ROX PAY S.R.L.
POLÍTICA DE PREVENÇÃO E COMBATE À BRANQUEAGEM DE DINHEIRO E FINANCIAMENTO DO TERRORISMO

1 - VISÃO GERAL

1.1 – PRINCIPAIS REGULAMENTOS E ORIENTAÇÕES

Este documento estabelece a Política da Rox Pay S.r.l. no combate à lavagem de dinheiro, ao financiamento do terrorismo e à violação de medidas restritivas[1]e se aplica a Rox Pay S.r.l. e suas operações.

As normas devem ser consideradas complementares e aplicáveis desde que não entrem em conflito com as disposições emitidas pelas Autoridades locais.

1.2 – DESTINATÁRIOS E MÉTODOS DE IMPLEMENTAÇÃO

A Política se aplica a Rox Pay S.r.l.

2 – PRINCÍPIOS GERAIS

2.1 QUADRO REGULATÓRIO LBC-CFT

O branqueamento de rendimentos de atividades ilegais e criminosas é uma das formas mais graves de crime nos mercados financeiros e é uma área de interesse específico para atividades criminosas organizadas.

O branqueamento de capitais tem um impacto negativo significativo em toda a economia: o reinvestimento de receitas ilegais em atividades legais e o conluio entre indivíduos ou instituições financeiras e organizações criminosas afetam profundamente os mecanismos de mercado, prejudicam a eficiência e a equidade das atividades financeiras e têm um efeito enfraquecedor na economia. O financiamento de atividades terroristas pode envolver a utilização de receitas derivadas legalmente e/ou provenientes de atividades criminosas.

A natureza mutável do branqueamento de capitais e do financiamento do terrorismo, também facilitada pela evolução contínua da tecnologia, exige uma adaptação constante das medidas de prevenção e contraste.

O quadro regulamentar de combate ao branqueamento de capitais (AML) e ao financiamento do terrorismo (CFT) baseia-se num conjunto abrangente de fontes reguladoras nacionais, da UE e internacionais.

A nível internacional, um contributo fundamental para a harmonização regulamentar veio do Grupo de Acção Financeira (GAFI), o principal organismo internacional activo na luta contra o branqueamento de capitais, o financiamento do terrorismo e a proliferação de armas de destruição maciça.

1 Conforme definido nas Orientações da EBA (EBA/GL/2024/14): "As medidas restritivas da União referidas no artigo 2.º, ponto 1, da Diretiva (UE) 2024/1226 e as medidas restritivas nacionais adotadas pelos Estados-Membros em conformidade com a sua ordem jurídica nacional (na medida em que se apliquem às instituições financeiras).

No cumprimento das suas responsabilidades, o GAFI estabeleceu um conjunto de normas internacionais, as "40 recomendações", às quais foram acrescentadas mais 9 recomendações especiais em 2001 para combater o financiamento do terrorismo internacional. O tema foi totalmente revisto em Fevereiro de 2012 com a adopção das Normas Internacionais de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo e da Proliferação, então resumidas nas já referidas "40 Recomendações".

No âmbito da luta contra a proliferação de armas de destruição maciça, as Nações Unidas prepararam um conjunto de medidas para combater o financiamento de programas de proliferação, incluindo a proibição de ajudar ou financiar qualquer pessoa envolvida em tais atividades.

Ao implementar as Resoluções adotadas no âmbito das Nações Unidas, a União Europeia emitiu um conjunto de disposições a fim de implementar medidas restritivas, como o congelamento de fundos e recursos económicos de pessoas ou entidades envolvidas no desenvolvimento de atividades de armas de destruição maciça sensíveis à proliferação.

O GAFI desenvolveu diretrizes para implementar as sanções financeiras adotadas pelas Nações Unidas.

Medidas específicas que abordam a proliferação de armas de destruição maciça foram recentemente incluídas nas Recomendações, em conformidade com as resoluções do Conselho de Segurança das Nações Unidas.

As diretrizes da UE sobre a prevenção da utilização do sistema financeiro para lavagem de dinheiro e financiamento do terrorismo estão contidas na Diretiva 2015/849 da UE[2]do Parlamento Europeu e do Conselho de 20 de maio de 2015 (Quarta Diretiva Anti-Lavagem de Dinheiro), conforme alterada pela Diretiva da UE 2018/843 (Quinta Diretiva Anti-Lavagem de Dinheiro), bem como nos Regulamentos e Diretrizes emitidos periodicamente, respectivamente, pela UE – União Europeia e pela EBA – Autoridade Bancária Europeia.

