AML policy

Quali sono gli obblighi di legge applicabili alla Società?

Cryptosmart S.p.A. (la "**Società**" o "**Cryptosmart**"), in qualità di prestatore di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale, è soggetta alle disposizioni normative concernenti il contrasto al riciclaggio di denaro e al finanziamento del terrorismo di cui al decreto legislativo 21 novembre 2007, n. 231, come successivamente modificato e integrato (il "**Decreto Antiriciclaggio**").

Cryptosmart ha pertanto adottato presidi volti a prevenire il coinvolgimento della Società in atti, fatti o eventi illegali e/o contrari alla legge e regolamenti applicabili, che possono, tra l'altro, determinare il coinvolgimento della Società in fenomeni di riciclaggio o finanziamento del terrorismo.

La Società fornisce ai propri utenti servizi legati alla tecnologia *blockchain*, attraverso, tra l'altro, una piattaforma *internet* – disponibile all'indirizzo www.cryptosmart.it nonché tramite apposita *app* per *smartphone* – che consente di acquistare e vendere valute virtuali o *token* / *asset* digitali, nonché di convertire valute virtuali o *token* / *asset* digitali tra loro o a fronte di valuta avente corso legale e viceversa (la "**Piattaforma**").

L'azione di prevenzione e contrasto del riciclaggio di denaro e finanziamento del terrorismo da parte di Cryptosmart si concretizza nell'adozione di presidi volti a garantire l'adeguata verifica del cliente, la tracciabilità delle operazioni dei clienti, l'individuazione e la segnalazione delle operazioni sospette e la conservazione di dati e documenti della clientela.

La Società ha adottato una propria *policy* interna (la "**Policy**") al fine di descrive le norme e le procedure interne implementate e gestite dalla Società per l'adempimento degli obblighi previsti dal Decreto Antiriciclaggio e dalla relativa normativa di attuazione, ove applicabile alla Società.

La predetta Policy è stata predisposta tenendo conto, tra l'altro, della natura, della dimensione e della complessità dell'attività svolta dalla Società, in conformità al principio di proporzionalità, nonché alla luce del rischio legato alle attività svolte da Cryptosmart, secondo il c.d. approccio basato sul rischio (*risk-based approach*).

A chi si applica la Policy?

La Policy si applica alle attività prestate dalla Società nei rapporti con i clienti che aderiscono alla Piattaforma ed eseguono operazioni per il tramite della stessa, nonché a qualsiasi altra forma di attività esercitata tempo per tempo dalla Società che comporti la prestazione di servizi relativi all'utilizzo di portafoglio digitale e/o di valuta virtuale.

La Policy non trova applicazione in relazione ai rapporti intrattenuti o alle operazioni eseguite dalla Società al di fuori delle attività di cui sopra – quali, ad esempio, i rapporti con i fornitori, i consulenti, i prestatori di servizi informatici, gli *outsourcer*, etc.

Le disposizioni della Policy trovano applicazione ai dipendenti, i collaboratori e gli esponenti aziendali della Società.

Quali sono le attività svolte dalla Società ai fini antiriciclaggio?

La Società, quale prestatore di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale, rientra nell'ambito dei "soggetti obbligati" che sono tenuti ad adempiere agli obblighi in materia di antiriciclaggio e contrasto al finanziamento del terrorismo previsti dalla normativa vigente.

Al fine di contrastare tali fenomeni e ai sensi del Decreto Antiriciclaggio, Cryptosmart adempie i seguenti quattro principali obblighi:

- adeguata verifica della clientela;
- conservazione di dati e informazioni della clientela;
- segnalazioni delle operazioni sospette;
- astensione.

Il Decreto Antiriciclaggio prevede un accurato censimento delle informazioni sulla clientela affinché Cryptosmart possa adottare procedure oggettive e coerenti per l'analisi e la valutazione dei rischi di riciclaggio e di finanziamento del terrorismo cui è esposta nell'esercizio della propria attività, secondo l'approccio basato sul rischio di cui sopra.

A tal proposito, Cryptosmart – sulla base, tra l'altro, della tipologia di clientela – realizza l'analisi e la valutazione dei rischi tenendo conto dell'area geografica di operatività, del rischio associato al cliente e delle caratteristiche dei prodotti e dei servizi offerti.

La Società presta la massima collaborazione con le autorità competenti in materia di contrasto del riciclaggio e del finanziamento del terrorismo – vale a dire, in particolare, il Ministero dell'Economia e delle Finanze, l'Unità di Informazione Finanziaria ("**UIF**") istituita presso la Banca d'Italia, le autorità di vigilanza dei singoli settori in cui operano i soggetti obbligati ai sensi del Decreto Antiriciclaggio, la Direzione Investigativa Antimafia (DIA) e la Guardia di Finanza.

In che cosa consistono le attività di adeguata verifica della clientela?

La raccolta delle informazioni concernenti il cliente e il relativo processo di identificazione ("*Know Your Customer*") costituisce un momento essenziale dei presidi antiriciclaggio adottati dalla Società nei rapporti con i propri clienti.

L'adeguata verifica della clientela, oltre a configurare un valido strumento per il contrasto del riciclaggio e del finanziamento del terrorismo, tutela la Società dall'esposizione a rischi di carattere commerciale, reputazionale nonché dall'applicazione di sanzioni amministrative, civili e penali.

Ai sensi del Decreto Antiriciclaggio, e come meglio descritto nella Policy, Cryptosmart realizza l'adeguata verifica della clientela, in particolare, in occasione dell'instaurazione di un rapporto continuativo con il cliente – vale a dire, al momento della registrazione sulla Piattaforma da parte di quest'ultimo – nonché quando vi è sospetto di riciclaggio o di finanziamento del terrorismo, o vi sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti ai fini dell'adeguata verifica della clientela.

