticità dei documenti o sull'identificazione del Titolare effettivo;
- quando vengono avviati rapporti di corrispondenza transfrontalieri con il Cliente, che è un istituto finanziario di un Paese terzo;
- in caso di esecuzione di una transazione o di un rapporto d'affari con il PEP, il familiare del PEP o una persona nota come stretto collaboratore del PEP;
- qualora la transazione o il Rapporto d'affari siano effettuati con persone fisiche residenti o persone giuridiche stabilite in Paesi Terzi ad alto rischio come individuati dalla Commissione Europea;

- il Cliente proviene da tale paese o territorio o il suo luogo di residenza o la sua sede o la sede del prestatore di servizi di pagamento del beneficiario si trova in un paese o territorio che, secondo fonti credibili quali valutazioni reciproche, relazioni o rapporti di follow-up pubblicati, non ha istituito sistemi efficaci di prevenzione del riciclaggio e del finanziamento del terrorismo conformi alle raccomandazioni del GAFI.

Prima di applicare le misure EDD, il Dipendente della Società si assicura che il Rapporto d'affari o la transazione abbiano un rischio elevato e che un tasso di rischio elevato possa essere attribuito a tale Rapporto d'affari o transazione. Soprattutto, prima di applicare le misure EDD, il Dipendente valuta se le caratteristiche sopra descritte sono presenti e le applica come motivi indipendenti (vale a dire, ciascuno dei fattori identificati consente l'applicazione delle misure EDD nei confronti del Cliente).

Nell'applicazione delle misure EDD in caso di avvio di un rapporto di corrispondenza transfrontaliera con il Cliente, che è un istituto finanziario di un Paese terzo, la Società deve applicare le seguenti misure:

- raccogliere informazioni sufficienti sul Cliente per comprendere appieno la natura della sua attività e per determinare, sulla base delle informazioni pubblicamente disponibili, la reputazione del Cliente e la qualità della vigilanza;
- valutare i meccanismi di controllo per l'antiriciclaggio del cliente e dell'entità che riceve i fondi;
- ottenere l'approvazione del membro del Consiglio di amministrazione prima di stabilire nuovi rapporti di corrispondenza;
- documentare le rispettive responsabilità del Cliente;
- essere soddisfatti che il Cliente abbia effettuato un'adeguata due diligence del Cliente (compresa la verifica dell'identità dei Clienti che hanno accesso diretto ai conti del Cliente e l'esecuzione di altre azioni di due diligence del Cliente) e che sia in grado di fornire i relativi dati di identificazione del Cliente alla Società su sua richiesta.

Nell'applicare le misure EDD, quando le transazioni o le relazioni d'affari sono effettuate con la PEP, il familiare della PEP o una persona nota come stretta collaboratrice della PEP, la Società deve applicare le seguenti misure:

- ottenere l'approvazione del membro del Consiglio di amministrazione prima di instaurare un rapporto d'affari con tale cliente o di continuare il rapporto d'affari con il cliente quando questi diventa una PEP;
- adottare misure adeguate per stabilire la fonte di ricchezza e la fonte di fondi che sono coinvolti nel Rapporto d'affari o nella transazione;
- effettuare un monitoraggio continuo della relazione commerciale con il cliente, aumentando il numero e la tempistica dei controlli applicati e selezionando i modelli di transazioni che necessitano di un ulteriore esame.

Nell'applicazione delle misure EDD in caso di transazioni o rapporti commerciali con persone fisiche residenti o persone giuridiche stabilite in Paesi Terzi ad alto rischio come individuati dalla Commissione Europea, la Società deve applicare le seguenti misure:

- ottenere ulteriori informazioni sul Cliente e sul suo Proprietario Beneficiario;
- ottenere ulteriori informazioni sulla natura prevista della Relazione d'affari;

- ottenere informazioni sulla fonte di fondi e sulla fonte di ricchezza del Cliente e del suo Proprietario Beneficiario;
- ottenere informazioni sulle ragioni delle transazioni previste o effettuate;
- ottenere l'approvazione del membro del Consiglio di amministrazione per l'avvio di rapporti commerciali con il Cliente o per la prosecuzione di rapporti commerciali con lo stesso;
- effettuare un monitoraggio continuo della relazione commerciale con il cliente, aumentando il numero e la tempistica dei controlli applicati e selezionando i modelli di transazioni che necessitano di un ulteriore esame;
- garantire che il primo pagamento sia effettuato tramite un conto intestato al Cliente presso un istituto di credito, laddove l'istituto di credito sia registrato nel SEE o in un Paese terzo che imponga requisiti equivalenti a quelli previsti dalla legge applicabile e sia sottoposto alla vigilanza delle autorità competenti per il rispetto di tali requisiti.

Quando si applicano le misure EDD nel caso in cui il Cliente provenga da tale Paese o territorio o il suo luogo di residenza o la sua sede o la sede del prestatore di servizi di pagamento del beneficiario si trovino in un Paese o territorio che, secondo fonti credibili quali valutazioni reciproche, relazioni o rapporti di follow-up pubblicati, non ha istituito sistemi efficaci di prevenzione del riciclaggio e del finanziamento del terrorismo conformi alle raccomandazioni del GAFI, la Società deve applicare le seguenti misure:

- ottenere l'approvazione del membro del Consiglio di amministrazione per l'avvio di rapporti commerciali con il Cliente o per la prosecuzione di rapporti commerciali con lo stesso;
- ottenere informazioni sulla fonte di fondi e sulla fonte di ricchezza del Cliente e del suo Proprietario Beneficiario;
- effettuare un monitoraggio continuo della relazione commerciale con il cliente, aumentando il numero e la tempistica dei controlli applicati e selezionando i modelli di transazioni che necessitano di un ulteriore esame;

In tutti gli altri casi in cui è necessario applicare misure di EDD, l'entità delle misure di EDD e la loro portata saranno determinate dal Dipendente che le applica. Possono essere seguite le seguenti misure di due diligence aggiuntive e pertinenti:

- verifica delle informazioni presentate in aggiunta all'identificazione del Cliente sulla base di documenti, dati o informazioni supplementari provenienti da una fonte credibile e indipendente;
- raccogliere ulteriori informazioni sullo scopo e sulla natura del Rapporto d'affari o della transazione e verificare le informazioni presentate sulla base di ulteriori documenti, dati o informazioni provenienti da una fonte affidabile e indipendente;
- raccogliere ulteriori informazioni e documenti sull'effettiva esecuzione delle transazioni effettuate nell'ambito del Rapporto d'affari, al fine di escludere l'ostensibilità delle transazioni;
- raccogliere ulteriori informazioni e documenti allo scopo di identificare la fonte e l'origine dei fondi utilizzati in una transazione effettuata nell'ambito della Relazione d'affari, al fine di escludere l'ostensibilità delle transazioni;
- l'effettuazione del primo pagamento relativo ad una transazione tramite un conto che è stato

aperto a nome del Cliente che partecipa alla transazione in un istituto di credito registrato o avente sede in uno Stato contraente dello Spazio Economico Europeo o in un Paese in cui sono in vigore requisiti pari a quelli della Direttiva (UE) 2015/849 del Parlamento Europeo e del Consiglio;

- l'applicazione di misure CDD relative al Cliente o al suo rappresentante mentre si trova nello stesso luogo del Cliente o del suo rappresentante;
- raccogliere ulteriori informazioni sul Cliente e sul suo Proprietario Beneficiario, compresa l'identificazione di tutti i proprietari del Cliente, compresi quelli la cui partecipazione azionaria è inferiore al 25%;
- raccogliere informazioni sull'origine dei fondi e del patrimonio del Cliente e del suo Beneficiario;
- migliorare il monitoraggio della Relazione Commerciale aumentando il numero e la frequenza delle misure di controllo applicate e scegliendo indicatori di transazione o modelli di transazione che vengono verificati ulteriormente;
- ottenere l'approvazione del membro del Consiglio di amministrazione per l'esecuzione di transazioni o l'instaurazione di rapporti commerciali con clienti nuovi ed esistenti;

Quando esegue l'EDD, in alcuni casi la Società è tenuta ad adottare misure ragionevoli per stabilire la fonte dei fondi e la fonte del patrimonio dei Clienti. La fonte dei fondi può essere verificata facendo riferimento, *tra l'altro, a*:

- una dichiarazione annuale dei redditi;
- un originale o una copia autenticata di una busta paga recente;
- conferma scritta del salario annuale firmata dal datore di lavoro;
- un originale o una copia certificata del contratto di vendita del bene immobile e un estratto originale di un istituto finanziario che attesti la ricezione dei fondi ottenuti dalla vendita del bene immobile, se disponibile;
- un originale o una copia autenticata di un testamento o di un documento equivalente che attesti l'eredità;
- un originale o una copia autenticata di un accordo di donazione (in forma scritta semplice o autenticata da un notaio nel caso in cui la forma notarile dell'accordo sia richiesta dalla legge);
- un originale o una copia autenticata di un contratto di prestito (in forma scritta semplice o autenticata da un notaio nel caso in cui la forma notarile del contratto sia richiesta dalla legge), e un estratto di un istituto finanziario che attesti la ricezione o l'invio di fondi relativi alla ricezione del prestito o alla restituzione di un prestito concesso; o una cambiale (in forma scritta semplice o autenticata da un notaio nel caso in cui la forma notarile del contratto sia richiesta dalla legge);
- una ricerca su Internet nel registro delle imprese per confermare la vendita di una società;
- originale o una copia autenticata del contratto di deposito;
- libro cassa o registro delle operazioni di cassa (per le persone giuridiche);
- altre informazioni.

Il dipendente dovrà comunicare le misure EDD applicate entro 2 giorni lavorativi dall'inizio dell'applicazione delle misure EDD inviando la relativa notifica all'MLRO.

In caso di applicazione di misure EDD, la Società rivaluta il profilo di rischio del Cliente al più tardi ogni sei mesi.

MISURE DI DUE DILIGENCE PER I CLIENTI

Identificazione del Cliente - persona fisica

La Società identifica il Cliente che è una persona fisica e, se del caso, il suo rappresentante e conserva i seguenti dati del Cliente:

- nome/i e cognome/i;
- numero personale;[11]
- cittadinanza;[12]
- fotografia;
- firma.[13]

I seguenti documenti d'identità validi che contengono i dati specificati sopra possono essere utilizzati come base per l'identificazione di una persona fisica:

- un documento d'identità della Repubblica di Lituania, ad eccezione del permesso di soggiorno della Repubblica di Lituania;
- un documento d'identità di uno Stato estero;

Il Cliente, persona fisica, non può avvalersi di un rappresentante nel corso del rapporto commerciale con la Società.