A nível nacional, a prevenção e o combate ao branqueamento de capitais e ao financiamento do terrorismo são regulados pelas seguintes leis primárias:

- **Decreto Legislativo Italiano nº. 109 de 22 de junho de 2007 e alterações e suplementos subsequentes que estabelecem "Disposições para prevenir, combater e reprimir o financiamento do terrorismo e a atividade de países que ameaçam a paz e a segurança internacional", implementando a Diretiva 2015/849 conforme modificada pela Diretiva da UE 2018/843;**
- **Decreto Legislativo Italiano nº. 231, de 21 de novembro de 2007, e subsequentes alterações e suplementos que implementam a Diretiva 2015/849/UE, que altera a Diretiva 2009/138/CE e 2013/36/UE, alterada pela Diretiva 2018/843/UE relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais e financiamento do terrorismo (doravante, também o Decreto).**

2 A Diretiva UE 2024/1640 do Parlamento Europeu e do Conselho, de 31/05/2024, relativa aos procedimentos a instaurar pelos Estados-Membros para prevenir a utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, a ser transposta até 10 de julho de 2027, altera a Diretiva UE 2019/1937 e revoga a Diretiva UE 2015/849.

Finalmente, existe também legislação secundária a nível nacional que foi emitida pelo Banco de Itália
e a Unidade de Informação Financeira ("UIF"), e está contida nas seguintes fontes regulatórias:

- **Disposição de 26 de março de 2019 que estabelece as disposições de execução em matéria de organização, procedimentos e controlos internos destinados a prevenir a utilização de intermediários financeiros e outras entidades para efeitos de branqueamento de capitais e financiamento do terrorismo, conforme alterada pela Disposição do Banco de Itália de 1 de agosto de 2023;**
- **Disposição de 28 de março de 2019 que estabelece instruções sobre comunicações objetivas;**
- **Disposição de 30 de julho de 2019 que estabelece disposições de execução em matéria de vigilância da clientela, conforme alterada pela disposição do Banco de Itália de 13 de junho de 2023;**
- **Disposição de 24 de março de 2020 que estabelece disposições de execução para armazenamento e disponibilidade de documentos, dados e informações relativas ao combate ao branqueamento de capitais e ao financiamento do terrorismo;**
- **Disposição de 25 de agosto de 2020 que estabelece disposições para a apresentação de relatórios agregados de LBC;**
- **Disposição de 12 de maio de 2023 sobre indicadores de anomalia para intermediários para facilitar a identificação de transações suspeitas, em vigor a partir de 1 de janeiro de 2024.**

Rox Pay S.r.l. (doravante "a Empresa") implementa os regulamentos acima em seus documentos regulatórios internos.

A nível geral, a Empresa adoptou a presente "Política de combate ao branqueamento de capitais e ao financiamento do terrorismo" (doravante a "Política") como expressão do seu compromisso no combate aos referidos fenómenos criminais a nível internacional, prestando especial atenção ao contraste, na consciência de que a prossecução da rentabilidade e da eficiência deve ser aliada à monitorização contínua e eficaz da integridade das estruturas corporativas.

A Política aplicada na Empresa descreve a política adotada pela Rox Pay S.r.l. de acordo com as regras e princípios ditados pelas disposições regulamentares nacionais e da UE, em conformidade com as normas internacionais relevantes e é implementado em conjunto com os procedimentos internos de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo, o Código de Ética e os procedimentos internos que implementam a legislação primária e secundária local em vigor, especificando processos, funções e responsabilidades.

A atual Política foi aprovada pelo Conselho de Administração da Companhia.

As diretrizes AML e CFT são aplicadas pela Rox Pay S.r.l. em coerência com as leis aplicáveis.

A Empresa está empenhada em cumprir este quadro regulamentar, bem como quaisquer disposições de implementação emitidas pelo Banco de Itália sobre a devida diligência do cliente, retenção de dados e informações, organização, procedimentos, controlos e controlos reforçados contra o financiamento de programas que visam a proliferação de armas de destruição em massa.

A Empresa está profundamente empenhada em garantir que a organização operacional e o sistema de controlo sejam completos, adequados, funcionais e fiáveis para a supervisão estratégica, para proteger a Empresa da tolerância ou mistura de formas de ilegalidade que possam prejudicar a sua reputação e afetar a sua estabilidade.

Por estas razões, Rox Pay S.r.l. adotou regras organizacionais e comportamentais e sistemas de monitoramento e controle que visam garantir o cumprimento da legislação vigente por parte dos órgãos de administração e controle, funcionários, colaboradores e consultores da Companhia. Estes controlos também são consistentes com as regras e procedimentos estabelecidos pelo código de proteção de dados pessoais.

A Empresa apoia-se também em indicadores de anomalias e padrões de comportamentos irregulares no ambiente económico e financeiro, que são emitidos ao longo do tempo pela Unidade de Informação Financeira (UIF) relativamente a potenciais atividades de branqueamento de capitais e financiamento do terrorismo.

