ROX PAY S.R.L.
POLITICA PRIVIND PREVENIREA ȘI COMBATEREA SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI

1 - PREZENTARE GENERALĂ

1.1 – REGULAMENTE CHEIE ȘI ORIENTARE

Acest document stabilește Politica Rox Pay S.r.l. privind combaterea spălării banilor, finanțării terorismului și încălcării măsurilor restrictive[1]și se aplică pentru Rox Pay S.r.l. și operațiunile sale.

Standardele trebuie considerate complementare și aplicabile, deoarece nu intră în conflict cu prevederile emise de autoritățile locale.

1.2 – DESTINATARI ȘI METODE DE IMPLEMENTARE

Politica se aplică pentru Rox Pay S.r.l.

2 – PRINCIPII GENERALE

2.1 CADRUL DE REGLEMENTARE CSB-CFT

Spălarea veniturilor din activități ilegale și infracționale este una dintre cele mai grave forme de criminalitate de pe piețele financiare și reprezintă un domeniu de interes specific pentru activitățile criminale organizate.

Spălarea banilor are un impact negativ semnificativ asupra întregii economii: reinvestirea veniturilor ilegale în activități legale și coluziunea între persoane fizice sau instituții financiare și organizații criminale afectează profund mecanismele pieței, subminează eficiența și corectitudinea activităților financiare și au un efect de slăbire asupra economiei. Finanțarea activităților teroriste poate implica utilizarea veniturilor obținute în mod legal și/sau a veniturilor obținute din infracțiuni.

Natura în schimbare a spălării banilor și a finanțării terorismului, facilitată și de evoluția continuă a tehnologiei, necesită o adaptare constantă a măsurilor de prevenire și contrast.

Cadrul de reglementare pentru combaterea spălării banilor (AML) și a combaterii finanțării terorismului (CFT) se bazează pe un set cuprinzător de surse de reglementare naționale, UE și internaționale.

La nivel internațional, o contribuție-cheie la armonizarea reglementărilor a venit din partea Grupului de acțiune financiară (GAFI), cel mai important organism internațional activ în lupta împotriva spălării banilor, finanțării terorismului și proliferării armelor de distrugere în masă.

1 După cum este definit în Orientările ABE (EBA/GL/2024/14): „Măsurile restrictive ale Uniunii menționate la articolul 2 punctul (1) din Directiva (UE) 2024/1226 și măsurile restrictive naționale adoptate de statele membre în conformitate cu ordinea lor juridică națională (în măsura în care se aplică instituțiilor financiare).

În îndeplinirea responsabilităţilor sale, FATF a stabilit un set de standarde internaţionale, „40 de recomandări", la care s-au adăugat încă 9 recomandări speciale în 2001 pentru combaterea finanţării internaţionale a terorismului. Subiectul a fost complet revizuit în februarie 2012 odată cu adoptarea Standardelor Internaționale privind Combaterea Spălării Banilor și Finanțarea Terorismului și Proliferării, apoi rezumate în „40 de Recomandări" menționate mai sus.

În cadrul luptei împotriva proliferării armelor de distrugere în masă, Organizația Națiunilor Unite a pregătit un set de măsuri pentru combaterea finanțării programelor de proliferare, inclusiv interzicerea asistenței sau finanțării oricăror persoane implicate în astfel de activități.

În implementarea Rezoluțiilor adoptate în cadrul Organizației Națiunilor Unite, Uniunea Europeană a emis un set de prevederi pentru a implementa măsuri restrictive precum înghețarea fondurilor și a resurselor economice ale persoanelor sau entităților implicate în dezvoltarea activităților sensibile la proliferare de arme de distrugere în masă.

FATF a elaborat linii directoare pentru implementarea sancțiunilor financiare adoptate de Națiunile Unite.

Măsuri specifice care abordează proliferarea armelor de distrugere în masă au fost incluse recent în Recomandări, în conformitate cu rezoluțiile Consiliului de Securitate al Națiunilor Unite.

Orientările UE privind prevenirea utilizării sistemului financiar pentru spălarea banilor și finanțarea terorismului sunt cuprinse în Directiva UE 2015/849.[2]a Parlamentului European și a Consiliului din 20 mai 2015 (A patra directivă împotriva spălării banilor), astfel cum a fost modificată prin Directiva UE 2018/843 (a cincea directivă împotriva spălării banilor), precum și în Regulamentele și Orientările emise periodic de UE – Uniunea Europeană și respectiv de EBA – Autoritatea Bancară Europeană.

La nivel național, prevenirea și combaterea spălării banilor și finanțării terorismului este reglementată de următoarele legi primare:

- **Decretul legislativ italian nr. 109 din 22 iunie 2007 și modificările și completările ulterioare care stabilește „Dispoziții pentru prevenirea, contracararea și reprimarea finanțării terorismului și a activității Țărilor care amenință pacea și securitatea internațională", de punere în aplicare a Directivei 2015/849 modificată prin Directiva UE 2018/843;**
- **Decretul legislativ italian nr. 231 din 21 noiembrie 2007, și modificările și completările ulterioare de punere în aplicare a Directivei 2015/849/UE, prin care se modifică Directiva 2009/138/CE și 2013/36/UE, modificată prin Directiva 2018/843/UE privind prevenirea utilizării sistemului financiar în scopul, de asemenea, de decretare și finanțare a terorismului.**

2 Directiva UE 2024/1640 a Parlamentului European și a Consiliului din 31/05/2024 privind procedurile ce urmează a fi puse în aplicare de către statele membre pentru

prevenirea utilizării sistemului financiar în scopuri de spălare a banilor sau finanțare a terorismului, care urmează să fie transpusă până la 10 iulie 2027, modifică Directiva UE 2019/2019/1937 și abrogă Directiva UE 2019/1937.

În sfârșit, există și legislație secundară la nivel național care a fost emisă de Banca Italiei și Unitatea de Informații Financiare („FIU") și este cuprinsă în următoarele surse de reglementare:

- **Dispoziția din 26 martie 2019 de stabilire a dispozițiilor de punere în aplicare privind organizarea, procedurile și controalele interne care vizează prevenirea utilizării intermediarilor financiari și a altor entități în scopuri de spălare a banilor și finanțare a terorismului, astfel cum a fost modificată prin Dispoziția Băncii Italiei din 1 august 2023;**
- **Dispoziție din 28 martie 2019 care stabilește instrucțiuni privind comunicările obiective;**
- **Dispoziție din 30 iulie 2019 de stabilire a dispozițiilor de punere în aplicare privind due diligence față de client, astfel cum a fost modificată de Dispoziția Băncii Italiei din 13 iunie 2023;**
- **Dispoziția din 24 martie 2020 de stabilire a dispozițiilor de punere în aplicare pentru stocarea și disponibilitatea documentelor, datelor și informațiilor privind combaterea spălării banilor și finanțarea terorismului;**
- **Dispoziție din 25 august 2020 de stabilire a dispozițiilor pentru depunerea rapoartelor agregate de CSB;**
- **Dispoziție din 12 mai 2023 privind indicatorii de anomalii pentru intermediari pentru a facilita identificarea tranzacțiilor suspecte, în vigoare de la 1 ianuarie 2024.**

Rox Pay S.r.l. (denumită în continuare „Compania") implementează reglementările de mai sus în documentele sale de reglementare interne.

La nivel general, Societatea a adoptat această „Politică de combatere a spălării banilor și finanțării terorismului" (denumită în continuare „Politica") ca expresie a angajamentului său de a combate fenomenele infracționale menționate pe plan internațional, acordând o atenție deosebită contrastului, în conștientizarea faptului că urmărirea rentabilității și eficienței trebuie combinată cu monitorizarea continuă și eficientă a integrității corporative.

Politica aplicata in cadrul Companiei descrie politica adoptata de Rox Pay S.r.l. în conformitate cu regulile și principiile dictate de prevederile de reglementare naționale și UE, cu respectarea standardelor internaționale relevante și este implementată în comun cu procedurile interne privind combaterea spălării banilor și combaterea finanțării terorismului, Codul de etică și procedurile interne care implementează legislația locală primară și secundară în vigoare cu specificarea proceselor, rolurilor și responsabilităților.

Actuala Politică a fost aprobată de Consiliul de Administrație al Companiei.