In tutte le ipotesi di cui sopra, gli obblighi di adeguata verifica sono assolti dalla Società con riferimento al cliente nonché, ove applicabile, al titolare effettivo e/o all'esecutore.

La Società ha approntato un apposito meccanismo per procedere all'adeguata verifica della clientela al momento dell'instaurazione del rapporto continuativo con la clientela, attraverso strumenti informatici che consentono l'identificazione del cliente da remoto in modo sicuro e affidabile. La Società provvede inoltre a riscontrare la veridicità dei dati identificativi contenuti nei documenti e delle informazioni acquisiti all'atto dell'identificazione, secondo le procedure dettagliate nella Policy.

In aggiunta a quanto sopra, la Società acquista e valuta le informazioni sullo scopo e sulla natura del rapporto continuativo, verificando la compatibilità dei dati e delle informazioni fornite dal cliente con le informazioni acquisite autonomamente dalla Società, anche avuto riguardo al complesso delle operazioni compiute in

costanza del rapporto o di altri rapporti precedentemente intrattenuti, nonché all'instaurazione di ulteriori rapporti.

In che cosa consiste il controllo costante del rapporto ai fini antiriciclaggio?

Cryptosmart esegue il controllo costante nel corso del rapporto continuativo attuando l'analisi delle operazioni effettuate e delle attività svolte o individuate durante tutta la durata del rapporto, in modo da verificare che esse siano coerenti con la conoscenza che la Società ha del cliente e del suo profilo di rischio, anche riguardo, se necessario, all'origine dei fondi.

Nel corso della relazione con il cliente, Cryptosmart aggiorna i dati e le informazioni concernenti l'adeguata verifica della clientela secondo la periodicità definita all'interno della Policy.

Quali sono gli obblighi dei clienti ai fini del processo di adeguata verifica svolto dalla Società?

Il cliente è tenuto a fornire, tramite la procedura indicata dalla piattaforma di Cryptosmart, sotto la propria responsabilità, tutte le informazioni necessarie e aggiornate richiesta dalla Società, per consentire a Cryptosmart di adempiere agli obblighi di adeguata verifica della clientela. La trasmissione di informazioni complete e veritiere costituisce un obbligo di legge, il cui adempimento è essenziale per consentire alla Società di poter svolgere correttamente le attività di adeguata verifica previste dal Decreto Antiriciclaggio.

In che cosa consiste l'adeguata verifica rafforzata?

In presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo, la Società adotta misure rafforzate di adeguata verifica della clientela acquisendo informazioni aggiuntive sul cliente e sul titolare effettivo; tali misure rafforzate possono consistere, a seconda dei casi, nell'acquisizione di ulteriori informazioni o riscontri in ordine al cliente, al titolare effettivo, allo scopo e alla natura del rapporto, nonché nell'intensificazione della frequenza delle procedure finalizzate a garantire il controllo costante del rapporto continuativo, secondo quanto ulteriormente riportato all'interno della Policy.

Come sono conservati i dati e le informazioni raccolte dalla Società?

La Società conserva i documenti, i dati e le informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo e a consentire lo svolgimento delle analisi effettuate, nell'ambito delle rispettive attribuzioni, dall'UIF o da altra Autorità competente, con particolare riferimento ai documenti acquisiti nell'ambito dell'adeguata verifica della clientela. Al fine del rispetto degli obblighi di conservazione previsti dal Decreto Antiriciclaggio, la Società ha istituito un registro informatico, il quale assicura che la gestione dei dati avvenga con chiarezza, completezza, affinché sussista l'immediatezza delle informazioni e la facilità nel consultarli.

La gestione e conservazione dei dati di cui sopra avviene nel rispetto, in ogni caso, delle applicabili disposizioni di legge in materia di tutela dei dati personali (GDPR). Quali sono le misure organizzative adottate dalla Società per assicurare il rispetto degli obblighi antiriciclaggio? La Società ha attribuito internamente le responsabilità delle attività relative al rispetto della normativa in materia di contrasto al riciclaggio e al finanziamento del terrorismo, attraverso la nomina di un Responsabile Antiriciclaggio.

Cryptosmart ha implementato specifici presidi organizzativi / normativi per l'assolvimento degli obblighi previsti dal Decreto Antiriciclaggio. Sono state, in particolare, predisposte adeguate procedure interne per gestire, attuare e disciplinare gli adempimenti prescritti dal Decreto Antiriciclaggio al fine di fornire, alle funzioni aziendali della Società, strumenti di consultazione e di supporto utili alla comprensione della materia.

Cryptosmart si è dotata di specifici strumenti informatici sia per l'analisi dei profili di rischio antiriciclaggio da attribuire alla clientela che per il monitoraggio delle operazioni "anomale". La Società ha adottato un proprio processo interno per le segnalazioni delle operazioni che destano sospetto circa la provenienza illecita dei fondi trasferiti.

La Società si assicura che vengano svolti programmi di formazione obbligatori (ad esempio, e-learning, corsi specializzati) per tutto il personale, i collaboratori e gli esponenti aziendali. Tali programmi di formazione sono finalizzati alla corretta applicazione delle disposizioni del Decreto Antiriciclaggio, al riconoscimento di operazioni connesse al riciclaggio o al finanziamento del terrorismo e all'adozione dei comportamenti e delle procedure che tutto il personale, i collaboratori e gli esponenti aziendali devono assumere per adempiere alle previsioni del Decreto Antiriciclaggio, secondo quanto delineato nella Policy della Società.