Identificazione del Cliente - persona giuridica

La Società identifica il Cliente, che è una persona giuridica, e il suo rappresentante e conserva i seguenti dati sul Cliente:

- nome o ragione sociale;
- forma giuridica;
- numero di registrazione, se tale numero è stato rilasciato;

[11] nel caso di uno straniero - la data di nascita (se disponibile - il numero personale o qualsiasi altra sequenza univoca di simboli concessi a quella persona, destinati all'identificazione personale);

[12] se un documento d'identità non contiene dati sulla cittadinanza del cliente, gli istituti finanziari e gli altri soggetti obbligati devono, quando identificano il cliente che è una persona fisica in presenza fisica del cliente, richiedere al cliente di fornire i dati sulla cittadinanza.

[13] tranne nei casi in cui è facoltativo nel documento d'identità;

- nome/i e cognome/i, numero personale (nel caso di uno straniero - data di nascita o, se disponibile, numero personale o qualsiasi altra sequenza unica di simboli concessa a

tale persona, destinata all'identificazione personale) e la cittadinanza del/dei direttore/i o del/dei membro/i del Consiglio di amministrazione o del/dei membro/i di un altro organismo equivalente, e le loro autorità in rappresentanza del Cliente;

- un estratto di registrazione e la sua data di emissione;
- sede legale (indirizzo) e indirizzo di esercizio effettivo
- I seguenti documenti, rilasciati da un'autorità o da un organismo competente non prima di sei mesi prima del loro utilizzo, possono essere utilizzati per l'identificazione del Cliente:
    - scheda anagrafica del registro pertinente; oppure
    - certificato di registrazione del registro pertinente; o
    - un documento equivalente ai documenti sopra citati o ai documenti di stabilimento del Cliente.

La Società verifica la correttezza dei dati del Cliente sopra indicati, utilizzando a tal fine informazioni provenienti da una fonte credibile e indipendente. Nel caso in cui la Società abbia accesso al relativo registro delle persone giuridiche, non è necessario richiedere al Cliente la presentazione dei documenti di cui sopra.

L'identità della persona giuridica e il diritto di rappresentanza della persona giuridica possono essere verificati sulla base di un documento specificato sopra, che è stato autenticato da un notaio o certificato da un notaio o ufficialmente, o sulla base di altre informazioni provenienti da una fonte credibile e indipendente, compresi i mezzi di identificazione elettronica e i servizi fiduciari per le transazioni elettroniche, utilizzando così almeno due fonti diverse per la verifica dei dati in tale caso.

L'identificazione del rappresentante del Cliente e il suo diritto di rappresentanza.

Il rappresentante del Cliente deve essere identificato come il Cliente, che è una persona fisica ai sensi delle presenti Linee guida. La Società deve inoltre identificare e verificare la natura e la portata del diritto di rappresentanza del Cliente. Il nome, la data di emissione e il nome dell'emittente del documento che funge da base per il diritto di rappresentanza devono essere accertati e conservati, tranne nel caso in cui il diritto di rappresentanza sia stato verificato utilizzando informazioni provenienti dal registro pertinente.

La Società deve rispettare le condizioni del diritto di rappresentanza concesso ai rappresentanti della persona giuridica e fornire servizi solo nell'ambito del diritto di rappresentanza.

L'autorizzazione deve essere in linea con i requisiti del Codice Civile lituano. L'autorizzazione rilasciata all'estero deve essere legalizzata o munita di Apostille. Nel caso in cui il diritto di rappresentanza del Cliente (persona giuridica) sia evidente dall'estratto del registro, dallo Statuto o da documenti equivalenti che attestino l'identità del Cliente (persona giuridica), non dovrebbe essere necessario un documento di autorizzazione separato (ad esempio una procura).

L'identificazione del Proprietario Beneficiario del Cliente

La Società deve identificare il Proprietario Beneficiario del Cliente - una persona fisica che in ultima analisi possiede o controlla il Cliente o per conto della quale viene condotta una transazione. L'Azienda deve inoltre adottare misure per verificare l'identità del Titolare effettivo, nella misura in cui ciò consente all'Azienda di accertarsi di sapere chi sia il Titolare effettivo. La Società non può presumere che i privati siano essi stessi il BO del Cliente, e deve sempre ottenere prima dal Cliente le informazioni su chi sia il BO. Per identificazione del BO si intende l'identificazione di una persona fisica o di un gruppo di persone fisiche.

Il La Società raccoglie i seguenti dati relativi al/i Titolare/i effettivo/i del Cliente:

- nome/i e cognome/i;
- numero personale;[14]
- cittadinanza.[15]

La Società richiederà al Cliente informazioni sul Proprietario effettivo del Cliente (ad esempio, fornendo al Cliente l'opportunità di specificare il proprio Proprietario effettivo al momento della raccolta dei dati sul Cliente).

La Società non instaura il rapporto commerciale se il Cliente, che è una persona fisica, ha un Proprietario Beneficiario che non è la stessa persona del Cliente.

L'identificazione del Beneficiario di una persona giuridica avviene per fasi, in cui il soggetto obbligato procede a ciascuna fase successiva se il Beneficiario della persona giuridica non può essere determinato nel caso della fase precedente. Le fasi sono le seguenti:

- è possibile identificare, per quanto riguarda il Cliente che è un'entità giuridica o una persona che partecipa alla transazione, la persona o le persone fisiche che effettivamente controllano in ultima istanza l'entità giuridica o esercitano un'influenza o un controllo su di essa in qualsiasi altro modo, indipendentemente dall'entità delle azioni, dei diritti di voto o dei diritti di proprietà o dalla sua natura diretta o indiretta;
- se il Cliente che è una persona giuridica o la persona che partecipa alla transazione ha una o più persone fisiche che possiedono o controllano la persona giuridica attraverso una partecipazione diretta[16] o indiretta[17] . Anche i legami familiari e i legami contrattuali devono essere presi in considerazione;
- chi è la persona fisica di vertice[18] , che deve essere definita come il Titolare effettivo, in quanto l'esecuzione delle due fasi precedenti non ha consentito al soggetto obbligato di identificare il Titolare effettivo.

Il senior manager del Cliente deve essere indicato come Titolare effettivo solo in casi eccezionali in cui la Società compie tutti gli sforzi ragionevoli per determinare il Titolare effettivo e a condizione che non vi siano motivi per sospettare che l'identità del Titolare effettivo sia nascosta. In questo caso, il senior manager deve essere inteso come il capo (ad esempio, l'amministratore delegato),

[14] nel caso di uno straniero - la data di nascita (se disponibile - il numero personale o qualsiasi altra sequenza unica di simboli concessi a quella persona, destinati all'identificazione personale);

[15] se un documento d'identità non contiene dati sulla cittadinanza del cliente, gli istituti finanziari e gli altri soggetti obbligati devono, quando identificano il cliente che è una persona fisica in presenza fisica del cliente, richiedere al cliente di fornire i dati sulla cittadinanza.

[16] **La proprietà diretta** è un modo di esercitare il controllo in cui la persona fisica possiede una partecipazione del 25% più un'azione o un diritto di proprietà superiore al 25% nella società.

[17] **La proprietà indiretta** è una modalità di esercizio del controllo in cui una partecipazione del 25% più un'azione o un diritto di proprietà superiore al 25% nella società è detenuto da una società controllata da una persona fisica o da più società controllate dalla stessa persona fisica.

[18] un **membro dell'alta direzione** è una persona che prende le decisioni strategiche che influenzano fondamentalmente le attività e/o le pratiche aziendali e/o l'andamento generale dell'azienda o che, in sua assenza, svolge le funzioni di gestione quotidiana o regolare dell'azienda nell'ambito del potere esecutivo (ad esempio, amministratore delegato (CEO), direttore finanziario (CFO), direttore o presidente, ecc.

Amministratore delegato, responsabile dell'amministrazione) del Cliente. I documenti utilizzati per l'identificazione dell'entità legale o gli altri documenti presentati non sono

non indicano direttamente chi è il Titolare effettivo della persona giuridica, i dati rilevanti (compresi quelli relativi all'appartenenza a un gruppo e alla struttura proprietaria e gestionale del gruppo) sono registrati sulla base della dichiarazione del rappresentante della persona giuridica o del documento scritto a mano dal rappresentante della persona giuridica.

La Compagnia applicherà misure ragionevoli per verificare l'accuratezza delle informazioni stabilite sulla base di dichiarazioni o di un documento scritto a mano (ad esempio, effettuando indagini nei registri pertinenti), richiedendo la presentazione della relazione annuale della persona giuridica o di altri documenti pertinenti. Se la Società nutre dubbi sull'accuratezza o la completezza delle informazioni pertinenti, la Società verificherà le informazioni fornite da fonti pubblicamente disponibili e, se necessario, richiederà ulteriori informazioni al Cliente.

Difficoltà incontrate durante l'identificazione del Proprietario Beneficiario

La Società deve essere consapevole del fatto che le informazioni sulla titolarità effettiva possono essere oscurate attraverso l'uso di società di comodo, strutture complesse di proprietà e controllo che comportano molti livelli di azioni registrate a nome di altre persone giuridiche, azionisti e amministratori designati, come stretti collaboratori e familiari, e in altri modi.

In molti casi, il ruolo degli amministratori e degli azionisti designati è quello di proteggere o nascondere l'identità del proprietario e del controllore di una società o di un bene. Una persona designata può aiutare a superare i controlli giurisdizionali sulla proprietà delle società e ad aggirare i divieti di amministrazione imposti da tribunali e autorità governative. Pertanto, la Società deve prestare particolare attenzione alle strutture societarie che favoriscono la complessità e aumentano la difficoltà di ottenere informazioni accurate sulla proprietà effettiva. Inoltre, la Società deve essere consapevole della possibilità che esistano accordi di nominee in cui amici, familiari o associati dichiarano di essere i BO di persone giuridiche, accordi legali o altre imprese.

Pertanto, la Società deve adottare misure appropriate e adeguate per determinare i veri BO e identificare le situazioni in cui la proprietà effettiva viene oscurata.

Nel determinare la BO, la Società deve raccogliere dati sulla struttura proprietaria del Cliente e verificarli sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente. In caso di proprietà a più livelli, lo schema della struttura proprietaria deve essere redatto dal Cliente o ottenuto da quest'ultimo.