Ghidurile CSB și CFT sunt aplicate de către Rox Pay S.r.l. în concordanță cu legile aplicabile.

Compania se angajează să respecte acest cadru de reglementare, precum și orice prevederi de implementare emise de Banca Italiei privind diligența față de client, păstrarea datelor și informațiilor, organizare, proceduri, controale și controale îmbunătățite împotriva finanțării programelor care vizează proliferarea armelor de distrugere în masă.

Compania se angajează temeinic să se asigure că organizarea operațională și sistemul de control sunt complete, adecvate, funcționale și de încredere pentru supravegherea strategică, pentru a proteja Societatea de toleranța sau amestecul de forme de ilegalitate care îi pot afecta reputația și stabilitatea.

Din aceste motive, Rox Pay S.r.l. a adoptat reguli organizatorice si comportamentale si sisteme de monitorizare si control menite sa asigure respectarea legislatiei in vigoare de catre organele administrative si de control, personalul, colaboratorii si consultantii Societatii. Aceste controale sunt, de asemenea, în concordanță cu regulile și procedurile stabilite de codul de protecție a datelor cu caracter personal.

Compania se bazează, de asemenea, pe indicatori de anomalii și tipare de comportamente neregulate în mediul economic și financiar, care sunt eliberați în timp de Unitatea de Informații Financiare (FIU) cu privire la potențiale activități de spălare a banilor și finanțare a terorismului.

2.2 - CADRUL DE REGLEMENTARE PRIVIND MĂSURI RESTRICTIVĂ ȘI EMBARGOURI

Toate măsurile restrictive stabilite pentru contracararea finanțării terorismului și toate activitățile ilicite sau suspecte care amenință pacea și securitatea internațională pot fi fie comerciale, cum ar fi restricții la import/export din/către o țară, fie financiare, precum blocarea parțială sau totală a transferului de fonduri, dar și limitări operaționale și înghețarea fondurilor.

Măsurile restrictive includ sancțiuni financiare internaționale, denumite și embargouri, implementate de statul italian, agenții străine (de exemplu OFAC, UKSL) și organizații supranaționale (ONU, UE) printr-o serie de obligații pe care Compania trebuie să le respecte. Anumite măsuri restrictive (sancțiuni) sunt impuse tuturor statelor membre ONU de către Consiliu pentru a pune în aplicare Rezoluțiile adoptate de Consiliul de Securitate al ONU în temeiul Capitolului VII al Cartei ONU. În plus, sancțiunile pot fi adoptate sau decise în mod autonom de către Uniunea Europeană prin reglementări ale Consiliului, care sunt imediat aplicabile în fiecare stat membru pentru a asigura aplicarea lor în timp util și simultan.

La nivel internațional, există reglementări care stabilesc interdicții sau restricții specifice privind investițiile în anumite sectoare industriale sau importul/exportul din/către „Țări cu risc ridicat sau semnificativ". În special, se referă la rezoluțiile Consiliului de Securitate al ONU (CSNU) în temeiul articolului 41 din capitolul VII al Cartei ONU, prin care se impun măsuri restrictive cu privire la persoane și/sau țări.

În ceea ce privește legislația comunitară, principalele prevederi sunt:

- Regulamentul Parlamentului European și al Consiliului 2021/821 din 20 mai 2021[3] **și modificările ulterioare, prin care se instituie un regim UE pentru controlul exporturilor, transferului, intermedierii și tranzitului de articole cu dublă utilizare;**

3 care a înlocuit Regulamentul Consiliului 428/2009/CE din 5 mai 2009

- Regulamentul (UE) 2023/1113 al Parlamentului European și al Consiliului din 31 mai 2023 privind informațiile care însoțesc transferurile de fonduri și anumite criptoactive și de modificare a Directivei (UE) 2015/849 (reformare);
- Regulamentul (UE) 2024/886 al Parlamentului European și al Consiliului din 13 martie 2024 de modificare a Regulamentelor (UE) nr. 260/2012 și (UE) 2021/1230 și a Directivelor 98/26/CE și (UE) 2015/2366 în ceea ce privește transferurile instantanee de credite în euro;
- Directiva (UE) 2024/1226 a Parlamentului European și a Consiliului din 24 aprilie 2024 privind definirea infracțiunilor și a pedepselor pentru încălcarea măsurilor restrictive ale Uniunii și de modificare a Directivei (UE) 2018/1673 transpusă în dreptul italian prin Decretul legislativ 211/2025.
- **Orientări ale Autorității Bancare Europene privind politicile, procedurile și controalele interne pentru a asigura punerea în aplicare a măsurilor restrictive la nivelul Uniunii și la nivel național (EBA/GL/2024/14)**[4];
- **Orientări ale Autorității Bancare Europene privind politicile, procedurile și controalele interne pentru a asigura punerea în aplicare a măsurilor restrictive la nivel comunitar și național, în conformitate cu Regulamentul (UE) 2023/1113 (EBA/GL/2024/15) privind informațiile care însoțesc transferurile de fonduri și anumite cripto-active și de modificare a Directivei (UE) 2015/849**[5].

În sfârșit, la nivel național, embargourile sunt reglementate după cum urmează:

- **Legislație primară:**
  - **Decretul legislativ nr. 221/2017, care a modificat și simplificat procedurile de autorizare a exportului de articole și tehnologii cu dublă utilizare și sancțiuni privind embargourile comerciale precum și toate tipurile de operațiuni de export de materiale proliferante.**
- **Legislație secundară:**
  - **Dispoziție Banca Italiei din 12 mai 2023 care conține indicatori de anomalii pentru intermediari pentru a facilita identificarea tranzacțiilor suspecte.**

În sfârșit, toate reglementările emise de autoritățile americane sunt relevante pentru activitatea Societății având în vedere aspectele reputaționale și referirea la aceste reglementări în angajamentele contractuale care implică aplicarea potențială a sancțiunilor cu efect extrateritorial (așa-numitele „sancțiuni secundare" americane). Asemenea prevederi de reglementare sunt cuprinse în USA Patriot Act6 și în măsurile referitoare la sancțiunile economice și comerciale emise de Guvernul SUA prin Biroul de Control al Activelor Străine (OFAC) al Departamentului Trezoreriei.[6]

4 pe care Banca Italiei și-a declarat intenția de a-l respecta în Nota nr. 48 din 8 aprilie 2025 și aplicabil de la 30 decembrie 2025.

5 pe care Banca Italiei și-a declarat intenția de a-l respecta în Nota nr. 52 din 19 mai 2025 și aplicabilă de la 30 decembrie 2025.

6 Legea federală a SUA din 26 octombrie 2001, intitulată oficial „Unirea și consolidarea Americii prin furnizarea de instrumente adecvate necesare pentru a intercepta și a obstrucționa Legea terorismului din 2001".

3 – MODELE ȘI METODOLOGII DE GRUP

3.1 – ASPECTE GENERALE

Cadrul național de reglementare stabilit pentru acțiunea preventivă împotriva spălării banilor, finanțării terorismului și încălcărilor Măsurilor restrictive se bazează pe o serie de obligații.

pe care destinatarii sunt obligați să respecte:

- obligația de a adopta structuri organizatorice, proceduri și măsuri de control intern adecvate;
- obligația de a adopta proceduri consecvente și coerente de analiză și evaluare a riscurilor legate de spălarea banilor, finanțarea terorismului și încălcarea Măsurilor restrictive, precum și de a stabili supraveghere, controale și proceduri necesare pentru atenuarea și gestionarea acestor riscuri;
- obligația de diligență față de client, prin care Societatea dobândește și verifică informații cu privire la identitatea unui client și a oricărui beneficiar efectiv, precum și scopul și natura intenționată a relației sau a tranzacției, asigurând în același timp monitorizarea constantă a tuturor tranzacțiilor efectuate de client;
- o abordare bazată pe risc, prin care obligațiile de due diligence ale clientului sunt împărțite în diferite grade de due diligence, proporționale cu profilul de risc al clientului;
- obligația de a păstra documentele, datele și informațiile pentru a permite achiziționarea în timp util, transparența, integralitatea, inalterabilitatea și integritatea acestora, precum și o accesibilitate globală și promptă;
- obligația de raportare a tranzacțiilor suspecte;
- obligația de a se abține de la a intra în orice relație cu clienții noi, de a efectua tranzacții ocazionale sau de a menține o relație de client existentă în cazul în care nu a fost efectuată diligența necesară sau se suspectează că ar putea exista o legătură cu spălarea banilor sau finanțarea terorismului;
- obligația de a sesiza Ministerul Economiei și Finanțelor încălcările prevăzute la articolele 49 și 50 din Decretul legislativ 231/07, precum și de a respecta limitările privind utilizarea numerarului și a titlurilor la purtător;
- monitorizarea tuturor tranzacțiilor cu persoane fizice și juridice și/sau cu țări incluse în Listele Consiliului Uniunii Europene (UE), în Office of Foreign Assets Control List (OFAC), în UK Sanctions List (UKSL)[7], în Lista consolidată a sancțiunilor Consiliului de Securitate al Națiunilor Unite (ONU) în Prevederile emise de autoritățile naționale care conțin măsuri restrictive specifice pentru combaterea terorismului;
- monitorizarea tranzacțiilor încheiate cu țări considerate necooperante în materie de fiscalitate, supraveghere financiară și combatere a spălării banilor, denumite în general „paradisuri fiscale” sau „centre financiare offshore”;
- adoptarea de programe adecvate de formare a personalului pentru a asigura implementarea și aplicarea corectă a legilor și reglementărilor;
- obligația de a furniza FIU „comunicații obiective” în conformitate cu specificul instructiuni privind metodele si frecventa comunicatiilor;

7 Lista OFSI (Office of Financial Sanctions Implementation HMT) a fost închisă la 28 ianuarie 2026; de la acea dată, Lista de sancțiuni din Regatul Unit este singura sursă oficială pentru toate desemnările de sancțiuni din Regatul Unit.

- obligația de a dezvălui orice încălcări sau încălcări care ar putea intra în atenția Organismelor de control în îndeplinirea sarcinilor lor;
- obligația de a adopta proceduri de gestionare a raportării interne a încălcărilor transmise de angajați (Whistleblowing).

În ceea ce privește activitățile de combatere a finanțării terorismului, legislația italiană impune părților obligate să facă următoarele:

- înghețarea fondurilor și resurselor economice ale anumitor persoane incluse în listele UE;
- informarea Unității de Informații Financiare (FIU) cu privire la măsurile aplicate pentru înghețarea fondurilor sau a Unității Speciale de Poliție Valută a Guardia di Finanza (Poliția Financiară) în cazul resurselor economice;
- informarea UIF cu privire la tranzacțiile suspecte, relațiile de afaceri și orice alte informații disponibile cu privire la părțile incluse în listele negre publicate chiar de UIF;
- raportarea tranzacțiilor suspecte care, pe baza informațiilor disponibile, sunt legate fie direct, fie indirect de activitățile de finanțare a terorismului.

În ceea ce privește sancțiunile internaționale (așa-numitele Embargouri) și expunerea la măsuri restrictive, legislația impune luarea anumitor măsuri, inclusiv, dar fără a se limita la:

- date personale și controale tranzacționale asupra operațiunilor legate de importurile și/sau exporturile efectuate de clienți, care vizează blocarea importurilor/exporturilor din sau către o țară, precum și reglementările corespunzătoare. Interdicția poate fi fie generală, implicând toate tipurile de mărfuri, cu excepția cazului în care este autorizată în mod specific, fie limitată la anumite tipuri de mărfuri, de ex. armament (vezi codul vamal);
- restricții totale sau parțiale privind transferurile financiare de la/către o țară;
- cerința de autorizare prealabilă pentru efectuarea transferurilor;
- obligația de a notifica transferurile (ieșite sau intrate);
- interdicția de a finanța, de a acorda asistență financiară sau de a pune la dispoziție Guvernului împrumuturi subvenționate (direct sau în unele cazuri indirect prin intermediul companiilor afiliate sau prin participarea la instituții financiare internaționale);
- interzicerea finanțării clienților care operează cu țări sancționate;
- implementarea măsurilor restrictive împotriva subiecților ruși și belarusi;
- trasabilitatea controalelor efectuate asupra operațiunilor venite din sau îndreptate către țări, persoane și entități supuse restricțiilor.

3.2 - CLIENT DUE DILIGENCE

3.2.1 – Aspecte generale

Compania ia toate măsurile de diligență față de client atunci când:

- stabilirea de relații de afaceri;
- efectuarea de tranzacții ocazionale, aranjate de clienți, precum transferuri bancare sau alte tranzacții egale sau peste pragul desemnat aplicabil, indiferent dacă tranzacția se

desfășoară într-o singură operațiune sau în mai multe operațiuni conexe sau că constă într-un transfer de fonduri, depășind limitele legale;

- există o suspiciune de spălare a banilor sau finanțare a terorismului, indiferent de orice derogare, scutire sau prag desemnat care s-ar putea aplica;
- există îndoieli cu privire la caracterul complet, fiabilitatea și veridicitatea informațiilor sau documentației dobândite anterior în scopul identificării unui Client.

Obligații de due diligence:

- sunt indeplinite:
  - față de noi clienți înainte de stabilirea unei relații în derulare sau de executarea unei tranzacții ocazionale;
  - față de clienții existenți, ori de câte ori diligența necesară este adecvată în lumina unei modificări a nivelului riscului de spălare a banilor sau de finanțare a terorismului asociat clientului sau în cazul în care există suspiciuni sau îndoieli cu privire la acuratețea sau caracterul adecvat al informațiilor obținute anterior de la client;

- și constau din următoarele activități:
  - identificarea Clientului, a beneficiarului efectiv și a executorului și verificarea identității acestora pe baza documentelor, datelor sau informațiilor obținute dintr-o sursă de încredere și independentă;
  - obținerea și evaluarea informațiilor cu privire la scopul și natura intenționată a relației de afaceri;
  - efectuarea unei monitorizări continue pe toată durata relației cu clienții.

În acest scop, Compania - prin angajații săi și/sau prin agenți/consilieri financiari autorizați să facă oferte în afara sediului și care intră în contact direct cu Clientul - obține informațiile cerute de reglementări și colectează orice altă documentație relevantă așa cum este specificat în prezenta Politică și în documentele procedurale ale Companiei.

Compania aplică măsuri de due diligence obișnuite, simplificate sau îmbunătățite în conformitate cu abordarea bazată pe risc aplicată clienților.

3.2.2 - Înregistrarea la distanță a clientului

În cazurile în care Societatea utilizează metode de identificare la distanță, astfel cum sunt permise de Decretul Legislativ nr. 231/07, articolul 19 alineatul (1) litera (a) alineatele (2) și (5), adoptă proceduri speciale pentru îndeplinirea obligațiilor sale de due diligence, și având în vedere riscul de fraudă asociat furtului de identitate. În acest caz, identificarea se bazează pe achiziția certificatului de semnătură electronică calificată, care este generat în urma unui proces de identificare efectuat prin:

- utilizarea Sistemului Public de Identitate Digitală (SPID) sau a Cărții de Identitate Electronică;
- prin tehnici și proceduri de identificare electronică securizate și reglementate, care sunt autorizate sau recunoscute de Agenția pentru Italia Digitală.

În toate cazurile, procesul de identificare la distanță presupune colectarea datelor de identificare ale clientului și ale oricărui executant în format electronic, precum și efectuarea de verificări și verificări privind autenticitatea datelor, în plus față de cele prevăzute pentru identificarea personală, conform unei abordări bazate pe risc, inclusiv prin contact telefonic la

un număr certificat (apel de bun venit) sau printr-un transfer de bani efectuat de către un intermediar bancar și financiar în Italia.

În vederea limitării expunerii la potențiale riscuri de spălare a banilor și/sau fraudă, nu este permisă stabilirea de relații bancare la distanță cu persoane juridice sau persoane fizice care acționează în numele unei persoane juridice, cu excepția cazului în care acestea au fost identificate personal (față în față).

Stabilirea de relații bancare la distanță cu clienții care nu sunt rezidenți în Italia nu este permisă.

3.2.3 – Evaluarea pre-implementare și monitorizarea continuă a proceselor de deschidere a relațiilor la distanță.