2.2 - O QUADRO REGULATÓRIO RELATIVO A MEDIDAS RESTRITIVAS E EMBARGOS

Todas as medidas restritivas estabelecidas para combater o financiamento do terrorismo e todas as actividades ilícitas ou suspeitas que ameaçam a paz e a segurança internacionais podem ser comerciais, tais como restrições à importação/exportação de/para um país, ou financeiras, tais como o bloqueio parcial ou total da transferência de fundos, mas também limitações operacionais e congelamento de fundos.

As medidas restritivas incluem sanções financeiras internacionais, também conhecidas como embargos, implementadas pelo Estado italiano, agências estrangeiras (por exemplo, OFAC, UKSL) e organizações supranacionais (ONU, UE) através de uma série de obrigações que a Empresa é obrigada a cumprir. Certas medidas restritivas (sanções) são impostas a todos os Estados-Membros da ONU pelo Conselho para implementar as Resoluções adoptadas pelo Conselho de Segurança da ONU ao abrigo do Capítulo VII da Carta das Nações Unidas. Além disso, as sanções podem ser adotadas, ou decididas autonomamente, pela União Europeia através de regulamentos do Conselho, que são imediatamente aplicáveis em cada Estado-Membro para garantir a sua aplicação atempada e simultânea.

A nível internacional, existem regulamentos que estabelecem proibições ou restrições específicas ao investimento em determinados sectores industriais ou à importação/exportação de/para "países de risco elevado ou significativo". Em particular, diz respeito às resoluções do Conselho de Segurança das Nações Unidas (CSNU) ao abrigo do Artigo 41 do Capítulo VII da Carta das Nações Unidas, através das quais são impostas medidas restritivas em relação a pessoas e/ou países.

No que diz respeito à legislação comunitária, as principais disposições são:

- o Regulamento 2021/821 do Parlamento Europeu e do Conselho, de 20 de maio de 2021[3] **e alterações subsequentes, através das quais é estabelecido um regime da UE para controlar as exportações, transferências, corretagem e trânsito de produtos de dupla utilização;**

3 que substituiu o Regulamento 428/2009/CE do Conselho, de 5 de maio de 2009

- o Regulamento (UE) 2023/1113 do Parlamento Europeu e do Conselho, de 31 de maio de 2023, relativo às informações que acompanham as transferências de fundos e de determinados criptoativos e que altera a Diretiva (UE) 2015/849 (reformulação);
- o Regulamento (UE) 2024/886 do Parlamento Europeu e do Conselho, de 13 de março de 2024, que altera os Regulamentos (UE) n.º 260/2012 e (UE) 2021/1230 e as Diretivas 98/26/CE e (UE) 2015/2366 no que diz respeito às transferências instantâneas de créditos em euros;
- a Diretiva (UE) 2024/1226 do Parlamento Europeu e do Conselho, de 24 de abril de 2024, relativa à definição de infrações penais e penas pela violação de medidas restritivas da União e que altera a Diretiva (UE) 2018/1673, transposta para o direito italiano pelo Decreto Legislativo 211/2025.
- **Orientações da Autoridade Bancária Europeia sobre políticas, procedimentos e controlos internos para garantir a implementação de medidas restritivas nacionais e da União (EBA/GL/2024/14)**[4];
- **Diretrizes da Autoridade Bancária Europeia sobre políticas, procedimentos e controlos internos para garantir a implementação de medidas restritivas nacionais e da União, em conformidade com o Regulamento (UE) 2023/1113 (EBA/GL/2024/15) relativo às informações que acompanham as transferências de fundos e determinados criptoativos, e que altera a Diretiva (UE) 2015/849**[5].

Finalmente, a nível nacional, os embargos são regulados da seguinte forma:

- **Legislação Primária:**
  - **Decreto Legislativo n.º 221/2017, que alterou e simplificou os procedimentos de autorização para exportar produtos e tecnologias de dupla utilização e sanções sobre embargos comerciais, bem como todos os tipos de operações de exportação de materiais em proliferação.**
- **Legislação Secundária:**
  - **Disposição do Banco de Itália de 12 de maio de 2023 que contém indicadores de anomalia para intermediários, a fim de facilitar a identificação de transações suspeitas.**

Por último, todos os regulamentos emitidos pelas Autoridades dos EUA são relevantes para a atividade da Empresa, tendo em conta os aspetos reputacionais e a referência a estes regulamentos em compromissos contratuais que envolvam a potencial aplicação de sanções com efeito extraterritorial (as chamadas 'sanções secundárias' dos EUA). Tais disposições regulamentares estão contidas no USA Patriot Act6 e nas medidas relativas às sanções económicas e comerciais emitidas pelo Governo dos EUA através do Gabinete de Controlo de Activos Estrangeiros (OFAC) do Departamento do Tesouro.[6]

4 que o Banco da Itália declarou sua intenção de cumprir na Nota nº. 48, de 8 de abril de 2025 e aplicável a partir de 30 de dezembro de 2025.