La Società deve anche assicurarsi di comprendere la struttura proprietaria e di controllo del Cliente, soprattutto se la struttura proprietaria e di controllo è complessa (ad esempio, gli azionisti provengono da più giurisdizioni diverse; gli azionisti sono di diverse entità giuridiche/disposizioni giuridiche, ci sono trust e veicoli di investimento privati all'interno della struttura proprietaria e di controllo, il Cliente ha emesso azioni al portatore). La Società deve valutare se la struttura proprietaria e di controllo ha senso dal punto di vista commerciale, economico o legale.

Utilizzo del sistema informativo dei partecipanti persone giuridiche

Per l'identificazione di un Proprietario Beneficiario, la Società deve inoltre utilizzare il Sistema

Informativo dei Partecipanti alle Persone Giuridiche (JADIS) da cui ottenere i dati relativi ai Proprietari Beneficiari deiIl cliente ha il diritto di utilizzare altri sistemi informativi e registri statali in cui sono raccolti i dati dei partecipanti alle persone giuridiche.

È possibile accedere a JADIS attraverso il Centro dei registri delle imprese statali lituane (SECR) mediante l'apposita applicazione. La domanda può essere presentata:

- elettronicamente attraverso il sistema self-service del Centro dei Registri;
- via e-mail info@registrucentras.lt che deve essere firmato con firma elettronica;
- presso gli Uffici del Servizio Clienti del Centro dei Registri, presentando l'originale.

Gli estratti JADIS preparati e le copie dei documenti possono essere:

- scaricato dal self-service del Centro dei registri (solo se la domanda è stata presentata tramite il self-service del Centro dei registri);
- ritirati presso gli uffici del servizio clienti del Centro dei registri;
- ricevuto per posta all'indirizzo indicato dal cliente.

Una volta accertata la discrepanza tra le informazioni sui Titolari effettivi del Cliente persona giuridica disponibili in JADIS e le informazioni sui Titolari effettivi dello stesso cliente a loro disposizione, ne danno comunicazione al Cliente e propongono di fornire informazioni accurate sui suoi Titolari effettivi all'elaboratore di dati di JADIS.

La Società non avvierà un Rapporto d'affari o eseguirà una transazione (ad eccezione delle operazioni monetarie o delle transazioni concluse e/o eseguite nel corso di un Rapporto d'affari), quando le informazioni sui Titolari effettivi del Cliente che è una persona giuridica non sono fornite in JADIS o quando le informazioni sui Titolari effettivi del Cliente che è una persona giuridica, fornite in JADIS, sono errate.

Identificazione della persona politica esposta

La Società adotterà misure per accertare se il Cliente, il Proprietario Beneficiario del Cliente o il rappresentante di questo Cliente è una PEP, un suo familiare[19] o uno stretto collaboratore[20] o se il Cliente è diventato una tale persona.

La Società richiederà al Cliente informazioni per identificare se il Cliente è una PEP, un suo familiare o un suo stretto collaboratore (ad esempio, fornendo al Cliente l'opportunità di specificare le informazioni pertinenti al momento della raccolta dei dati sul Cliente).

La Società verificherà i dati ricevuti dal Cliente effettuando ricerche nelle banche dati pertinenti o nelle banche dati pubbliche o effettuando ricerche o verificando i dati sui siti web delle autorità di vigilanza o delle istituzioni competenti del paese in cui il Cliente ha la residenza o la sede. La PEP deve essere inoltre verificata utilizzando un motore di ricerca internazionale (ad esempio Google) e il motore di ricerca locale del paese di origine del Cliente, se presente, inserendo il nome del Cliente in alfabeto latino e locale con la data di nascita del Cliente.

Inoltre, lo screening dello status di PEP è implementato ed eseguito dalla soluzione antiriciclaggio automatizzata Sum & Substance. La soluzione fornisce una revisione continua dello status di PEP ed esegue l'identificazione dei membri della famiglia e degli stretti collaboratori di PEP.

Almeno le seguenti persone sono considerate PEP:

- il capo dello Stato, il capo del governo, un ministro, un viceministro o un viceministro, un segretario di Stato, un cancelliere del parlamento, del governo o di un ministero;
- un membro del Parlamento;
- un membro della Corte Suprema, della Corte Costituzionale o di qualsiasi altra autorità giudiziaria suprema le cui decisioni non sono soggette ad appello;
- un sindaco del comune, un capo dell'amministrazione comunale;
- un membro dell'organo di gestione dell'istituzione suprema di revisione o controllo statale, o un presidente, un vicepresidente o un membro del consiglio della banca centrale;
- ambasciatori di Stati esteri, un incaricato d'affari ad interim, il capo delle forze armate lituane, il comandante delle forze armate e delle unità, il capo dello staff della difesa o un alto ufficiale delle forze armate straniere;
- un membro dell'organo di gestione o di vigilanza di un'impresa pubblica, di una società per azioni o di una società a responsabilità limitata, le cui azioni o parte di esse, che detengono più di 1/2 dei voti totali all'assemblea generale degli azionisti di tali società, sono di proprietà dello Stato;

[19] per **familiare** si intende il coniuge, la persona con cui è stata registrata l'unione (cioè il convivente), i genitori, i fratelli, le sorelle, i figli e i coniugi dei figli,
conviventi dei figli

[20] per **stretto collaboratore** si intende una persona fisica che, insieme alla PEP, è membro della stessa entità giuridica o di un ente privo di personalità giuridica o intrattiene altri rapporti d'affari; oppure una persona fisica che è l'unico Proprietario effettivo dell'entità giuridica o di un ente privo di personalità giuridica costituito o operante di fatto allo scopo di acquisire proprietà o altri vantaggi personali per la PEP.

- un membro dell'organo di gestione o di vigilanza di un'impresa municipale, di una società per azioni o di una società a responsabilità limitata le cui azioni o parte di esse, che detengono più di 1/2 dei voti totali all'assemblea generale degli azionisti di tali società, sono di proprietà dello Stato e che sono considerate grandi imprese ai sensi della Legge sui bilanci degli enti della Repubblica di Lituania;
- un direttore, un vicedirettore o un membro dell'organo di gestione o di vigilanza di un'organizzazione intergovernativa internazionale;
- un leader, un vice leader o un membro dell'organo direttivo di un partito politico.

La Società identificherà gli stretti collaboratori e i familiari delle PEP solo se il loro legame con la PEP è noto al pubblico o se la Società ha motivo di credere che tale legame esista.

Nel caso in cui a un PEP non sia più affidata una Funzione Pubblica Preminente, la Società dovrà, entro 12 mesi dalla data di dimissioni del PEP dalle funzioni pubbliche, prendere in considerazione i rischi che rimangono legati al Cliente. Dopo un periodo di 12 mesi dalla data di dimissioni della PEP dalle funzioni pubbliche, la Società è tenuta a rivalutare i rischi associati a tale cliente.

Identificazione dello scopo e della natura del rapporto commerciale o della transazione

La Società deve comprendere lo scopo e la natura dell'instaurazione del rapporto commerciale o dell'esecuzione della transazione. Per quanto riguarda i servizi forniti, la Società può richiedere al Cliente le seguenti informazioni per comprendere lo scopo e la natura del rapporto commerciale o della transazione:

- se il Cliente utilizzerà i servizi della Società per le proprie esigenze o se rappresenterà gli interessi di un'altra persona;
- informazioni di contatto;
- informazioni sull'indirizzo registrato e sull'indirizzo effettivo di residenza del Cliente;
- il fatturato stimato delle transazioni con la Società per anno solare;
- la fonte stimata dei fondi utilizzati nella Relazione d'affari o nella transazione;
- se il Rapporto d'affari o la transazione sono legati allo svolgimento di attività economiche o professionali da parte del Cliente e di quali attività si tratta;
- informazioni sulla fonte dei fondi relativi al Rapporto d'affari o alla transazione, se l'importo delle transazioni (compreso l'importo previsto) supera il limite stabilito.

La Società applicherà misure aggiuntive e raccoglierà informazioni aggiuntive per identificare lo scopo e la natura della Relazione Commerciale nei casi in cui:

- c'è una situazione che si riferisce a un valore elevato o è insolita e/o
- qualora il rischio e/o il profilo di rischio associato al Cliente e la natura del Rapporto d'Affari giustifichino l'esecuzione di azioni aggiuntive al fine di poter monitorare adeguatamente il Rapporto d'Affari.

Se il Cliente è una persona giuridica, oltre a quanto sopra, la Società dovrà identificare il **settore di attività** del Cliente, dove la Società dovrà comprendere ciò che il Cliente tratta e intende trattare nel corso del Rapporto d'affari e come questo corrisponde allo scopo e alla natura del Rapporto d'affari in generale e se è ragionevole, comprensibile e plausibile.

L'area di attività deve rientrare nel profilo di esperienza del rappresentante del Cliente (o delle persone chiave) e/o del Proprietario Beneficiario. Pertanto, la Società deve identificare la capacità, l'abilità, le competenze e le conoscenze (l'esperienza in generale) del rappresentante e/o del Proprietario Beneficiario per operare in questo settore di attività, con questi volumi di affari e con questi principali partner commerciali.

Monitoraggio della relazione commerciale

La Società monitorerà le Relazioni d'affari consolidate in cui vengono attuate le seguenti misure di due diligence (periodica):

- garantire che i documenti, i dati o le informazioni raccolti nel corso dell'applicazione delle misure di due diligence siano aggiornati regolarmente e in caso di eventi scatenanti, ossia principalmente i dati relativi al Cliente, al suo rappresentante (incluso il diritto di rappresentanza) e al Proprietario Beneficiario, nonché lo scopo e la natura del Rapporto d'Affari;
- monitoraggio continuo del rapporto commerciale, che riguarda le transazioni effettuate nel rapporto commerciale per garantire che le transazioni corrispondano alla conoscenza che la Società ha del Cliente, delle sue attività e del suo profilo di rischio;
- l'identificazione della fonte e dell'origine dei fondi utilizzati nelle operazioni.

La Società dovrà **verificare e aggiornare** regolarmente **i documenti, i dati e le informazioni** raccolte nel corso dell'attuazione delle misure di CDD e aggiornare il profilo di rischio del Cliente. La regolarità dei controlli e degli aggiornamenti deve essere basata sul profilo di rischio del Cliente e i controlli devono avvenire almeno:

- una volta a cadenza semestrale per il Cliente con profilo ad alto rischio;
- una volta all'anno per il Cliente con profilo di rischio medio;
- una volta ogni due anni per il Cliente con profilo a basso rischio.