Procesele de identificare la distanță a clienților și de onboarding sunt formalizate și detaliate în reglementările interne. Modelul de supraveghere a acestor procese include:

I. evaluarea preliminară a soluției de onboarding la distanță (așa-numita Evaluare Pre-Implementare[8]) care vizează:
   (i) evaluarea gradului de adecvare a solutiei in ceea ce priveste integralitatea si acuratetea datelor si documentelor ce urmeaza a fi colectate, precum si a fiabilitatii si independentei surselor de informatii utilizate;
   (ii) să evalueze impactul utilizării soluției asupra riscurilor de afaceri, inclusiv a riscurilor operaționale, reputaționale și juridice, prin implicarea funcțiilor tehnice și de specialitate relevante;
   (iii) să identifice măsuri de atenuare și acțiuni corective pentru fiecare risc identificat;
   (iv) definiți teste ex ante pentru a evalua riscurile TIC și de fraudă și teste de la capăt la funcționarea soluției.

II. monitorizarea continuă a soluției de onboarding adoptată prin controale periodice și bazate pe evenimente pentru a asigura buna funcționare a acesteia în timp (așa-numita Monitorizare continuă).

III. revizuirea evaluării preliminare în soluția de onboarding la distanță (așa-numita Evaluare Pre-Implementare) atunci când apar modificări structurale ale soluției adoptate sau anumite evenimente, cum ar fi:
   (i) modificări ale expunerii la riscuri în domeniile combaterii spălării banilor și combaterii finanțării terorismului, precum și embargouri;
   ii) deficiențe detectate pentru ca soluția noastră să funcționeze;
   iii) o creștere a tentativelor de fraudă;
   (iv) modificări ale legislației.

3.2.4 – Obligații simplificate de due diligence

În general, Compania utilizează o abordare bazată pe risc pentru a identifica tipurile de clienți cărora li se pot aplica măsuri simplificate de due diligence. Acestea includ cazurile în care sunt prezenți „indicatori de risc scăzut”, așa cum se indică în Anexa 1 a Dispoziției Băncii Italiei privind due diligence asupra clienților din 30 iulie 2019 (denumită în continuare „Dispoziția”).

8 Nota nr. 32 din 13 iunie 2023 prin care Banca Italiei și-a declarat intenția de a respecta Orientările EBA (EBA/GL/2022/15) privind utilizarea soluțiilor de onboarding de la distanță a clienților.

„Indicatorii de risc scăzut" relevanți în vederea aplicării unei proceduri simplificate de due diligence se bazează pe tipul de client, executor sau beneficiar efectiv, zona geografică de reședință sau în care este stabilit sediul social, produs, serviciu sau canal de distribuție specific.

În detaliu, tipurile de clienți considerați a fi expuși unui risc scăzut de spălare a banilor, cărora li se poate aplica due diligence simplificată, includ:

- Administratii Publice, Institutii sau Organisme care indeplinesc functii publice, in conformitate cu legea Uniunii Europene;
- Companii listate pe o piață reglementată și supuse cerințelor de dezvăluire, inclusiv asigurarea unei transparențe adecvate a proprietarului efectiv final;
- instituțiile financiare și de credit ale Comunității Europene enumerate la articolul 3 alin. (2) din Decretul de combatere a spălării banilor — cu excepția celor de la literele i), o), s), v)[9]— și instituțiile de credit și financiare cu reședința în state membre sau în țări terțe cu sisteme eficiente de spălare a banilor și finanțare a terorismului;
- Clienți, executori sau beneficiari reali cu reședința sau stabilirea în zone geografice cu risc scăzut de spălare a banilor.

Compania nu aplică măsuri simplificate de due diligence asupra clienților atunci când:

- apar îndoieli, incertitudini sau inconsecvențe cu privire la datele și informațiile de identificare culese în timpul identificării clientului, executorului sau beneficiarului efectiv;
- nu mai sunt îndeplinite condițiile de diligență simplificată a clienților pe baza indicatorilor de risc prevăzuți de decretul de combatere a spălării banilor și de reglementarea secundară relevantă;
- monitorizarea operațiunilor de ansamblu efectuate de client și informațiile adunate pe parcursul relației exclud un tip de risc scăzut;
- încă mai apare suspectul de spălare a banilor sau de finanțare a terorismului.

Funcția de combatere a spălării banilor are responsabilitatea exclusivă asupra evaluării și autorizării măsurilor simplificate de due diligence a clienților, desfășurate prin parcurgerea tuturor pașilor necesari procesului obișnuit de due diligence a clienților - inclusiv obligația de a identifica și verifica identitatea clientului, a executorului și a Beneficiarului, și de a achiziționa toate datele și documentele necesare pentru înregistrarea completă a acestora (de exemplu, cod, denumire legală, denumire fiscală, de ex. deși reducând nivelul lor de profunzime, sferă și frecvență.

3.2.5 – Obligații sporite de due diligence

Compania aplică măsuri sporite de due diligence a clienților în prezența clienților sau a situațiilor cu un risc mai mare de spălare a banilor sau de finanțare a terorismului și în toate cazurile menționate la articolul 24 din Decret. Aceste măsuri consolidate includ, inter alia, implicarea unor roluri de responsabilitate proporționale cu nivelul de risc identificat în raport cu clientul.

9 i) brokerii menționați la art. 201 din TUF; o) intermediarii de asigurări prevăzuți la art. 109, alin. 2, lit. a), b), și d), din CAP, care își desfășoară activitatea în ramurile de activitate prevăzute la art. 2 alin. 1 din CAP; s) societăți fiduciare înregistrate în registrul înființat potrivit art. 106 din TUB; v) consilierii financiari prevazuti la art. 18-bis din TUF si firmele de consultanta financiara prevazute la art. 18-ter din TUF.

În ceea ce privește clienții de private banking, Compania evaluează factorii de risc specifici inerenți naturii afacerii lor și aplică măsuri de due diligence consolidate pe baza informațiilor generale disponibile și a evaluărilor efectuate.

Implicarea Funcției de combatere a spălării banilor este necesară în următoarele cazuri:

- persoanele fizice și juridice incluse în listele persoanelor sau entităților supuse măsurilor de înghețare a fondurilor în temeiul reglementărilor sau decretelor europene în temeiul Decretului legislativ 109/07, precum și celor strâns asociate acestora;
- o relație bancară corespondent transfrontalier stabilită cu o bancă sau o instituție situată într-o țară terță, pe baza factorilor geografici de risc ridicat (așa cum se raportează în anexa 2 la dispozițiile Băncii Italiei privind diligența cu privire la client);
- relații sau tranzacții în care clientul sau beneficiarul final este o persoană expusă politic[10];
- situații care implică elemente de risc care necesită aplicarea unor măsuri specifice de confidențialitate;
- situație cu risc mai mare de spălare a banilor sau de finanțare a terorismului din cauza unor neprevăzute obiective, de mediu sau subiective;
- clienți clasificați ca „Trust", servicii de transfer de bani și schimburi valutare virtuale;
- Companii de încredere, cu excepția cazurilor prevăzute la paragraful 3.4;

Mai mult, înainte de a intra, continua sau menține o relație continuă cu Persoane Expuse Politic sau Entități Corespondente din țări terțe, este necesară obținerea autorizației corespunzătoare de la Directorul General sau de la delegatul acestuia, după obținerea avizului Funcției Anti-Spălarea Banilor. În cazul delegaților în temeiul articolului 25 din Decretul legislativ 231/07 aparținând Funcției de combatere a spălării banilor, această autorizare este inclusă în procesul de due diligence consolidat.

În toate celelalte cazuri, aplicarea măsurilor îmbunătățite este proporțională cu nivelul de risc atribuit clientului. În cazul în care riscul este considerat mediu/ridicat, sau dacă sunt prezenți anumiți factori de risc indiferent de punctajul atribuit, este necesară implicarea șefului unității de afaceri responsabilă cu managementul comercial al clientului.