5 que o Banco da Itália declarou sua intenção de cumprir na Nota nº. 52 de 19 de maio de 2025 e aplicável a partir de 30 de dezembro de 2025.

6 Lei federal dos EUA de 26 de outubro de 2001, oficialmente intitulada "Unindo e Fortalecendo a América através do Fornecimento de Ferramentas Apropriadas Necessárias para Interceptar e Obstruir o Terrorismo Lei de 2001".

3 – MODELOS E METODOLOGIAS DE GRUPO

3.1 – ASPECTOS GERAIS

O quadro regulamentar nacional estabelecido para a acção preventiva contra o branqueamento de capitais, o financiamento do terrorismo e as violações das Medidas Restritivas baseia-se numa série de obrigações

que os destinatários são obrigados a respeitar:

- obrigação de adotar estruturas organizacionais, procedimentos e medidas de controle interno adequados;
- obrigação de adotar procedimentos consistentes e coerentes para análise e avaliação dos riscos relacionados à lavagem de dinheiro, financiamento do terrorismo e violação das Medidas Restritivas, bem como estabelecer supervisão, controles e procedimentos necessários para mitigar e gerenciar esses riscos;
- obrigação de due diligence do cliente, através da qual a Empresa adquire e verifica informações relativas à identidade de um cliente e de qualquer beneficiário efetivo, bem como a finalidade e a natureza pretendida da relação ou da transação, assegurando ao mesmo tempo a monitorização constante de todas as transações realizadas pelo cliente;
- uma abordagem baseada no risco, em que as obrigações de devida diligência do cliente são divididas em diferentes graus de devida diligência, proporcionais ao perfil de risco do cliente;
- obrigação de conservar documentos, dados e informações de forma a permitir a sua aquisição atempada, transparência, integralidade, inalterabilidade e integridade, e uma acessibilidade global e rápida;
- obrigação de comunicação de transações suspeitas;
- obrigação de abster-se de iniciar qualquer novo relacionamento com clientes, realizar transações ocasionais ou manter um relacionamento existente com clientes quando a devida diligência não tiver sido realizada ou se houver suspeita de que possa haver uma ligação com lavagem de dinheiro ou financiamento do terrorismo;
- obrigação de notificar o Ministério da Economia e Finanças das infrações referidas nos artigos 49.º e 50.º do Decreto Legislativo 231/07, e de cumprir as limitações à utilização de numerário e títulos ao portador;
- monitorizar todas as transações com pessoas singulares e coletivas e/ou com países incluídos nas Listas do Conselho da União Europeia (UE), na Lista do Gabinete de Controlo de Ativos Estrangeiros (OFAC), na Lista de Sanções do Reino Unido (UKSL)[7], na Lista Consolidada de Sanções do Conselho de Segurança das Nações Unidas (ONU) nas Disposições emitidas pelas Autoridades Nacionais contendo medidas restritivas específicas para o combate ao terrorismo;
- monitorizar as transações celebradas com países considerados não cooperantes em matéria fiscal, de supervisão financeira e de combate ao branqueamento de capitais, geralmente designados por "paraísos fiscais" ou "centros financeiros offshore";
- adotar programas apropriados de treinamento de pessoal para garantir a implementação e aplicação adequada de leis e regulamentos;
- obrigação de fornecer à UIF "comunicações objetivas" de acordo com instruções sobre métodos e frequência de comunicações;

7 A lista OFSI (Gabinete de Implementação de Sanções Financeiras HMT) foi encerrada em 28 de janeiro de 2026; a partir dessa data, a Lista de Sanções do Reino Unido é a única fonte oficial para todas as designações de sanções do Reino Unido.

- obrigação de divulgar quaisquer violações ou infrações que possam chegar ao conhecimento dos Órgãos de Controle no desempenho de suas tarefas;
- obrigação de adotar procedimentos para gerenciar denúncias internas de violações apresentadas pelos colaboradores (Whistleblowing).

No que diz respeito às atividades de financiamento antiterrorista, a legislação italiana exige que as partes obrigadas façam o seguinte:

- congelamento de fundos e recursos económicos de certas pessoas incluídas nas listas da UE;
- informar a Unidade de Informação Financeira (UIF) das medidas aplicadas para o congelamento de fundos, ou a Unidade Especial de Polícia Cambial da Guardia di Finanza (Polícia Financeira) em caso de recursos económicos;
- informar a UIF sobre transações suspeitas, relações comerciais e quaisquer outras informações disponíveis sobre as partes incluídas nas listas negras publicadas pela própria UIF;
- comunicar transações suspeitas que, com base nas informações disponíveis, estejam direta ou indiretamente relacionadas com atividades de financiamento do terrorismo.