La Società ha implementato un sistema di archiviazione, sistematizzazione e controllo dei documenti dei Clienti. Il sistema segnala automaticamente al dipendente responsabile la necessità di richiedere un documento aggiornato in base al profilo di rischio del Cliente. Il sistema prevede anche il controllo delle date di scadenza e invia una notifica se il documento d'identità/prova d'indirizzo del Cliente è prossimo alla scadenza.

I documenti, i dati e le informazioni raccolti devono essere controllati anche se si è verificato un evento che indica la necessità di aggiornare i documenti, i dati e le informazioni raccolti.

Nel corso del **monitoraggio continuo del Rapporto d'affari**, la Società controllerà le transazioni concluse nel corso del Rapporto d'affari in modo tale da poter determinare se le transazioni da concludere corrispondono alle informazioni precedentemente note sul Cliente (vale a dire, ciò che il Cliente ha dichiarato al momento dell'instaurazione del Rapporto d'affari o ciò che è diventato noto nel corso del Rapporto d'affari).

La Società monitorerà inoltre la Relazione d'Affari per accertare le attività del Cliente o i fatti che indicano attività criminali, riciclaggio di denaro o finanziamento del terrorismo o la cui relazione con il riciclaggio di denaro o il finanziamento del terrorismo è probabile, comprese le transazioni complicate, di valore elevato e insolite e gli schemi di transazione che non hanno alcuno scopo economico o legittimo ragionevole o ovvio o che non sono caratteristici delle caratteristiche specifiche dell'attività in questione. Nel corso della Relazione d'affari, l'Azienda valuterà costantemente il
cambiamenti nelle attività del Cliente e valutare se tali cambiamenti possono aumentare il livello di rischio associato al Cliente e al Rapporto d'affari, dando luogo alla necessità di applicare misure EDD.

Nel corso del monitoraggio continuo della Relazione d'affari, la Società applica le seguenti misure:

- screening, cioè il monitoraggio delle transazioni in tempo reale;
- il monitoraggio, cioè l'analisi successiva

delle transazioni. L'obiettivo dello **screening** è

quello di identificare:

- transazioni sospette e insolite e modelli di transazione;
- transazioni che superano le soglie previste;
- persone politicamente esposte e circostanze relative alle sanzioni.

Lo screening delle transazioni viene effettuato automaticamente e comprende le seguenti misure:

- soglie stabilite per le transazioni del Cliente, a seconda del profilo di rischio del Cliente e del fatturato stimato delle transazioni dichiarato dal Cliente;
- l'assegnazione di portafogli di Moneta Virtuale dove la Moneta Virtuale sarà inviata in conformità all'ordine del Cliente;
- il punteggio dei portafogli di Valuta Virtuale da cui viene ricevuta la Valuta Virtuale.

Se il Cliente ordina una transazione che supera la soglia stabilita o una transazione verso un portafoglio di valuta virtuale con un punteggio di rischio elevato (ad esempio, portafogli legati a frodi, crimini, ecc.), la transazione sarà approvata manualmente dal Dipendente, che valuterà, prima dell'approvazione, la necessità di applicare eventuali misure CDD aggiuntive (ad esempio, l'applicazione di misure EDD, la richiesta della fonte e dell'origine dei fondi o la richiesta di informazioni aggiuntive sulla transazione).

Nel **monitorare le transazioni** il Dipendente deve valutare le transazioni al fine di individuare attività e transazioni che:

- si discostano da quanto è ragionevole aspettarsi in base alle misure di CDD eseguite, ai servizi forniti, alle informazioni fornite dal Cliente e ad altre circostanze (ad esempio, superamento del fatturato stimato delle transazioni, invio di Valuta Virtuale ogni volta a un nuovo portafoglio di Valuta Virtuale, volume di transazioni superiore al limite);
- senza che ciò possa essere derogato dalla clausola precedente, si può ritenere che facciano parte di un'operazione di riciclaggio di denaro o di finanziamento del terrorismo;
- possono influire sul punteggio del profilo di rischio del cliente.

Nel caso in cui venga rilevato il fatto di cui sopra, il Dipendente dovrà informare MLRO e rimandare qualsiasi transazione del Cliente fino alla decisione di MLRO in merito.
Oltre a quanto sopra, l'MLRO deve esaminare regolarmente (almeno una volta alla settimana) le transazioni della Società per garantire che:

- i Dipendenti della Società hanno eseguito correttamente i suddetti obblighi;
- non vi sono transazioni e schemi di transazione complicati, di valore elevato e inusuali, che non abbiano uno scopo economico o legittimo ragionevole o ovvio o che non siano caratteristici delle caratteristiche specifiche.

La Società **identifica la fonte[21] e l'origine[22] dei fondi** utilizzati nelle transazioni, se necessario. La necessità di identificare la fonte e l'origine dei fondi dipende dalle precedenti attività del Cliente e da altre informazioni note. Pertanto, l'identificazione della fonte e dell'origine dei fondi utilizzati nella transazione sarà effettuata nei seguenti casi:

- le operazioni superano i limiti stabiliti dalla Società;
- le transazioni non corrispondono alle informazioni precedentemente note sul Cliente;
- la Società vuole o dovrebbe ragionevolmente ritenere necessario valutare se le transazioni corrispondono alle informazioni precedentemente note sul Cliente;
- la Società sospetta che le transazioni indichino attività criminali, riciclaggio di denaro o finanziamento del terrorismo o che la relazione delle transazioni con il riciclaggio di denaro o il finanziamento del terrorismo sia probabile, incluse transazioni complicate, di valore elevato e insolite e schemi di transazioni che non hanno alcuno scopo economico o legittimo ragionevole o ovvio o che non sono caratteristici delle caratteristiche specifiche dell'attività in questione.

ATTUAZIONE DELLE SANZIONI

Al momento dell'entrata in vigore, della modifica o della cessazione delle Sanzioni, la Società verificherà se il Cliente, il suo Proprietario Beneficiario o una persona che intende intrattenere il Rapporto d'affari o la transazione con lui è soggetto a Sanzioni. Se la Società identifica una persona soggetta a sanzioni o che la transazione prevista o effettuata da tale persona è in violazione delle sanzioni, la Società applicherà le sanzioni e ne informerà il FCIS entro 3 ore.

Procedura per l'identificazione dell'oggetto delle sanzioni e di una transazione che viola le sanzioni

La Società utilizzerà almeno le seguenti fonti (banche dati) per verificare la relazione del Cliente con le Sanzioni:

- Un elenco consolidato delle sanzioni dell'UE;
- Un elenco consolidato delle sanzioni delle Nazioni Unite
- Ufficio per il controllo delle attività estere (OFAC).

Oltre alle fonti sopra citate, la Società può utilizzare qualsiasi altra fonte su decisione del Dipendente che applica le misure di CDD.

[21] **la fonte dei fondi** utilizzati nella transazione è il motivo, la spiegazione e la base (rapporto giuridico e suo contenuto) per cui i fondi sono stati trasferiti

[22] **l'origine dei fondi** utilizzati nella transazione è l'attività con la quale i fondi sono stati guadagnati o ricevuti

Per verificare che i nomi delle persone risultanti dall'indagine siano gli stessi delle persone elencate in una notifica contenente una o più sanzioni, si utilizzeranno i loro dati personali, le cui caratteristiche principali sono, per una persona giuridica, la denominazione o il marchio, il codice di registrazione o la data di registrazione, e per una persona fisica, il nome e l'identificazione personale o la data di nascita.

Al fine di stabilire l'identità delle persone indicate nell'atto giuridico o nella comunicazione in questione, che sono le stesse identificate a seguito dell'interrogazione delle banche dati, la Società deve analizzare i nomi delle persone trovate a seguito dell'interrogazione in base al possibile effetto di fattori che distorcono i dati personali (ad es. trascrizione di nomi stranieri, ordine diverso delle parole, sostituzione di diacritici o doppie lettere, ecc.)

La Società effettuerà le suddette verifiche su base continuativa nel corso di un rapporto commerciale consolidato. La frequenza delle verifiche continue dipende dal profilo di rischio del Cliente:

- una volta alla settimana per il cliente con profilo ad alto rischio;
- una volta al mese per il Cliente con profilo a medio rischio;
- una volta al trimestre per il Cliente con profilo a basso rischio.

Se il Dipendente ha il dubbio che una persona sia soggetta a sanzioni, deve informare immediatamente l'MLRO o il membro del Consiglio di amministrazione. In questo caso, l'MLRO o il membro del Consiglio di amministrazione decideranno se chiedere o acquisire ulteriori dati dalla persona o se notificare immediatamente al FCIS il loro sospetto.

La Società dovrà in primo luogo acquisire autonomamente ulteriori informazioni sulla persona che è in Relazione d'Affari o che sta eseguendo una transazione con essa, nonché sulla persona che intende instaurare la Relazione d'Affari, eseguire una transazione o un atto con essa, preferendo informazioni provenienti da una fonte credibile e indipendente. Se, per qualche motivo, tali informazioni non sono disponibili, la Società chiederà alla persona che è in Relazione d'affari o che sta eseguendo una transazione o un atto con essa, nonché alla persona che intende stabilire una Relazione d'affari, eseguire una transazione o un atto con essa, se le informazioni provengono da una fonte credibile e indipendente e valuterà la risposta.

Azioni da intraprendere quando si identifica l'oggetto delle sanzioni o una transazione che viola le sanzioni

Se il dipendente della Società viene a conoscenza del fatto che il cliente che è in rapporto d'affari o sta eseguendo una transazione con la Società, così come una persona che intende stabilire il rapporto d'affari o eseguire una transazione con la Società, è oggetto di sanzioni, il dipendente dovrà immediatamente informare l'MLRO o il membro del Consiglio di amministrazione, circa l'identificazione del soggetto delle sanzioni, del dubbio su di esso e delle misure adottate.

L'MLRO o il membro del consiglio di amministrazione rifiutano di concludere un'operazione o un procedimento, adottano le misure previste dall'atto sull'imposizione o l'attuazione delle sanzioni e comunicano immediatamente all'FCIS i loro dubbi e le misure adottate.

Quando si identifica il soggetto delle sanzioni, è necessario identificare le misure adottate per sanzionare questa persona. Tali misure sono descritte nell'atto giuridico che attua la legge

Le sanzioni, quindi, sono necessarie per identificare l'esatta sanzione che viene applicata alla persona per garantire un'applicazione legale e corretta delle misure.