Exemple de astfel de cazuri sunt:

- clienți persoane juridice cu un Executor identificat ca PEP sau PEP indirect, indiferent de profilul de risc;
- servicii oferite prin intermediul rețelelor de agenți financiari, consilieri financiari, contractori și agenți;
- clienți clasificați ca Fundație/Organizații non-profit;
- clienți persoane juridice în faza de onboarding;
- clienții cu știri negative în timpul fazei de onboarding („știri adverse");

10 Persoane Expuse Politic (PEP): astfel cum sunt enumerate la art. 1, alin.2, lit. dd) Decretul legislativ 231/07.

- clienți cu reședința sau cu sediul în țări terțe cu risc ridicat sau în cazul unor relații în curs, servicii profesionale și operațiuni care implică țări cu risc ridicat;
- companii care au emis acțiuni la purtător sau care au o societate care emite acțiuni la purtător în structura lanțului de control;
- relații sau tranzacții în care clientul și beneficiarul final dețin o funcție publică, alta decât cele enumerate pentru persoanele expuse politic[11];
- companii deținute de trusturi, societăți de trust, fundații, societăți pe acțiuni prin mai multe niveluri de participare sau participații încrucișate;
- clienții angajați într-un tip de activitate economică care este deosebit de expuși riscului de spălare a banilor sau în sectoare de activitate „controversate”[12] sau activități comerciale intensive în numerar, cum ar fi numerar pentru aur, schimb de bani, jocuri de noroc/pariuri, inclusiv on-line, industria armelor, minerit, colectarea și eliminarea deșeurilor, producția de energie regenerabilă, companiile care operează în sectorul cripto-active, construcții, achiziții de instrumente farmaceutice;
- clienții care participă la contracte publice sau care primesc finanțare publică (asistență medicală, construcții, colectarea și eliminarea deșeurilor, producția de energie regenerabilă, minerit, furnizarea de instrumente farmaceutice);
- în cazul clienților care au dobândit cetățenia unui stat membru sau au obținut drepturi de ședere într-un stat membru (UE) printr-un program de cetățenie prin investiții sau un program de rezidență prin investiții;
- în cazul clienților persoane juridice rezidente într-o țară a UE, în care drepturile de proprietate ale companiei sunt deținute – direct sau indirect – în proporție de peste 40% de către o persoană juridică, organizație sau organism stabilit în Rusia, sau de către o persoană fizică cu reședința sau cetățenia rusă.

Implicarea șefului unității de afaceri responsabilă cu managementul comercial al clientului este necesară și în cazul oricăror erori informatice care ar putea împiedica calcularea în timp real a riscului de spălare a banilor al clientului.

Măsurile de due diligence consolidate includ obținerea de informații suplimentare despre client, executorul și beneficiarul efectiv, investigarea scopului și naturii relației și creșterea frecvenței procedurilor care vizează asigurarea monitorizării continue pe parcursul relației în derulare.

În deplină conformitate cu legislația în vigoare și cu prevederile procedurilor interne privind combaterea spălării banilor și a finanțării terorismului și în conformitate cu Codul de etică al Companiei, Compania nu acceptă tranzacții cu clienți care operează în sectoare controversate care
(i) nu sunt conforme cu legislația națională în vigoare și (ii) nu sunt, dacă este cazul, autorizate în prealabil de autoritățile naționale italiene competente, în special:

- producerea, tranzitul și/sau comercializarea materialelor de armament;
- producția și vânzarea de marijuana ușoară, locuri de divertisment pentru adulți;

11 Funcții publice, altele decât cele deținute de Persoanele Expuse Politic (PEP) menționate la nota 1), care se aplică tuturor celor care dețin funcții în, dar fără a se limita la, organismele publice, consorții, asociații cu caracter public enumerate la secțiunea A 8) din Anexa 2 la Dispoziție.
12 un sector economic este „controversat” dacă bunurile/serviciile fabricate/oferite și/sau modurile în care sunt produse/oferite sunt în contrast cu valorile larg împărtășite de etică și durabilitate, chiar și atunci când serviciile sau activitățile sunt legale și, prin urmare, nu sunt în contrast cu obligațiile legale.

- activități comerciale intensive în numerar, altele decât cele enumerate mai sus, cum ar fi organizațiile de caritate nereglementate și ONG-urile, producția de metale și pietre prețioase, remitențe de bani.

În plus, Compania acordă o atenție deosebită respectării măsurilor restrictive puse în aplicare de statul italian, organismele străine (de exemplu OFAC, UKSL) și/sau organismele supranaționale (ONU, UE). Aceste măsuri pot fi de natură comercială (de exemplu, blocarea importurilor/exporturilor) sau de natură financiară, cum ar fi blocarea parțială/totală a transferurilor de bani din sau către o anumită țară sau limitări ale operațiunilor și/sau înghețarea fondurilor deținute la intermediarii financiari.

În vederea respectării obligațiilor prevăzute în Decretul legislativ italian 109/07 - care vizează prevenirea și combaterea finanțării terorismului și a activităților țărilor care amenință pacea și securitatea internațională, prin aplicarea unor măsuri restrictive de „înghețare" a fondurilor și resurselor economice deținute de persoane fizice și juridice, grupuri și entități identificate în mod specific de către Națiunile Unite și Uniunea Europeană („Obligațiile stabilite de Națiunile Unite și de Uniunea Europeană") în Decretul legislativ italian 231/07, Compania a adoptat proceduri de control automat. Aceste proceduri sunt capabile să verifice coerența dintre datele de identificare a clienților obținute prin procesul de due diligence și cele cuprinse în listele elaborate de UE și alte instituții și organisme internaționale, cum ar fi:

- persoanele fizice cărora le este încredințată o funcție publică proeminentă sau care au încetat din funcție de mai puțin de un an (PEP), membrii familiei acestora și cei care au legături strânse cu aceștia conform definiției art. 1 c. 2 lit.dd din Decretul legislativ 231/07 (PEP rezidente si nerezidente);
- persoane cu domiciliul în Italia care ocupă funcții publice, care nu se încadrează în definiția PEP, dar sunt totuși expuse unui risc semnificativ de corupție și spălare de bani;
- persoanele fizice și juridice care își desfășoară activitatea, chiar și parțial, în state care nu impun măsuri și reglementări echivalente, conform liniilor directoare ale Băncii Italiei sau ale altor instituții naționale sau supranaționale implicate în prevenirea criminalității;
- persoane fizice și juridice supuse măsurilor de embargo sau înghețare a fondurilor/resurselor economice și a activelor financiare (Liste de sancțiuni ONU, UE, UKSL, OFAC).

3.3 - PROFILARE CLIENT

Societatea adoptă proceduri adecvate care vizează definirea profilului de risc de spălare a banilor și finanțare a terorismului (PR) atribuibil fiecărui client, pe baza informațiilor obținute și a analizelor efectuate, cu referire atât la elementele de evaluare indicate în Prevedere, cât și la elementele ulterioare care pot fi adoptate de către Societate însăși în timp (așa-numita profilare).

Pe baza profilării clienților, care se efectuează și periodic, Compania aplică măsuri standard sau îmbunătățite, care includ implicarea unor roluri de responsabilitate proporționale cu nivelul de risc identificat al clientului. Avizul prealabil al Funcției de combatere a spălării banilor este necesar în conformitate cu responsabilitățile prevăzute în documentul intern „Proceduri interne de combatere a spălării banilor și a finanțării terorismului".

Clasificarea clienților pentru due diligence simplificată este autorizată de către Funcția Anti-Spălare a Banilor, la solicitarea șefului Unității de Afaceri Operaționale.

În acest caz, sfera și frecvența cerințelor sunt reduse, verificarea expirând după 8 ani indiferent de scorul de risc, cu excepția cazului în care nu mai sunt îndeplinite condițiile de aplicare a due diligence simplificate.

În plus, Compania a pus în aplicare o procedură IT pentru a evalua profilul de risc al clientului și pentru a defini în mod consecvent un interval de timp de reevaluare adecvat nivelului de risc calculat; frecvența de reevaluare depinde de procesul identificat în ultima evaluare efectuată sau, în absența unui chestionar KYC, de profilul de risc al clientului, după cum se specifică mai jos:

Clasa de risc (RP)	Scor	Proces de due diligence	Rol de validare	Frecvența reevaluării
Clienți clasificați ca fiind supuși unei verificări simplificate	N / A	Simplificat	Acceptare automată/ Manager unitatea de afaceri (*)	8 ani
Imaterial	<=5	Standard	Acceptare automată	8 ani
Scăzut	>=6 e <=12			6 ani
Mediu	>=13 și <=24	Îmbunătățit	Manager unitate de afaceri (**)	2 ani
Ridicat	>=25			1 an
În cazul elementelor de risc specifice (***)		Îmbunătățit	Funcția de validare AML	1 an

(*) furnizat în cazul în care scorul de risc calculat sau rezultat din KYC efectuat este cel puțin mediu. (**) furnizate chiar și în prezența unor elemente de risc definite care mențin profilul de risc sub mediu.
(***) furnizate chiar și în prezența Persoanelor Juridice cu RP >39, dacă desfășoară activități comerciale legate de achiziționarea de aur, jocuri de noroc și pariuri și colectarea și eliminarea deșeurilor (coduri ATECO de risc ridicat) și/sau dacă sunt supuse auditurilor/investigațiilor.