No que diz respeito às sanções internacionais (os chamados Embargos) e à exposição a medidas restritivas, a legislação exige que sejam tomadas certas medidas, incluindo, mas não se limitando a:

- dados pessoais e controles transacionais sobre operações ligadas a importações e/ou exportações realizadas por clientes, destinadas a bloquear importações/exportações de ou para um país, e regulamentos correspondentes. A proibição pode ser geral, envolvendo todos os tipos de mercadorias, a menos que seja especificamente autorizada, ou restrita a certos tipos de mercadorias, por exemplo. armamentos (ver código aduaneiro);
- restrições totais ou parciais às transferências financeiras de/para um país;
- exigência de autorização prévia para realização de transferências;
- obrigação de notificar transferências (de saída ou de entrada);
- proibição de financiar, fornecer assistência financeira ou disponibilizar empréstimos subsidiados ao Governo (directamente ou, em alguns casos, indirectamente através de empresas afiliadas ou participação em instituições financeiras internacionais);
- proibição de financiar clientes que operam com países sancionados;
- implementação de medidas restritivas contra cidadãos russos e bielorrussos;
- a rastreabilidade dos controlos realizados nas operações provenientes ou dirigidas a países, pessoas e entidades sujeitas a restrições.

3.2 - DEVIDA DILIGÊNCIA DO CLIENTE

3.2.1 – Aspectos gerais

A Empresa toma todas as medidas de devida diligência do cliente quando:

- estabelecer relações comerciais;
- realizar operações ocasionais, organizadas pelos clientes, tais como transferências

bancárias ou outras operações iguais ou superiores ao limite designado aplicável, independentemente de a operação ser realizada numa única operação ou em várias operações relacionadas ou consistir numa transferência de fundos, excedendo os limites legais;

- existe uma suspeita de branqueamento de capitais ou de financiamento do terrorismo, independentemente de qualquer derrogação, isenção ou limiar designado que possa ser aplicável;
- existam dúvidas sobre a integralidade, fiabilidade e veracidade da informação ou documentação previamente adquirida para efeitos de identificação de um Cliente.

Obrigações de devida diligência:

- são cumpridos:
  - junto de novos clientes antes do estabelecimento de uma relação contínua ou da realização de uma transação ocasional;
  - junto dos clientes existentes, sempre que a devida diligência seja apropriada face a uma alteração no nível de risco de branqueamento de capitais ou de financiamento do terrorismo associado ao cliente ou quando existam suspeitas ou dúvidas quanto à exatidão ou adequação da informação anteriormente obtida do cliente;

- e consiste nas seguintes atividades:
  - identificar o Cliente, o beneficiário efetivo e o executor e verificar a sua identidade com base em documentos, dados ou informações obtidos de fonte confiável e independente;
  - obter e avaliar informações sobre o propósito e a natureza pretendida da relação comercial;
  - realizando monitoramento contínuo durante todo o relacionamento com o cliente.

Para tal, a Empresa - através dos seus colaboradores e/ou através de agentes/assessores financeiros autorizados a fazer ofertas fora do estabelecimento comercial e que entram em contacto direto com o Cliente - obtém as informações exigidas pela regulamentação e recolhe qualquer outra documentação relevante conforme especificado nesta Política e nos documentos processuais da Empresa.

A Empresa aplica medidas de due diligence ordinárias, simplificadas ou reforçadas de acordo com a abordagem baseada no risco aplicada aos clientes.

3.2.2 - Integração remota do cliente

Nos casos em que a Empresa utilize métodos de identificação remota conforme permitido pelo Decreto Legislativo nº. 231/07, artigo 19.º, n.º 1, alínea a), pontos 2 e 5, adota procedimentos especiais para o cumprimento das suas obrigações de devida diligência, também tendo em conta o risco de fraude associado ao roubo de identidade. Neste caso, a identificação baseia-se na aquisição do certificado de assinatura eletrónica qualificada, que é gerado após um processo de identificação efetuado através de:

- a utilização do Sistema Público de Identidade Digital (SPID) ou Bilhete de Identidade Eletrónico;
- por meio de técnicas e procedimentos de identificação eletrônica seguros e regulamentados, autorizados ou reconhecidos pela Agência para a Itália Digital.

Em todos os casos, o processo de identificação remota envolve a recolha de dados de identificação do cliente e de qualquer executor em formato eletrónico, bem como a realização de verificações e controlos da autenticidade dos dados, para além dos previstos para a

identificação presencial, de acordo com uma abordagem baseada no risco, nomeadamente através de contacto telefónico num número certificado (chamada de boas-vindas) ou de uma transferência de dinheiro efetuada pelo cliente através de um intermediário bancário e financeiro sediado em Itália.

Com vista a limitar a exposição a potenciais riscos de branqueamento de capitais e/ou fraude, não é permitido estabelecer relações bancárias à distância com pessoas colectivas ou singulares que actuem em nome de uma pessoa colectiva, a menos que tenham sido identificadas pessoalmente (presencialmente).