RIFIUTO DELLA TRANSAZIONE O DEL RAPPORTO COMMERCIALE E LA LORO CESSAZIONE

Alla Società è vietato instaurare un Rapporto d'affari e il Rapporto d'affari o la transazione instaurati saranno interrotti (a meno che non sia oggettivamente impossibile farlo) nel caso in cui:

- la Società sospetta un riciclaggio di denaro o un finanziamento del terrorismo;
- è impossibile per la Società applicare le misure di CDD, perché il Cliente non presenta i dati rilevanti o si rifiuta di presentarli o i dati presentati non danno la certezza che i dati raccolti siano adeguati;
- il Cliente il cui capitale è costituito da azioni al portatore o da altri titoli al portatore desidera instaurare il Rapporto d'affari;
- il Cliente, che è una persona fisica dietro la quale si cela un'altra persona, effettivamente beneficiaria, vuole instaurare il rapporto commerciale (sospetto che venga utilizzata una persona che funge da prestanome);
- il profilo di rischio del Cliente è diventato inadeguato rispetto alla propensione al rischio dell'Azienda (ovvero il livello del profilo di rischio del Cliente è "vietato").

In caso di cessazione del Rapporto d'affari ai sensi del presente capitolo, la Società trasferirà i beni del Cliente entro un termine ragionevole, ma preferibilmente non oltre un mese dalla cessazione, su un conto aperto presso un istituto di credito registrato o la cui sede operativa si trovi in uno Stato contraente dello Spazio economico europeo o in un paese in cui si applichino requisiti pari a quelli stabiliti nelle direttive pertinenti del Parlamento europeo e del Consiglio. In casi eccezionali, il patrimonio può essere trasferito su un conto diverso da quello del Cliente o emesso in contanti. Indipendentemente dal destinatario dei fondi, l'informazione minima fornita in inglese nei dettagli di pagamento del trasferimento del patrimonio del Cliente è che il trasferimento è legato alla cessazione straordinaria del rapporto con il Cliente.

OBBLIGO DI SEGNALAZIONE

La Società deve sospendere l'operazione a prescindere dall'importo della stessa (salvo i casi in cui ciò sia oggettivamente impossibile per la natura dell'Operazione Monetaria o della transazione, per le modalità di esecuzione della stessa o per altre circostanze) e tramite il proprio MLRO deve segnalare al FCIS l'attività o le circostanze che individua nel corso delle attività economiche e con le quali:

- la Società ha stabilito che il Cliente sta effettuando una transazione sospetta;

- la Società sa o sospetta che beni di qualsiasi valore siano stati ottenuti direttamente o indirettamente da attività criminali o dalla partecipazione a tali attività.

Le caratteristiche minime delle transazioni sospette sono indicate nelle linee guida del FCIS (uno degli allegati delle presenti Linee guida).

Le segnalazioni di cui sopra devono essere effettuate prima del completamento della transazione se la Società sospetta o è a conoscenza della commissione di reati di Riciclaggio o di Finanziamento del Terrorismo o di reati correlati e se tali circostanze vengono identificate prima del completamento della transazione.

Nel caso in cui si renda necessaria la segnalazione di cui sopra, il Dipendente che ne è venuto a conoscenza deve darne immediata comunicazione all'MLRO.

In ogni caso (cioè anche nel caso in cui un'attività o una circostanza venga identificata dopo il completamento della transazione), **l'obbligo di segnalazione per le suddette segnalazioni deve essere assolto immediatamente, ma non oltre le tre ore lavorative** successive all'identificazione dell'attività o della circostanza o all'emergere del sospetto effettivo (cioè la situazione in cui il sospetto non può essere dissipato).

Obbligo di segnalazione di specifiche tipologie di transazioni

La Società, tramite il proprio MLRO, deve inviare informazioni al FCIS entro e non oltre 7 giorni lavorativi dall'identificazione di operazioni di cambio di Valuta Virtuale o di transazioni in Valuta Virtuale, se il valore giornaliero di tali operazioni è pari o superiore a 15.000 euro o all'importo equivalente in valuta estera o in Valuta Virtuale, indipendentemente dal fatto che l'operazione sia conclusa in una o più transazioni monetarie correlate.

Nel caso specificato sopra, le informazioni presentate al FCIS devono includere:

- i dati che confermano l'identità del Cliente e, nel caso in cui la transazione sia effettuata tramite un rappresentante, anche i dati che confermano l'identità del rappresentante;
- l'importo della transazione;
- la valuta in cui è stata eseguita la transazione;
- la data di esecuzione della transazione;
- le modalità di esecuzione dell'Operazione Monetaria;
- l'entità a beneficio della quale è stata eseguita l'Operazione monetaria (se possibile);
- altri dati specificati nelle relative istruzioni del FCIS.

Tutti i rapporti descritti nel presente capitolo devono essere inviati in conformità con le linee guida della Società in materia di rapporti attraverso un canale sicuro che garantisca la piena riservatezza (uno degli allegati delle presenti Linee guida).

Alla Società, a un'unità strutturale della Società, a un membro del Consiglio di amministrazione, all'MLRO e al Dipendente è vietato informare una persona, il suo Proprietario effettivo, un rappresentante o un terzo in merito a una segnalazione presentata su di loro al FCIS, a un piano per la presentazione di tale segnalazione o al verificarsi di una situazione di conflitto di interessi.

di segnalazione, nonché su un precetto emesso dall'FCIS o sull'avvio di un procedimento penale.

OBBLIGO DI FORMAZIONE

L'Azienda si assicura che i suoi Dipendenti, i suoi appaltatori e le altre persone che partecipano all'attività su base simile e che svolgono mansioni lavorative importanti per prevenire l'uso dell'attività dell'Azienda per il riciclaggio di denaro o il finanziamento del terrorismo ("Soggetti Rilevanti") abbiano le qualifiche necessarie per tali mansioni lavorative. Quando un Soggetto Rilevante viene assunto, le sue qualifiche vengono verificate nell'ambito del processo di assunzione/nomina mediante l'esecuzione di un controllo dei precedenti, documentato mediante un apposito modulo standard di valutazione dell'idoneità dei dipendenti.

In conformità ai requisiti applicabili alla Società per garantire l'idoneità dei Soggetti Rilevanti, la Società si assicura che tali persone ricevano costantemente una formazione e un'informazione adeguate per essere in grado di adempiere agli obblighi della Società in conformità alla legislazione applicabile. Attraverso la formazione si assicura che tali persone siano informate in materia di antiriciclaggio e di lotta al finanziamento del terrorismo in misura adeguata alle loro mansioni e funzioni. La formazione deve fornire, innanzitutto, informazioni su tutti i più moderni metodi di riciclaggio e di finanziamento del terrorismo e sui rischi che ne derivano.

Questa formazione fa riferimento a parti rilevanti del contenuto delle norme e dei regolamenti applicabili, alla valutazione del rischio della Società, alle Linee guida e alle procedure della Società e alle informazioni che dovrebbero facilitare ai Soggetti rilevanti l'individuazione di sospetti di riciclaggio di denaro e di finanziamento del terrorismo. La formazione è strutturata sulla base dei rischi identificati attraverso la politica di valutazione dei rischi.

Il contenuto e la frequenza della formazione sono adattati ai compiti e alle funzioni della persona su questioni relative alle misure di prevenzione del riciclaggio e del finanziamento del terrorismo. Se le Linee guida vengono aggiornate o modificate in qualche modo, il contenuto e la frequenza della formazione vengono adeguati di conseguenza.

Per i nuovi dipendenti, la formazione comprende una revisione del contenuto delle norme e dei regolamenti applicabili, della politica di valutazione dei rischi della Società, delle presenti Linee guida e di altre procedure pertinenti.

I dipendenti e i membri del Consiglio di gestione ricevono una formazione continua sotto l'egida dell'MLRO, secondo il seguente piano di formazione:

- periodicità: almeno una volta all'anno per i membri del Consiglio di amministrazione. Almeno una volta all'anno per i Dipendenti e i Soggetti Rilevanti della Società.
- ambito: revisione delle norme e dei regolamenti applicabili, delle Linee guida della Società e di altre procedure pertinenti. Informazioni specifiche relative alle novità/aggiornamenti delle norme e dei regolamenti applicabili. Relazione e scambio di esperienze relative alle operazioni esaminate dopo la formazione precedente.

Oltre a quanto sopra, i Soggetti Rilevanti sono costantemente informati sulle nuove tendenze, modelli e metodi e ricevono altre informazioni rilevanti per la prevenzione del riciclaggio di denaro e del finanziamento del terrorismo.

La formazione svolta deve essere documentata elettronicamente e confermata con la firma della persona rilevante. La documentazione deve includere il contenuto della formazione, i nomi dei partecipanti e la data della formazione.

RACCOLTA E ARCHIVIAZIONE DI DATI, DIARI DI BORDO

La Società, tramite la persona (compresi i dipendenti, i membri del Consiglio di gestione e l'MLRO) che per prima riceve le informazioni o i documenti pertinenti, registra e conserva i seguenti dati:

- tutti i dati raccolti nell'ambito dell'attuazione delle misure CDD;
- informazioni sulle circostanze del rifiuto dell'instaurazione del rapporto commerciale da parte della Società;
- le circostanze del rifiuto di instaurare un rapporto commerciale su iniziativa del Cliente, se il rifiuto è legato all'applicazione di misure CDD da parte della Società;
- informazioni su tutte le operazioni effettuate per identificare la persona che partecipa alla transazione o il Beneficiario del Cliente;
- informazioni se non è possibile eseguire le misure delCDD;
- informazioni sulle circostanze di cessazione del rapporto commerciale in relazione all'impossibilità di applicare le misure CDD
- la data o il periodo di ciascuna transazione e una descrizione del contenuto della transazione, compresi l'importo della transazione, la valuta e il numero di conto o un altro identificatore (compreso l'hash delle transazioni in valuta virtuale e dei portafogli di valuta virtuale relativi alla transazione);
- informazioni che servono come base per gli obblighi di segnalazione specificati nelle Linee guida;
- dati di transazioni o circostanze sospette o insolite di cui il FCIS non è stato informato (ad esempio, transazioni complesse o insolitamente grandi, transazioni condotte in modo insolito e transazioni che non hanno un apparente scopo economico o lecito, rapporti commerciali o operazioni monetarie con clienti di Paesi terzi in cui le misure di prevenzione del riciclaggio di denaro e/o del finanziamento del terrorismo sono insufficienti o non soddisfano gli standard internazionali secondo le informazioni pubblicate ufficialmente da organizzazioni intergovernative internazionali).