3.4 - INSTRUMENTE PENTRU SPRIJINEREA DUI DILIGENCE

Compania a implementat instrumente avansate din punct de vedere tehnologic pentru a sprijini procesele de combatere a spălării banilor, alături de aplicațiile tradiționale deja utilizate:

- Robotic Process Automation (RPA) aplicat activităților de colectare a datelor în domeniile due diligence față de clienți și raportarea tranzacțiilor suspecte;
- Artificial Intelligence Engine, bazat pe componente statistice și indicatori predictivi (Predict Index AML, Reputational Index și Criminal Infiltration Index) construit cu tehnici Data Analytics, aplicate procesului obișnuit de revizuire a clienților;
- Platforma de inteligență Cogito, o aplicație utilizată pentru colectarea de știri, documente și informații textuale pentru a căuta știri adverse cu privire la clienții supuși due diligence;
- Rozes, un instrument de informare a datelor care, prin analiza situațiilor financiare în timp real, permite identificarea companiilor al căror bilanț și indicatori financiari sunt similari cu cei regăsiți în companiile supuse infiltrării criminale.

Mai mult, în sfera instrumentelor avansate menționate mai sus, au fost identificate anumite „evenimente declanșatoare", care au ca scop interceptarea evenimentelor privind clientul și/sau relațiile aferente, determinând o variație a datei de expirare a „Evaluării Clientului - KYC", de exemplu:

- în cazul modificărilor datelor de registru ale beneficiarului efectiv și ale reprezentantului legal;
- în cazul unei modificări a Profilului de Risc din cauza prezenței anumitor factori de risc ridicat printre cei prevăzuți de Dispoziție;
- în cazul în care un beneficiar efectiv își asumă rolul de PEP sau înregistrarea unui nou beneficiar efectiv PEP;
- în cazul delegării unei relații cu client persoană fizică acordată unei persoane clasificate ca PEP;
- în cazul unei neconcordanțe între beneficiarul efectiv înscris în registru și probele strânse din extrasele Camerei de Comerț;
- în cazul controalelor de nivel al doilea de către Funcția AML.

Responsabilitatea pentru procesul de due diligence al unui client revine unității de management al relațiilor cu clientul, care se ocupă de obicei de stabilirea de noi relații în curs de desfășurare, execută orice tranzacții ocazionale, reevaluează periodic clienții existenți și asigură monitorizarea continuă a relației cu clienții.

3.5 - OBLIGAȚII DE ABSȚINERE

Societatea se abține de la stabilirea, executarea sau continuarea relației, operațiunilor și serviciilor profesionale (așa-numita obligație de abținere) în cazul unei imposibilități obiective de a efectua due diligence față de client, evaluând dacă să raporteze o tranzacție suspectă către UIF.

În acele cazuri, în care abținerea nu este posibilă, întrucât există obligația legală de a executa operațiunea care nu poate fi amânată sau dacă refuzul ar putea împiedica ancheta, Societatea este totuși obligată să raporteze imediat tranzacția suspectă.

Mai mult, dacă după o evaluare ulterioară sau în aval de procesul de due diligence consolidat, apar elemente de risc ridicat care ar putea afecta profilul legal și/sau reputațional al Societății, Societatea își rezervă dreptul de a limita sau de a înceta relația de afaceri cu clientul. Aceste limitări pot viza, de exemplu, accesul clienților la anumite tipuri de produse sau pot duce la întreruperea serviciilor oferite de Companie în legătură cu contul/relația.

Măsurile de due diligence a clienților adoptate de Societate nu împiedică/interzice, însă, accesul la servicii financiare pentru clienții sau categorii întregi de clienți cu risc ridicat care ar avea dreptul la acestea conform legislației în vigoare, cu excepția cazurilor prevăzute expres de Decretul Legislativ 231/07, privind interzicerea menținerii relațiilor cu anumite tipuri de entități.

Compania nu intră într-o relație de corespondent cu o bancă shell și se abține de la a intra în relații cu entități care permit accesul la relații de corespondent cu o bancă shell. Nu va intra într-o relație de afaceri cu entități a căror structură de proprietate (corporativă, fiscală și financiară) este caracterizată de un grad ridicat de opacitate care împiedică identificarea clară a beneficiarului efectiv sau a naturii și scopului structurii.

În acest scop, Compania ia toate măsurile pentru a se asigura că nu colaborează în mod deliberat și cu bună știință cu instituțiile financiare care, la rândul lor, operează cu bănci ființe.

În plus, Compania se abține de la a intra sau de a continua o relație de afaceri cu persoane expuse în special riscului de spălare a banilor/finanțare a terorismului, cum ar fi:

- Societăți de trust cu sediul social într-o țară indicată de FATF ca fiind expusă unui risc mai mare de spălare a banilor sau care nu adoptă măsuri conforme cu obligațiile impuse de Decretul Legislativ 231/07 sau Directivele Europene;
- Trusturi pentru care nu sunt disponibile informații adecvate, exacte și actualizate privind proprietarul efectiv al trustului și natura și scopul acestuia;
- Companii de pariuri, inclusiv jocuri de noroc online, cazinouri și operatori de bingo pentru care nu au fost eliberate și/sau verificate autorizațiile și/sau licențele cerute de legislația italiană și internațională;
- Entități afiliate și agenți ai prestatorilor de servicii de plată (la care se face referire în definiția art.1 c. 2 lit.nn) și instituțiilor de monedă electronică care nu respectă prevederile capitolului V din Decretul legislativ 231/07 la articolele 43 și următoarele;
- Societăți cu răspundere limitată sau companii controlate prin acțiuni la purtător, cu sediul în Țări cu risc ridicat;
- Clienții care operează în producția și vânzarea de marijuana ușoară sau locuri de divertisment pentru adulți, în cazul în care nu este în măsură să verifice autorizațiile cerute de lege.

Compania folosește toate informațiile dobândite în timpul procesului de due diligence cu privire la clienții săi și tranzacțiile acestora pentru a determina dacă o tranzacție sau o relație de afaceri este, direct sau indirect, legată de persoane sau entități implicate în spălarea banilor, finanțarea terorismului sau în dezvoltarea armelor de distrugere în masă și nu sprijină în niciun fel tranzacții care implică arme și tratamente internaționale, interzise și controversate.
de ex. arme nucleare, biologice și chimice, bombe cu dispersie, arme care conțin uraniu sărăcit, mine antipersonal.

În ceea ce privește producția, tranzitul și/sau comercializarea materialelor de armament, altele decât cele menționate mai sus, Societatea poate sprijini tranzacții care au fost autorizate în mod corespunzător de autoritățile competente și care sunt conforme cu legislația aplicabilă și în vigoare.

3.6 – RAPORTAREA TRANZACȚIUNILOR SUSPICIOSE

Ori de câte ori Compania suspectează sau are motive întemeiate să suspecteze că o operațiune de spălare a banilor sau de finanțare a terorismului a fost sau este efectuată sau încercată:

- transmite un raport de tranzacție suspectă la Unitatea de Informații Financiare (FIU), dacă tranzacția are sediul în Italia;

- în cazul în care tranzacția are sediul în altă țară, respectă prevederile legislației locale și, în cazul în care aceasta din urmă prevede aplicarea unor măsuri echivalente cu cele prevăzute de Legea UE, informează cu promptitudine Șeful Serviciului Anti-Spălare a Banilor, luând toate măsurile de precauție necesare pentru a proteja identitatea persoanelor care raportează tranzacția suspectă.