Não é permitido o estabelecimento de relações bancárias à distância com clientes não residentes em Itália.

3.2.3 – Avaliação Pré-Implementação e acompanhamento contínuo dos processos de abertura de relacionamento remoto.

Os processos de identificação e integração remota de clientes estão formalizados e detalhados em normativo interno. O modelo de supervisão desses processos inclui:

I. a avaliação preliminar da solução de integração remota (a chamada Avaliação de Pré-Implementação[8]) destinado a:
   (i) avaliar a adequação da solução em termos da integralidade e exatidão dos dados e documentos a recolher, bem como da fiabilidade e independência das fontes de informação utilizadas;
   (ii) avaliar o impacto da utilização da solução nos riscos empresariais, incluindo riscos operacionais, reputacionais e jurídicos, através do envolvimento das funções técnicas e especializadas relevantes;
   (iii) identificar medidas de mitigação e ações corretivas para cada risco identificado;
   (iv) definir testes ex ante para avaliar os riscos de fraude e TIC e testes ponta a ponta sobre o funcionamento da solução.

II. monitoramento contínuo da solução de onboarding adotada por meio de controles periódicos e orientados a eventos para garantir seu bom funcionamento ao longo do tempo (o chamado Monitoramento Contínuo).

III. a revisão da avaliação preliminar na solução de onboarding remoto (a chamada Avaliação Pré-Implementação) quando ocorrerem alterações estruturais na solução adotada ou determinados eventos como:
   (i) mudanças na exposição a riscos nas áreas de combate à lavagem de dinheiro e combate ao financiamento do terrorismo, bem como embargos;
   ii) deficiências detectadas para que nossa solução funcione;
   iii) um aumento nas tentativas de fraude;
   (iv) alterações na legislação.

3.2.4 – Obrigações simplificadas de due diligence

Geralmente, a Empresa utiliza uma abordagem baseada no risco para identificar os tipos de clientes aos quais podem ser aplicadas medidas simplificadas de due diligence. Isto inclui casos em que estão presentes "indicadores de baixo risco", conforme indicado no Anexo 1 da Disposição do Banco de Itália sobre a devida diligência do cliente de 30 de julho de 2019 (doravante "A Disposição").

8 Nota n.º 32 de 13 de junho de 2023 através da qual o Banco de Itália declarou a sua intenção de cumprir as Diretrizes da EBA (EBA/GL/2022/15) sobre a utilização de soluções remotas de integração de clientes.

Os "indicadores de baixo risco" relevantes para a aplicação de um procedimento simplificado de due diligence baseiam-se no tipo de cliente, executor ou beneficiário efetivo, na área geográfica de residência ou sede, no produto, serviço ou canal de distribuição específico.

Em detalhe, os tipos de clientes considerados de baixo risco de branqueamento de capitais, aos quais se pode aplicar a devida diligência simplificada, incluem:

- Administrações Públicas, Instituições ou Organismos que exerçam funções públicas, nos termos da legislação da União Europeia;
- Empresas cotadas num mercado regulamentado e sujeitas a requisitos de divulgação, incluindo a garantia de transparência adequada da propriedade efetiva final;
- as instituições financeiras e de crédito da Comunidade Europeia listadas no Artigo 3 (2) do Decreto Anti-Lavagem de Dinheiro - exceto aquelas nas letras i), o), s), v)[9]— e as instituições financeiras e de crédito residentes em Estados-Membros ou países terceiros com sistemas eficazes de branqueamento de capitais e de financiamento do terrorismo;
- Clientes, executores ou beneficiários efetivos residentes ou estabelecidos em áreas geográficas com baixo risco de branqueamento de capitais.

A Empresa não aplica medidas simplificadas de due diligence do cliente quando:

- surjam dúvidas, incertezas ou inconsistências relativamente aos dados e informações identificativas recolhidas durante a identificação do cliente, executor ou beneficiário efetivo;
- as condições para a devida diligência simplificada do cliente deixam de ser cumpridas com base nos indicadores de risco previstos no decreto anti-branqueamento de capitais e na regulamentação secundária relevante;
- o acompanhamento da globalidade das operações realizadas pelo cliente e da informação recolhida ao longo da relação exclui uma modalidade de baixo risco;
- a suspeita de lavagem de dinheiro ou financiamento do terrorismo ainda surge.

A Função de Combate ao Branqueamento de Capitais tem responsabilidade exclusiva pela avaliação e autorização de medidas simplificadas de due diligence do cliente, realizadas seguindo todos os passos exigidos para o processo normal de due diligence do cliente - incluindo a obrigação de identificar e verificar a identidade do cliente, do executor e do Beneficiário Efectivo, e adquirir todos os dados e documentos necessários ao seu registo completo (e.g., nome, estatuto jurídico, sede social e, quando aplicável, código fiscal) - embora reduzindo o seu nível de profundidade, âmbito e frequência.