Alcuni dei dati sopra specificati saranno inseriti nel registro (come descritto di seguito) in ordine cronologico sulla base dei documenti che confermano un'operazione o una transazione monetaria o di altri documenti legalmente validi relativi all'esecuzione di operazioni o transazioni monetarie, immediatamente, ma non più tardi di 3 giorni lavorativi dopo l'esecuzione di un'operazione o transazione monetaria.

I dati sopra indicati dovranno essere conservati per 8 anni dopo la scadenza del rapporto commerciale o dell'operazione di completamento. I dati relativi all'adempimento dell'obbligo di comunicazione devono essere conservati per 5 anni dall'adempimento dell'obbligo di comunicazione. Il

La corrispondenza di un rapporto commerciale con il Cliente deve essere conservata per 5 anni dalla data di cessazione delle transazioni o del rapporto commerciale.

I documenti e i dati devono essere conservati in modo da consentire una risposta esaustiva e immediata alle richieste del FCIS o, in base alla normativa, di altre autorità di vigilanza, di indagine o del tribunale.

La Società attua tutte le norme di protezione dei dati personali in applicazione dei requisiti derivanti dalla legge applicabile. La Società è autorizzata a trattare i dati personali raccolti nell'ambito dell'attuazione della CDD solo per prevenire il riciclaggio di denaro e il finanziamento del terrorismo e i dati non devono essere ulteriormente trattati in modo non conforme allo scopo, ad esempio per scopi di marketing.

La Società cancella i dati conservati dopo la scadenza del periodo di tempo, a meno che la legislazione che regola il settore pertinente non stabilisca una procedura diversa. Sulla base di una disposizione dell'autorità di vigilanza competente, i dati importanti per la prevenzione, l'individuazione o l'investigazione del riciclaggio di denaro o del finanziamento del terrorismo possono essere conservati per un periodo più lungo, ma non per più di due anni dopo la scadenza del primo periodo di tempo.

Tenuta dei registri di registrazione

Ai fini dell'adempimento degli obblighi antiriciclaggio, la Società dovrà tenere (compilare) i seguenti registri di registrazione delle Operazioni e transazioni monetarie (di seguito - registri):

- registro dei clienti che eseguono transazioni in Valuta Virtuale, indipendentemente dal fatto che le transazioni siano eseguite occasionalmente o nel corso del rapporto commerciale;
- registro delle operazioni monetarie o delle transazioni effettuate tra il Cliente e la Società prima che la Società sia obbligata ad applicare misure di CDD;
- registro delle segnalazioni[23] e delle transazioni monetarie sospette;
- registro dei Clienti con i quali sono state rifiutate o interrotte operazioni o Rapporti d'affari in circostanze legate a violazioni della procedura di prevenzione del Riciclaggio e/o del Finanziamento del Terrorismo.

Il registro di registrazione dei clienti che effettuano transazioni in valuta virtuale deve includere quanto segue:

- dati che confermano l'identità del Cliente e del suo rappresentante (se la transazione monetaria viene eseguita o conclusa tramite un rappresentante): nome e cognome di una persona fisica, codice di identificazione personale (data di nascita di un Cliente straniero), cittadinanza; codice personale, se tale codice è previsto;
- nel caso di transazioni in Valuta Virtuale o di transazioni per le quali non è oggettivamente possibile identificare il beneficiario, altre informazioni che consentano di identificare l'indirizzo della Valuta Virtuale.

[23] come descritto nel relativo capitolo delle presenti Linee guida

legati all'identità del proprietario della valuta virtuale: indirizzo di protocollo Internet (IP), indirizzo e-mail, ecc;

- Indirizzo/i di valuta virtuale relativo/i alla transazione e hash della transazione;
- metodo di transazione: deposito o prelievo di Valuta Virtuale, la Valuta Virtuale viene scambiata con denaro o viceversa, la Valuta Virtuale viene scambiata con altra Valuta Virtuale, la transazione di scambio di Valuta Virtuale è stata mediata (scambio p2p);

Il registro di registrazione delle operazioni monetarie o delle transazioni effettuate tra il Cliente e la Società prima del momento in cui la Società è tenuta ad applicare le misure di CDD deve includere quanto segue:

- dati che confermano l'identità del Cliente e del suo rappresentante (se la transazione monetaria viene eseguita o conclusa tramite un rappresentante): nome e cognome di una persona fisica, codice di identificazione personale (data di nascita di un Cliente straniero), cittadinanza; codice personale, se tale codice è previsto;
- dati relativi alla transazione monetaria o alla transazione: la data della transazione, la descrizione dei beni oggetto della transazione (contanti, immobili, Valuta Virtuale, ecc.) e il relativo valore (importo del denaro, valuta in cui viene effettuata la transazione monetaria o la transazione, valore di mercato dei beni, ecc;)
- metodo di transazione: La Valuta virtuale viene scambiata con denaro o viceversa, il Cliente ha effettuato un pagamento anticipato per l'acquisto di Valuta virtuale, ecc.

Il registro di registrazione delle segnalazioni, delle operazioni monetarie e delle transazioni sospette deve includere, in ordine cronologico, quanto segue:

- dati che confermano l'identità del Cliente e del suo rappresentante (se la transazione monetaria viene eseguita o conclusa tramite un rappresentante): nome e cognome di una persona fisica, codice di identificazione personale (data di nascita di un Cliente straniero), cittadinanza; codice personale, se tale codice è previsto;
- il criterio approvato dal Ministero degli Interni della Repubblica di Lituania, in base al quale si riconosce che la transazione monetaria o la transazione del Cliente è considerata sospetta, la transazione o la transazione è conforme a;
- Modalità di completamento dell'operazione o transazione monetaria sospetta;
- Data e ora dell'operazione monetaria o della transazione sospetta, caratterizzazione delle attività oggetto della transazione (contanti, ecc.) e relativo valore (importo del denaro, valuta utilizzata per condurre l'operazione monetaria o la transazione, valore di mercato delle attività);
- i dati relativi al/i beneficiario/i della transazione: nome e cognome e numero di identificazione personale di una persona fisica (in caso di straniero: data di nascita, se disponibile, numero di identificazione personale o qualsiasi altra sequenza univoca di simboli assegnata all'individuo in questione per l'identificazione personale), e in caso di persona giuridica, titolo, forma giuridica, indirizzo registrato e numero di registrazione, se assegnato;

- Dati di contatto del Cliente: numero/i di telefono, indirizzo/i e-mail, persona/e di contatto, relativi numeri di telefono, indirizzi e-mail, ecc;
- Descrizione dei beni che il Cliente non può controllare o utilizzare dal momento della sospensione della transazione monetaria o della transazione sospetta (luogo e altre informazioni che caratterizzano i beni);
- In caso di transazione monetaria sospetta o di transazione non sospesa, i motivi sono rilevanti;
- Metodi di gestione dei conti;
- Altri dettagli rilevanti, secondo la decisione del dipendente.

La Società inserirà nel registro di registrazione dei clienti, dove le transazioni o i rapporti commerciali sono stati interrotti, quanto segue, in ordine cronologico:

- dati che confermano l'identità del Cliente e del suo rappresentante (se la transazione monetaria viene eseguita o conclusa tramite un rappresentante): nome e cognome di una persona fisica, codice di identificazione personale (data di nascita di un Cliente straniero), cittadinanza; codice personale, se tale codice è previsto;
- dati sulla transazione monetaria o sulla transazione: la data della transazione, la descrizione dei beni oggetto della transazione (contanti, immobili, Valuta Virtuale, ecc.) e il suo valore (importo del denaro, valuta in cui viene effettuata la transazione monetaria o la transazione, valore di mercato dei beni, ecc;)
- nel caso di transazioni in Moneta Virtuale o di transazioni per le quali non è oggettivamente possibile identificare il beneficiario, altre informazioni che consentano di collegare l'indirizzo della Moneta Virtuale all'identità del proprietario della Moneta Virtuale: indirizzo del Protocollo Internet (IP), indirizzo e-mail, ecc;
- nel caso di transazioni in Valuta Virtuale Indirizzo/i di Valuta Virtuale relativo/i alla transazione e hash della transazione;
- i dati relativi al/i beneficiario/i del Cliente: nome e cognome e numero di identificazione personale di una persona fisica (in caso di straniero: data di nascita, se disponibile, numero di identificazione personale o qualsiasi altra sequenza unica di simboli assegnata all'individuo in questione per l'identificazione personale), e in caso di persona giuridica, titolo, forma giuridica, indirizzo registrato e numero di registrazione, se assegnato;
- Motivi di interruzione delle transazioni o dei rapporti commerciali relativi a violazioni della procedura di prevenzione del riciclaggio di denaro e/o del finanziamento del terrorismo.

Procedura per la tenuta e la gestione dei registri di immatricolazione

L'archiviazione dei dati di log deve essere completata e conservata su supporto elettronico dal membro del Consiglio di amministrazione, se è in viaggio di lavoro, o è altrimenti indisponibile per altri motivi validi, un altro Dipendente, come indicato nell'ordine speciale del direttore, che stabilisce l'ambito dei compiti e delle responsabilità assegnati a una persona che agisce come sostituto.

Il Consiglio di amministrazione nominerà un dipendente incaricato di garantire la protezione dei dati inclusi nei registri di registrazione, e trattati su supporto elettronico, dalla cancellazione, dall'alterazione o dall'uso non autorizzato da parte di terzi non autorizzati.

I dettagli devono essere archiviati utilizzando un software che consenta l'esportazione dei dettagli archiviati in Microsoft Office Excel, Word o un software equivalente a codice aperto, senza danneggiare l'integrità dei dettagli.

La tenuta dei registri di registrazione sarà verificata da un membro del Consiglio di amministrazione, in caso di viaggio di lavoro o di indisponibilità per altri validi motivi, da un altro dipendente responsabile nominato dalla Società, come indicato nell'apposito provvedimento del direttore, che definisce l'ambito dei compiti e delle responsabilità assegnati a una persona che funge da sostituto.

Ai Dipendenti della Società è vietato informare, o far sapere in altro modo, a qualsiasi Cliente o ad altri individui che le informazioni sulle Operazioni Monetarie in corso, o le transazioni condotte da un Cliente, o le indagini che ne derivano sono comunicate al FCIS.