Compania a pus în aplicare proceduri și procese pentru a monitoriza, identifica și raporta activitățile suspecte în conformitate cu calendarul și metodele cerute de Legea aplicabilă.

Angajații raportează cu promptitudine orice cunoaștere sau suspiciune de spălare a banilor, finanțare a terorismului sau alte activități infracționale, ori venituri din activități infracționale, indiferent de mărimea acestora, în conformitate cu modelul organizatoric actualizat și modurile de funcționare prevăzute în regulamentul intern de referință. Până la finalizarea procesului de raportare, Societatea se abține de la executarea tranzacției, cu excepția cazului în care acest lucru este imposibil întrucât există o obligație legală de a accepta actul sau executarea operațiunii nu poate fi amânată din cauza desfășurării normale a activității sau în cazul în care ar putea obstrucționa investigațiile. În aceste cazuri, raportul este transmis imediat după ce tranzacția a fost executată.

Motivele de suspiciune includ caracteristicile, amploarea și natura tranzacției, încercarea de scindare a tranzacției și orice altă împrejurare care vine la cunoștința angajaților ca urmare a atribuțiilor lor, ținând cont, de asemenea, de sfera financiară și de natura activității desfășurate de subiectul tranzacției suspecte, pe baza elementelor dobândite în temeiul legislației de combatere a spălării banilor în perioada exigibilă (ex.

Pentru a limita riscul de implicare al Companiei – chiar dacă neintenționat – în activitățile ilegale menționate mai sus, se activează un proces de due diligence consolidat în acordurile de transfer de fonduri în care jucătorii implicați în acest tip de tranzacție (originator, beneficiar, băncile implicate în transferul de fond) pot duce la suspiciunea de spălare a banilor, finanțare a terorismului sau încălcări ale anumitor entități internaționale aplicabile, persoane sau încălcări ale unor bunuri aplicabile.

În aval de procesul de raportare, Societatea poate limita și/sau întrerupe relația de afaceri cu clienții, în special în cazul în care relația respectivă poate constitui un risc juridic sau reputațional semnificativ pentru Rox Pay S.r.l.

3.7 – PĂSTRAREA DATELOR

Compania păstrează toate documentele și înregistrează toate datele obținute prin procesul de due diligence a clienților, asigurând trasabilitatea tranzacțiilor clienților pentru a facilita funcțiile de control ale Băncii Italiei și ale FIU, inclusiv inspecțiile.

În acest scop, Rox Pay S.r.l., în calitate de intermediar financiar cu sediul în Italia, a înființat o Arhivă Electronică Unică (Archivio Unico Informatico sau AUI) care îi permite să furnizeze informații Băncii Italiei și FIU conform standardelor tehnice specificate în Anexa 2 a Dispozițiilor privind păstrarea datelor. Această arhivă stochează electronic toate datele de identificare și alte informații legate de relațiile de afaceri în desfășurare și tranzacțiile cu clienții, conform cerințelor legii aplicabile.

În acest sens, ca răspuns la actualizările recente introduse de „Prevederile privind păstrarea datelor și accesul la documente, date și informații” și „dispoziții privind transmiterea agregată

a datelor", Compania a decis să adopte anumite principii pentru scutirea de obligațiile de înregistrare așa cum sunt prevăzute în mod expres. În special, datele și informațiile privind tranzacțiile organizate de intermediarii bancari și financiari, care se încadrează în cazurile specificate la art.

8 din Dispozițiile privind păstrarea datelor și articolul 3 din Prevederile privind datele agregate nu sunt înregistrate în Arhiva Electronică Unică.

În ceea ce privește cerințele de due diligence, Compania păstrează copii sau înregistrări ale tuturor documentelor necesare pentru o perioadă de zece ani de la încheierea relației de afaceri.

În ceea ce privește tranzacțiile și relațiile de afaceri aflate în derulare, toate probele și înregistrările justificative, de exemplu, documentele originale sau copiile admisibile în procedurile judiciare, sunt păstrate pe o perioadă de zece ani de la executarea tranzacției sau după încheierea relației de afaceri.

3.8 – PREVENIRE REGARGIN MĂSURI RESTRICTIVA

Având în vedere natura, dimensiunea și complexitatea activității sale, precum și gama și tipul de servicii furnizate, Compania este expusă riscului de încălcare a măsurilor restrictive.

În vederea menținerii unui sistem organizatoric și procedural care vizează asigurarea respectării măsurilor restrictive internaționale UE și naționale, riscul încălcării măsurilor restrictive este evaluat de către Funcția de combatere a spălării banilor pe baza factorilor geografici, clienților, produselor/serviciilor și canalului de distribuție, asigurând monitorizarea constantă a eficacității sistemului, garantată și prin desfășurarea periodică a unor acțiuni de autoidentificare, care să permită desfășurarea periodică a unui răspuns corect. la detectarea problemelor critice existente și/sau adoptarea unor măsuri adecvate de prevenire și atenuare a riscurilor.

Compania a stabilit proceduri și procese pentru a monitoriza, identifica și raporta activitățile care încalcă măsurile restrictive, cu termene și metode conforme cu cerințele legale.

Controalele existente asupra persoanelor fizice/entităților și tranzacțiilor sunt efectuate printr-un proces de screening automatizat, care se realizează atât zilnic, cât și în faza de onboarding, prin utilizarea unor liste specifice – actualizate de două ori pe zi – referitoare la clienți, contrapărți, țări și tranzacții.

Sunt în vigoare procese de monitorizare a fluxurilor de intrare sau de ieșire cu țări și/sau entități supuse sancțiunilor financiare internaționale, cu responsabilități definite între departamentele competente.

Se asigură că personalul este instruit corespunzător și este informat cu privire la politicile, procedurile și controalele pentru a respecta măsurile restrictive.

4 – LISTA PROCESELOR CHEIE

4.1 – MANAGEMENTUL RISCURILOR DE SPĂLARE DE BANI ȘI FINANȚARE TEROISTĂ

Procesul „Managementul riscului de spălare a banilor și finanțare a terorismului” este procesul prin care se desfășoară următoarele activități în cadrul Societății pentru a atenua riscul de nerespectare a cerințelor de combatere a spălării banilor și finanțării terorismului:

- Identificarea riscului de nerespectare a cerințelor CSB-CFT prin supravegherea

continuă a modificărilor legislației și evaluarea impactului asupra proceselor și procedurilor de afaceri, precum și prin identificarea și evaluarea riscurilor CSB-CFT folosind o abordare bazată pe risc;

- Gestionarea și atenuarea riscului de spălare a banilor și finanțare a terorismului prin implementarea și monitorizarea acțiunilor de diminuare a riscului de neconformitate stabilite în Planul anual (Planul AML) sau identificate de Guvernanța Companiei așa cum sunt aplicate de toate funcțiile de afaceri relevante în implementarea procedurilor (reglementări interne, aplicații IT, procese operaționale, controale);
- Verificări de conformitate (ex-ante și ex-post) în domeniile de reglementare atribuite de proprietate prin definirea și monitorizarea indicatorilor de risc și a evoluției acestora în timp. Scopul este de a găsi posibile situații de neconformitate, precum și de a desfășura activitățile de control ex-ante și ex-post;
- Oferă consultanță și suport în problemele CSB/CFT, participând în echipe de lucru transversale și acordând sprijin fie structurilor de afaceri, fie Organismelor de top management în probleme și procese de afaceri în care riscul de spălare a banilor și finanțare a terorismului este relevant, prin îndeplinirea îndeplinirilor prevăzute de reglementările de supraveghere și efectuarea unei evaluări preliminare a conformității în acest domeniu la oferirea de noi produse/servicii;
- Monitorizarea și controlul riscului CSB/CFT prin analizarea fluxurilor de informații primite de la nivelul I și alte funcții de control legate de cerințele operaționale de combatere a spălării banilor și prin implementarea controalelor de monitorizare a riscurilor și verificarea constantă a adecvării acestora;
- Efectuarea autoevaluării AML prin desfășurarea activităților preliminare necesare completării așa-numitelor Chestionare „de sistem” și „Operaționale” precum și pentru determinarea riscului rezidual;
- Raportarea la Topul Organismelor Corporative și Autorităților de Supraveghere, mai precis pregătirea de a raporta anual Organismelor Corporative și Consiliului de Supraveghere precum și pregătirea de a raporta periodic asupra activităților desfășurate și a oricăror solicitări specifice din partea Autorităților de Supraveghere;
- Furnizarea de cursuri de formare specifice CSB/CFT prin organizarea unui plan de instruire adecvat împreună cu celelalte funcții corporative responsabile de formare. Scopul este realizarea unei pregătiri continue a angajaților și colaboratorilor.