3.2.5 – Obrigações reforçadas de devida diligência

A Empresa aplica medidas reforçadas de vigilância do cliente na presença de clientes ou situações com maior risco de branqueamento de capitais ou financiamento do terrorismo e em todos os casos referidos no artigo 24.º do Decreto. Estas medidas reforçadas incluem, entre outras coisas, o envolvimento de funções de responsabilidade proporcionais ao nível de risco identificado em relação ao cliente.

9 i) Os corretores a que se refere o artigo 201.º do TUF; o) Os mediadores de seguros referidos no artigo 109.º, n.º 2, alíneas a), b) e d), do PAC, que exerçam a sua atividade nos ramos de atividade referidos no artigo 2.º, n.º 1, do PAC; s) sociedades fiduciárias inscritas no registo instituído nos termos do artigo 106.º do TUB; v) os consultores financeiros a que se refere o artigo 18-bis do TUF e as consultorias financeiras a que se refere o artigo 18-ter do TUF.

Relativamente aos clientes de private banking, a Companhia avalia os fatores de risco específicos inerentes à natureza da sua atividade e aplica medidas reforçadas de due diligence com base na informação global disponível e nas avaliações efetuadas.

O envolvimento da Função de Combate ao Branqueamento de Capitais é necessário nos seguintes casos:

- pessoas singulares e colectivas incluídas nas listas de pessoas ou entidades sujeitas a medidas de congelamento de fundos ao abrigo de regulamentos ou decretos europeus nos termos do Decreto Legislativo 109/07, bem como aquelas que lhes estão estreitamente associadas;
- uma relação bancária de correspondente transfronteiriço estabelecida com um banco ou instituição localizada num país terceiro, com base em fatores geográficos de alto risco (conforme relatado no Anexo 2 das disposições do Banco de Itália sobre a devida diligência do cliente);
- relacionamentos ou transações em que o cliente ou beneficiário final é uma pessoa politicamente exposta[10];
- situações que envolvam elementos de risco que exijam a aplicação de medidas específicas de confidencialidade;
- situação com maior risco de branqueamento de capitais ou financiamento do terrorismo devido a contingências objetivas, ambientais ou subjetivas;
- clientes classificados como "Trust", serviços de Transferência de Dinheiro e Câmbios Virtuais;
- Sociedades Fiduciárias, exceto conforme disposto no parágrafo 3.4;

Além disso, antes de iniciar, continuar ou manter uma relação contínua com Pessoas Politicamente Expostas ou Entidades Correspondentes de terceiros países, é necessário obter a autorização adequada do Diretor Geral ou do seu delegado, após obter o parecer da Função de Combate ao Branqueamento de Capitais. No caso dos delegados nos termos do artigo 25 do Decreto Legislativo 231/07 pertencentes à Função de Combate ao Branqueamento de Capitais, esta autorização está incluída no processo de devida diligência reforçada.

Em todos os outros casos, a aplicação de medidas reforçadas é proporcional ao nível de risco atribuído ao cliente. Se o risco for considerado médio/alto, ou se estiverem presentes determinados fatores de risco independentemente da pontuação atribuída, é necessário o envolvimento do Responsável da unidade de negócio responsável pela gestão comercial do cliente.

Exemplos de tais casos são:

- clientes pessoas jurídicas com Executor identificado como PEP ou PEP indireto, independentemente do perfil de risco;
- serviços oferecidos através de redes de agentes financeiros, consultores financeiros, empreiteiros e agentes;
- clientes classificados como Fundação/Organizações sem fins lucrativos;
- clientes pessoa jurídica durante a fase de onboarding;
- clientes com notícias negativas durante a fase de onboarding ("Notícias Adversas");

10 Pessoas Politicamente Expostas (PEPs): conforme elenca o art. 1, parágrafo 2, letra dd) Decreto Legislativo 231/07.

- clientes residentes ou sediados em países terceiros de alto risco ou no caso de relações contínuas, serviços profissionais e operações envolvendo países de alto risco;
- sociedades que tenham emitido ações ao portador ou que possuam sociedade emissora de ações ao portador na sua estrutura de cadeia de controle;
- relacionamentos ou transações em que o cliente e o beneficiário final ocupam cargos públicos diferentes daqueles listados para pessoas politicamente expostas[11];
- empresas pertencentes a trustes, sociedades fiduciárias, fundações, sociedades por ações através de múltiplos níveis de participação ou participações cruzadas;
- clientes que exerçam um tipo de atividade económica particularmente exposta ao risco de branqueamento de capitais ou em setores de atividade "controversos"[12]ou atividades comerciais com uso intensivo de dinheiro, como troca de dinheiro por ouro, câmbio de dinheiro, jogos/apostas, incluindo on-line, indústria de armamento, mineração, coleta e eliminação de resíduos, produção de energia renovável, empresas que operam no setor de criptoativos, construção, aquisição de instrumentos farmacêuticos;
- clientes participantes em contratos públicos ou beneficiários de financiamento público (cuidados de saúde, construção, recolha e eliminação de resíduos, produção de energias renováveis, mineração, fornecimento de instrumentos farmacêuticos);
- nos casos de clientes que tenham adquirido a cidadania de um Estado-Membro ou obtido direitos de residência num Estado-Membro (UE) através de um programa de cidadania por investimento ou de um programa de residência por investimento;
- nos casos de entidades jurídicas clientes residentes num país da UE, onde os direitos de propriedade da empresa são detidos - direta ou indiretamente - em mais de 40% por uma entidade jurídica, organização ou organismo estabelecido na Rússia, ou por uma pessoa singular com residência ou cidadania russa.