CONTROLLO INTERNO DELL'ESECUZIONE DELLE LINEE GUIDA

L'esecuzione delle Linee guida sarà controllata internamente dal membro del Consiglio di amministrazione o dal dipendente nominato dal Consiglio di amministrazione per lo svolgimento delle funzioni pertinenti (di seguito nel presente capitolo - Preposto al controllo interno). Il Preposto al controllo interno deve disporre delle competenze, degli strumenti e dell'accesso alle informazioni rilevanti in tutte le unità strutturali della Società.

Il Preposto al controllo interno svolge funzioni di controllo interno almeno nei seguenti ambiti:

- la conformità della Società alla politica di valutazione del rischio e alla propensione al rischio stabilite;
- Attuazione delle misure CDD;
- attuazione delle sanzioni;
- l'obbligo della Società di rifiutare la transazione o il rapporto d'affari e la loro cessazione;
- l'obbligo di segnalazione della Società al FCIS;
- l'obbligo di formazione della Società in merito agli obblighi di prevenzione del riciclaggio e del finanziamento del terrorismo;
- gli obblighi della Società in materia di raccolta e conservazione dei dati.

Le misure esatte per l'esecuzione del controllo interno sono determinate dal Preposto al controllo interno e devono corrispondere alle dimensioni della Società e alla natura, alla portata e al livello di complessità delle attività e dei servizi forniti. Gli Uffici di controllo interno devono prendere in considerazione almeno i campi di esame sopra specificati. Le misure di controllo interno devono essere eseguite nel momento stabilito dal Preposto al controllo interno con la frequenza da lui stabilita, almeno una volta al mese, se la natura della misura non prevede espressamente altro.

I risultati dell'attuazione delle misure di controllo interno (di seguito nel presente capitolo - i Dati di controllo interno) saranno salvati separatamente dagli altri dati e conservati entro 5 anni. Solo i membri del Consiglio di amministrazione e il Preposto al controllo interno possono avere accesso ai dati di controllo interno.

Dati di controllo. Il Preposto al controllo interno può consentire l'accesso ai dati di controllo interno ad altri dipendenti o a terzi (ad esempio, consulenti, revisori, ecc.) solo previo consenso del Consiglio di amministrazione. Le persone che hanno accesso ai dati di controllo interno non devono rivelarli a nessuno senza il previo consenso del Consiglio di amministrazione.

I dati di controllo interno devono essere salvati in ordine cronologico con un formato che consenta di analizzarli e di collegarli in modo comprensibile ad altri dati rilevanti.

Il Preposto al controllo interno fornirà la relazione sul controllo interno al Consiglio di amministrazione con cadenza almeno trimestrale e all'assemblea generale degli azionisti della Società con cadenza almeno annuale. La relazione sul controllo interno deve includere almeno i seguenti elementi:

- periodo di esercizio del controllo interno;
- nome e posizione della persona che esegue il controllo interno;
- descrizione delle misure di controllo interno che sono state eseguite;
- risultati del controllo interno;
- conclusioni generali del controllo interno esercitato;
- carenze determinate, che sono state eliminate nel periodo di esercizio del controllo interno;
- carenze accertate, che non sono state eliminate alla fine del periodo di esercizio del controllo interno;
- misure che è necessario attuare per eliminare le carenze riscontrate.

Il Consiglio di amministrazione esamina il rapporto di controllo interno fornito e delibera in merito. L'essenza di tale delibera deve essere comunicata al Preposto al controllo interno in un formato che può essere riprodotto per iscritto. Per questo motivo, il Consiglio di amministrazione è tenuto a:

- analizzare i risultati del controllo interno effettuato;
- attuare azioni per eliminare le carenze riscontrate.

La Società deve riesaminare e, se necessario, aggiornare la procedura di controllo interno almeno annualmente e nei seguenti casi:

- a seguito della pubblicazione da parte della Commissione europea dei risultati di una valutazione del rischio di riciclaggio di denaro e di finanziamento del terrorismo a livello europeo (disponibile sul sito web della Commissione europea http://ec.europa.eu);
- dopo la pubblicazione dei risultati del National Money Laundering and Terrorist Financing Risk Assessment (pubblicato nella sezione "National Money Laundering and Terrorist Financing Risk Assessment" della sezione "Prevention of Money Laundering" del sito www.fntt.lt);
- al ricevimento di un'istruzione da parte del FCIS per rafforzare le procedure di controllo interno applicabili;

- in caso di eventi o cambiamenti significativi nella gestione e nelle operazioni dell'operatore del deposito di moneta virtuale e dell'operatore del cambio di moneta virtuale.

Valutazione del rischio e propensione al rischio

L'obiettivo dell'attuazione delle misure di controllo interno per la conformità della Società alla politica di valutazione del rischio stabilita (compresa la propensione al rischio stabilita) è l'esame delle seguenti circostanze:

- La Società stabilisce e utilizza un approccio basato sul rischio quando fornisce servizi ai Clienti (ad esempio, misure di CDD implementate in base al livello di rischio);
- La Società ha determinato i fattori che influenzano l'insorgere dei rischi di riciclaggio e di finanziamento del terrorismo e i fattori determinati sono rilevanti;
- La Società ha determinato e valutato il ML/TF di tutti i servizi da essa forniti;
- La Società compone il profilo di rischio del Cliente prima di eseguire le transazioni o di creare un rapporto d'affari;
- La Società aggiorna regolarmente il profilo di rischio del Cliente;
- L'azienda segue la propensione al rischio stabilita;
- L'azienda conserva le registrazioni di tutti gli incidenti in conformità con la politica di valutazione dei rischi stabilita;
- La politica di valutazione dei rischi è stata rivista nel corso dell'ultimo anno e non risulta che l'MLRO abbia richiesto una revisione precedente.

Attuazione delle misure di due diligence dei clienti

L'obiettivo dell'attuazione delle misure di controllo interno per la conformità della Società alle misure CDD è l'esame delle seguenti circostanze:

- la Società applichi le misure di CDD prescritte dalle Linee Guida a tutti i Clienti interessati;
- la Società raccoglie documenti e informazioni adeguati quando applica le misure di CDD;
- la Società verifica adeguatamente i dati e i documenti raccolti nell'applicazione delle misure di CDD;
- la Società applica il livello pertinente di misure CDD (ad es. misure EDD, ecc.);
- l'Azienda applica misure EDD adeguate a clienti specifici (ad es. PEP, paesi ad alto rischio, ecc.);
- l'Azienda esegue l'identificazione dei Clienti in conformità alla procedura stabilita;
- la Società identifichi correttamente il/i rappresentante/i del Cliente;
- l'Azienda identifica correttamente i titolari effettivi dei Clienti;
- l'Azienda identifica correttamente lo status di PEP dei Clienti;

- la Società identifica correttamente lo scopo e la natura del rapporto commerciale o della transazione;
- la Società monitora adeguatamente i rapporti commerciali con i Clienti.

Nell'applicare le misure EDD nei confronti delle persone fisiche/giuridiche residenti/stabilizzate in Paesi terzi ad alto rischio determinati dalla Commissione europea, l'azienda deve:

- ottenere ulteriori informazioni sul Cliente e su BO;
- ottenere ulteriori informazioni sulla natura prevista della Relazione d'affari;
- ottenere informazioni sulla fonte di fondi e sul patrimonio del Cliente e di BO;
- ottenere informazioni sulle ragioni delle transazioni previste o concluse;
- ottenere l'approvazione del Senior Manager per l'instaurazione di rapporti d'affari con tali clienti o il consenso a proseguire i rapporti d'affari con tali clienti
- eseguire l'EDD aumentando il numero e la tempistica dei controlli e selezionando i tipi di transazioni che richiederanno ulteriori indagini;
- garantire che il primo pagamento da parte di un Cliente sia effettuato da un conto detenuto presso un istituto di credito che abbia sede in uno Stato membro dell'UE o in un paese terzo che preveda requisiti equivalenti a quelli della Legge e sia sottoposto alla vigilanza delle autorità competenti.

Attualmente i Paesi terzi ad alto rischio determinati dalla Commissione europea sono elencati nel Regolamento delegato della Commissione n. 2016/1675 del 14 luglio 2016 che integra la direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio individuando i Paesi terzi ad alto rischio con carenze strategiche e modificato dai seguenti regolamenti:

Regolamento delegato n. 2018/105 della Commissione del 27 ottobre 2017 che modifica il Regolamento delegato (UE) 2016/1675, per quanto riguarda l'aggiunta dell'Etiopia all'elenco dei Paesi terzi ad alto rischio di cui alla tabella del punto I dell'allegato;

Regolamento delegato n. 2018/212 della Commissione del 13 dicembre 2017 che modifica il regolamento delegato (UE) 2016/1675 che integra la direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, per quanto riguarda l'aggiunta di Sri Lanka, Trinidad e Tobago e Tunisia alla tabella del punto I dell'allegato;

Regolamento delegato della Commissione n. 2018/1467 del 27 luglio 2018 che modifica il regolamento delegato (UE) 2016/1675 che integra la direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, per quanto riguarda l'aggiunta del Pakistan alla tabella del punto I dell'allegato.

Sulla base dei risultati della valutazione del rischio nazionale di riciclaggio di denaro e di finanziamento del terrorismo, nel caso in cui nella Repubblica di Lituania venga identificato un livello elevato di rischio di riciclaggio di denaro e di finanziamento del terrorismo in relazione ai Paesi terzi ad alto rischio determinati dalla Commissione europea, la Società, quando avvia o conduce rapporti di corrispondenza internazionale con istituzioni finanziarie stabilite in tali Paesi, deve adottare una o più misure aggiuntive per ridurre efficacemente il rischio di riciclaggio di denaro e di finanziamento del terrorismo:

- applicare misure aggiuntive di monitoraggio rafforzato delle relazioni commerciali per ridurre il rischio di riciclaggio e di finanziamento del terrorismo;
- rendere più stringente la segnalazione di operazioni e transazioni monetarie sospette;
- limitare i rapporti o le transazioni commerciali con persone fisiche o giuridiche stabilite in paesi terzi ad alto rischio identificati dalla Commissione Europea.

Se queste misure aggiuntive non sono sufficienti a ridurre tale rischio, la Società deve rifiutarsi di stipulare o cessare di condurre, o interrompere il rapporto di corrispondenza internazionale con tali istituzioni finanziarie.

Attualmente i Paesi terzi ad alto rischio iscritti nelle liste del GAFI degli Stati che presentano gravi carenze in materia di prevenzione del riciclaggio e del finanziamento del terrorismo e di lotta contro questi reati sono: http://www.fatf-gafi.org/countries/#high-risk. Tuttavia, poiché l'elenco è in continua evoluzione, la Società deve monitorare se l'elenco non è stato modificato e adottare le misure appropriate se necessario.