Regulile și responsabilitățile specifice ale Companiei cu privire la acest proces sunt detaliate în documentul intern
document, „Proceduri interne de combatere a spălării banilor și a finanțării terorismului”.

4.2 – MANAGEMENTUL RELAȚIILOR CU AUTORITĂȚILE DE SUPRAVEGHERE PENTRU COMBATEREA SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI

Procesul de management al relațiilor de reglementare CSB/CFT este procesul prin care se desfășoară activități în cadrul Companiei pentru a gestiona, analiza, dirija și monitoriza toate comunicările cu autoritățile de reglementare în probleme legate de combaterea spălării banilor și a finanțării terorismului. Obiectivul este de a supraveghea aceste activități, inclusiv arhivarea documentelor într-un singur depozit.

În cadrul acestui proces se desfășoară următoarele activități:

- Gestionarea relatiilor cu Autoritatile de Supraveghere (Anti-Spalarea Banilor), gestionarea, analizarea si adresarea comunicatiilor si solicitarilor din partea Autoritatilor de Supraveghere privind conformitatea in domeniu;
- Gestionarea rapoartelor de Supraveghere împotriva spălării banilor, prin pregătirea fluxului și transmiterea rapoartelor de Supraveghere împotriva spălării banilor;

- Gestionarea procedurilor administrative legate de combaterea spălării banilor prin examinarea cererilor reconvenționale aferente procedurilor administrative notificate Societății de către autoritățile competente (GdF și UIF) precum și reprezentarea Societății în fața MEF, prin răspunderea de recensământ a procedurilor în aplicația aferentă și pentru alocarea la Provizionul pentru Riscuri și Taxe și eventuale sancțiuni cu bugetul de plată.

Regulile și responsabilitățile specifice ale Companiei cu privire la acest proces sunt detaliate în documentul intern, „Proceduri interne de combatere a spălării banilor și a finanțării terorismului".

4.3 – GESTIONAREA CERINȚELOR OPERAȚIONALE PENTRU COMBATEREA SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI

Procesul de management al cerințelor operaționale CSB/CFT este procesul prin care se desfășoară următoarele activități în cadrul Companiei pentru a se conforma cerințelor de reglementare:

- limitarea utilizării numerarului și a titlurilor la purtător, prin îndeplinirea cerințelor de reglementare privind limitările de utilizare a numerarului și a obligațiunilor/titlurilor la purtător;
- gestionarea obligațiilor adecvate de due diligence a clienților, prin executarea activităților de due diligence a clienților (sau de due diligence îmbunătățită) în cazurile stabilite de Legea italiană (Decretul legislativ 231/07 și modificările ulterioare) în funcție de profilul de risc al clienților, sprijinirea Rețelei Societății în îndeplinirea obligațiilor cerute de legile și reglementările actuale, oferind suport pentru gestionarea structurilor și reglementărilor companiei. și contrapărți bancare și financiare pentru a permite stabilirea și menținerea relațiilor;
- gestionarea obligațiilor de raportare a tranzacțiilor suspecte, prin desfășurarea activităților de raportare a tranzacțiilor suspecte prin executarea delegărilor de autoritate ale Consiliului de Administrație (ex art. 36 D.Lg. 231/07) și monitorizarea solicitărilor primite de la UIF;
- gestionarea obligațiilor privind finanțarea combaterii terorismului, prin definirea metodologiei de screening care vizează asigurarea implementării măsurilor restrictive Uniunii și naționale, verificarea transpunerii actualizărilor Listei de sancțiuni precum și raportarea către autoritățile competente (naționale și de supraveghere) cu privire la măsurile restrictive (UIF, MAECI și MEF) cu privire la măsurile de înghețare a capitalului (ex-Decret legislativ) și realizarea cerințelor de funcționare necesare;109/07;
- gestionarea obligațiilor de păstrare a datelor, prin verificarea fiabilității Sistemului Informațional prin actualizarea Archivio Unico Informatico (AUI), efectuarea oricăror revizuiri, trimiterea periodică a datelor agregate către UIF și transmiterea către UIF și Banca Italiei a notificărilor impuse de reglementări;
- monitorizarea aplicării corespunzătoare a sancțiunilor financiare internaționale (embargouri financiare);
- monitorizarea continuă a clienților cu cel mai mare risc de spălare a banilor și finanțare a terorismului, monitorizarea cererilor de investigare ulterioară a clienților care expun Compania la riscuri mari de spălare a banilor, activarea, acolo unde este necesar, a procesului de evaluare a tranzacțiilor suspecte și a procesului de screening a clienților care expun Compania la riscuri mari de spălare a banilor.

Regulile și responsabilitățile specifice ale Companiei cu privire la acest proces sunt detaliate în documentul intern
document, „Proceduri interne de combatere a spălării banilor și a finanțării terorismului”.

5 - CADRE ORGANIZAȚIONALE ȘI ORGANISME DE CONTROL

Pentru a gestiona eficient riscul de spălare a banilor și finanțare a terorismului, precum și de încălcare a Măsurilor restrictive, Societatea a identificat funcțiile, resursele și procedurile organizatorice care sunt în concordanță și proporționale cu tipul și dimensiunea activității desfășurate, complexitatea organizațională precum și caracteristicile operaționale.

Monitorizarea riscurilor legate de spălarea banilor și finanțarea terorismului este asigurată:

- de către Funcția Anti Spălare a Banilor a Rox Pay S.r.l., a cărei responsabilitate este atribuită Șefului Funcției AML care raportează direct Directorului General.
- De către Membrul organului de conducere responsabil cu combaterea spălării banilor, cu responsabilitate încredințată CEO-ului, care este principalul punct de contact între șeful Funcției de combatere a spălării banilor și Consiliul de Administrație și se asigură că Consiliul deține informațiile necesare pentru a înțelege pe deplin relevanța riscurilor de spălare a banilor pentru care Rox Pay S.r.l. este expus.

Monitorizarea riscurilor legate de încălcarea Măsurilor restrictive:

- este asigurată de Personalul Superior responsabil cu Măsurile Restrictive, a cărui responsabilitate este atribuită Șefului Departamentului AML, care supraveghează adecvarea și eficacitatea politicilor, procedurilor interne și controalelor referitoare la managementul Măsurilor Restrictive, sancțiunilor și embargourilor. Personalul Superior propune, în colaborare cu funcțiile relevante ale companiei, modificări organizatorice și procedurale necesare și/sau adecvate pentru a asigura monitorizarea adecvată a riscului de încălcare a măsurilor restrictive, sancțiunilor și embargourilor.

În conformitate cu reglementările în vigoare, Societatea și-a stabilit structura organizatorică și guvernanța corporativă astfel încât să protejeze interesele Societății, asigurând, în același timp, un management sănătos și prudent și să evite riscul - chiar dacă neintenționat.
- a oricărei implicări directe în acte de spălare de bani și/sau finanțare a terorismului.

În acest scop, în conformitate cu Sistemul de Control Intern adoptat de Companie, Consiliul de Administrație și Auditorii Statutari sunt implicați în atenuarea riscurilor de mai sus prin sarcini și responsabilități clar definite.

În plus, Compania a înființat o unitate centralizată pentru gestionarea sistemului intern de raportare a încălcărilor, cu responsabilitatea de a supraveghea activitățile de primire, analiză și evaluare a alertelor transmise de către angajați prin procedura de Avertizare.

6 – REVIZUIREA ȘI ACTUALIZAREA POLITICII

Funcția de combatere a spălării banilor revizuiește politica cel puțin anual, o actualizează dacă și acolo unde este necesar și pregătește textul spre aprobare de către Consiliul de Administrație la propunerea Directorului General.

Orice modificare a Politicii aprobate de Consiliul de Administratie al Rox Pay S.r.l. sunt ulterior implementate în cadrul Companiei prin rezoluție a conducerii superioare, aliniind responsabilitățile, procesele și regulile interne.