Nell'applicare le misure EDD nei confronti di persone fisiche/giuridiche residenti/stabilizzate in Paesi terzi ad alto rischio iscritti nelle liste GAFI degli Stati che presentano gravi carenze nel campo della prevenzione del riciclaggio e del contrasto di tali reati, la Società deve:

- ricevere l'approvazione del Senior Manager per concludere il rapporto d'affari con tali clienti o per continuare il rapporto d'affari con tali clienti;
- adottare misure appropriate per stabilire la fonte del patrimonio e la fonte dei fondi relativi al Rapporto d'affari o alla transazione;
- effettuare un monitoraggio continuo e rafforzato del rapporto commerciale con tali clienti.

Nel determinare quali clienti presentano un elevato rischio di riciclaggio e di finanziamento del terrorismo, la Società deve effettuare una valutazione del rischio sui rapporti commerciali. Tenendo conto dei risultati almeno della valutazione del rischio della Società, della valutazione del rischio nazionale e della valutazione del rischio sovranazionale, la Società deve prestare particolare attenzione nel valutare i rischi di riciclaggio e di finanziamento del terrorismo potenzialmente posti dalle seguenti persone ed entità:

- commercianti di beni che, nel corso della loro attività, normalmente effettuano o ricevono importi significativi di pagamenti in contanti;
- soggetti che operano nei sottosettori finanziari o nei prodotti che hanno a che fare con il contante (ad esempio, uffici di cambio, trasferimenti di fondi, alcuni prodotti di moneta elettronica);
- alcune società FinTech (ossia di servizi finanziari abilitati e supportati dalla tecnologia), in particolare con un numero elevato di rapporti commerciali non faccia a faccia;
- operatori di piattaforme di scambio di valute virtuali e/o fornitori di portafogli depositari;
- Altri soggetti obbligati, in particolare i fornitori di servizi di gabling e/o di lotterie e macchine da gioco;
- organizzazioni non profit;
- altri.

Inoltre, nel valutare i rischi di riciclaggio e di finanziamento del terrorismo potenzialmente posti dai clienti, la Società dovrebbe prendere in particolare considerazione:

- i Clienti per i quali è stata precedentemente presentata una STR;
- i Clienti che in passato sono stati inclusi in liste di sanzioni finanziarie internazionali o nazionali e altro;
- i clienti che sono oggetto di una richiesta o di informazioni ricevute dall'UIF, da altre autorità investigative preliminari, dalla procura o da un tribunale in merito a informazioni su un cliente o sulle sue operazioni o transazioni monetarie che potrebbero essere collegate al riciclaggio di denaro e al finanziamento del terrorismo o ad altre attività criminali.

Nel determinare l'esistenza di un rischio più elevato di riciclaggio e di finanziamento del terrorismo, la Società deve valutare almeno i seguenti fattori:

- caratteristiche del Cliente:
- il Rapporto d'affari del Cliente si svolge in circostanze insolite che non hanno alcuno scopo economico o legale evidente;
- il domicilio del Cliente si trova in un paese terzo;
- le persone giuridiche e gli enti privi di personalità giuridica sono impegnati nell'attività di impresa individuale di gestione immobiliare;
- la società ha degli azionisti formali che agiscono per conto di un'altra persona o detiene azioni al portatore;
- Il contante è dominante nell'attività;
- la struttura patrimoniale dell'entità giuridica è apparentemente insolita o eccessivamente complessa se si considera la natura delle attività dell'entità giuridica,
- caratteristiche del prodotto, del servizio, della transazione o del canale di servizio:
- private banking;
- prodotto o transazione può creare condizioni favorevoli all'anonimato;
- I rapporti commerciali o le transazioni occasionali sono conclusi o eseguiti senza la presenza fisica;
- i pagamenti vengono ricevuti da terzi sconosciuti o non collegati;
- prodotto o pratica commerciale, compreso il meccanismo di fornitura del servizio, sono nuovi, anche l'uso di tecnologie nuove o in via di sviluppo coinvolte nel lavoro con prodotti sia nuovi che precedenti,
- caratteristiche del territorio:
- in base ai dati dei rapporti o di documenti analoghi del GAFI o di altre organizzazioni regionali simili, sono state riscontrate significative non conformità del sistema di prevenzione del riciclaggio e del finanziamento del terrorismo con i requisiti internazionali;
- Secondo i dati delle organizzazioni governative e non governative riconosciute a livello mondiale che monitorano e valutano il livello di corruzione, un alto livello di corruzione è stato raggiunto.

corruzione o altre attività criminali nello Stato;

- lo Stato è soggetto a sanzioni, embargo o misure simili imposte, ad esempio, dall'UE o dalle Nazioni Unite;
- lo Stato finanzia o sostiene attività terroristiche, o organizzazioni terroristiche incluse nelle liste stilate da organizzazioni internazionali operano nel territorio dello Stato.

Attuazione delle sanzioni

L'obiettivo dell'attuazione delle misure di controllo interno per la conformità della Società all'attuazione delle sanzioni è l'esame delle seguenti circostanze:

- la Società applica la procedura per l'identificazione di un soggetto sottoposto a sanzioni o di una transazione che viola le sanzioni;
- la Società esegue azioni se identifica un soggetto di Sanzioni o una transazione che viola le Sanzioni.

Obbligo di rifiuto della transazione o del rapporto commerciale e loro cessazione

L'obiettivo dell'implementazione delle misure di controllo interno per l'adempimento dell'obbligo della Società di rifiutare la transazione o il rapporto d'affari e la loro cessazione è l'esame delle seguenti circostanze:

- la Società rifiuta la transazione o il rapporto d'affari se è obbligatorio ai sensi delle Linee guida;
- la Società rifiuta o interrompe la transazione o il rapporto d'affari se è obbligatorio ai sensi delle Linee guida.

Obbligo di rendicontazione

L'obiettivo dell'attuazione delle misure di controllo interno per l'adempimento dell'obbligo di rendicontazione da parte della Società è l'esame delle seguenti circostanze:

- la Società invia rapporti e informazioni alla FCIS, se richiesto dalle Linee guida (incluse le linee guida della FCIS);
- i rapporti inviati al FCIS siano compilati in conformità alle linee guida del FCIS.

Obbligo di formazione

L'obiettivo dell'attuazione delle misure di controllo interno per l'adempimento dell'obbligo di formazione in materia di antiriciclaggio è l'esame delle seguenti circostanze:

- tutti i dipendenti (compresi i membri dell'MLRO e del Consiglio di amministrazione) hanno una formazione adeguata;
- ogni dipendente (compresi i membri dell'MLRO e del Consiglio di amministrazione) è stato formato negli ultimi 360 giorni.

Obbligo di raccolta e conservazione dei dati

L'obiettivo dell'implementazione delle misure di controllo interno per l'adempimento degli obblighi di raccolta e conservazione dei dati da parte della Società è l'esame delle seguenti circostanze:

- tutti i dati che devono essere salvati in conformità con le Linee guida (di seguito in questo capitolo - i Dati salvati) sono stati salvati correttamente in ordine cronologico con un formato che consente di analizzarli e di collegarli in modo comprensibile ad altri dati rilevanti;
- solo i dipendenti (compresi i membri dell'MLRO e del Consiglio di amministrazione) o terzi autorizzati hanno accesso ai dati salvati;
- tutti i registri pertinenti siano tenuti in conformità con le Linee guida;
- i Dati salvati in formato elettronico hanno un backup;
- i Dati salvati in altri formati (ad esempio su carta) hanno un backup in formato elettronico;
- i Dati salvati sono irrevocabilmente cancellati in conformità alle Linee guida.

ALLEGATI

Titolo dell'allegato	Descrizione del documento
Politica di valutazione dei rischi	Stabilisce i principi per la gestione del rischio dell'azienda (compresa la valutazione del rischio e i fattori di rischio) per quanto riguarda il riciclaggio di denaro e il riciclaggio di denaro. Rischi di finanziamento del terrorismo.
Profili dei clienti	Tabella per la valutazione del rischio dei clienti e per la documentazione di tale valutazione. Include i fattori di rischio di ciascuna categoria di rischio.
Procedura di onboarding del cliente	Imposta le istruzioni per l'onboarding del cliente utilizzate nell'ambito dell'attuazione delle misure di CDD.
Questionari	La quantità di informazioni richieste durante l'esecuzione delle misure di CDD (compresa l'applicazione delle misure EDD, la richiesta di SoW/SoF, ecc.)
Elenco delle fonti	Contiene un elenco non esaustivo di risorse che possono essere utilizzate per l'attuazione delle misure di CDD.
Elenco dei criteri per il riciclaggio di denaro e l'identificazione di operazioni o transazioni sospette.	Istruzioni ed esempi di transazioni e altre circostanze che devono essere considerate sospette dal punto di vista del ML/FT.
L'elenco dei dipendenti e le loro responsabilità	L'elenco dei Dipendenti con le relative responsabilità nell'ambito delle Linee Guida specificate
Diari di bordo	La tabella deve essere utilizzata per la tenuta dei registri.
Modulo di segnalazione dell'MLRO	Il modulo di segnalazione che l'MLRO trasmette trimestralmente al consiglio di amministrazione.
Linee guida per la compilazione dei moduli per l'invio di informazioni al FCIS	Linee guida FCIS per la compilazione dei moduli e dei moduli stessi.

Sospensione di transazioni o operazioni monetarie sospette e trasmissione di informazioni su transazioni o operazioni monetarie sospette al FCIS	Le linee guida FCIS pertinenti.
Requisiti tecnici per l'identificazione del cliente tramite trasmissione video in diretta	Linee guida FCIS sui requisiti tecnici pertinenti
Protocollo di formazione	bozza del documento che dovrà essere compilato per ogni formazione effettuata dalla Società ai Soggetti Rilevanti (inclusa la familiarizzazione con le Linee Guida).
Risoluzione di approvazione delle Linee guida	La bozza di delibera dei dirigenti della Società per l'approvazione delle presenti Linee guida.

TABELLA DI CONTROLLO DELLA VERSIONE

Versione	**Data di approvazione**	**Modifiche Descrizione**
1.0	gg.mm.aaaa	Prima edizione
1.1	28.03.2023	Versione aggiornata
1.2	11.07.2023	Versione aggiornata
2.0	07.08.2023	Secondo numero
2.1	06.12.2023	Versione aggiornata
2.2	18.03.2024	Versione aggiornata

Mariana Achim
18.03.2024