O envolvimento do responsável pela unidade de negócio responsável pela gestão comercial do cliente é também necessário em caso de erros informáticos que possam impedir o cálculo em tempo real do risco de branqueamento de capitais do cliente.

As medidas reforçadas de devida diligência incluem a aquisição de informações adicionais sobre o cliente, o executor e o beneficiário efetivo, investigando o propósito e a natureza do relacionamento e aumentando a frequência dos procedimentos destinados a garantir o monitoramento contínuo durante o relacionamento contínuo.

Em total conformidade com a legislação vigente e com o disposto nos procedimentos internos de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo e em consonância com o Código de Ética da Companhia, a Companhia não apoia transações com clientes que atuam em setores controversos que
(i) não estejam em conformidade com a legislação nacional em vigor e (ii) não sejam, quando aplicável, previamente autorizados pelas autoridades nacionais italianas competentes, em particular:

- a produção, trânsito e/ou comercialização de materiais de armamento;
- a produção e venda de maconha light, locais de entretenimento adulto;

11 Cargos públicos que não sejam exercidos por Pessoas Politicamente Expostas (PEP) conforme referido na nota 1), aplicando-se a todos os que exerçam cargos em, mas não limitados a, organismos públicos, consórcios, associações de natureza pública, conforme listado na secção A 8) do Anexo 2 da Disposição.
12 um setor económico é "controverso" se os bens/serviços fabricados/oferecidos e/ou as formas como são produzidos/oferecidos contrastam com os valores amplamente partilhados de ética e sustentabilidade, mesmo quando os serviços ou atividades são legais e, portanto, não contrastam com as obrigações legais.

- atividades comerciais com uso intensivo de dinheiro, além das listadas acima, como instituições de caridade e ONGs não regulamentadas, produção de metais e pedras preciosas, remessas de dinheiro.

Além disso, a Empresa presta especial atenção ao cumprimento das medidas restritivas implementadas pelo Estado italiano, organismos estrangeiros (por exemplo, OFAC, UKSL) e/ou organismos supranacionais (ONU, UE). Estas medidas podem ser de natureza comercial (por exemplo, bloqueio de importações/exportações) ou de natureza financeira, como o bloqueio parcial/total de transferências de dinheiro de ou para um país específico ou limitações de operações e/ou congelamento de fundos detidos com intermediários financeiros.

Para cumprir as obrigações estabelecidas no Decreto Legislativo Italiano 109/07 - que visa prevenir e combater o financiamento do terrorismo e as atividades de países que ameaçam a paz e a segurança internacionais, através da aplicação de medidas restritivas para "congelar" fundos e recursos económicos detidos por pessoas singulares e coletivas, grupos e entidades especificamente identificados pelas Nações Unidas e pela União Europeia ("sujeitos designados") - e as obrigações reforçadas de devida diligência estabelecidas no Decreto Legislativo Italiano 231/07, a Empresa adotou automática procedimentos de controle. Estes procedimentos são capazes de verificar a consistência entre os dados de identificação do cliente obtidos através do processo de due diligence e os contidos nas listas produzidas pela UE e outras instituições e organismos internacionais, tais como:

- os indivíduos a quem seja confiado cargo público de destaque ou que tenham deixado de exercer o cargo há menos de um ano (PEP), seus familiares e aqueles que com eles tenham vínculos estreitos, conforme definição do art. 1 c. 2ª letra dd do Decreto Legislativo 231/07 (PEPs residentes e não residentes);
- indivíduos residentes em Itália que ocupam cargos públicos, que não se enquadram na definição de PEP, mas que estão, no entanto, expostos a um risco significativo de corrupção e branqueamento de capitais;
- pessoas físicas e jurídicas que operam, mesmo parcialmente, em Estados que não impõem medidas e regulamentos equivalentes, de acordo com as diretrizes do Banco da Itália ou de outras instituições nacionais ou supranacionais envolvidas na prevenção do crime;
- pessoas singulares e coletivas sujeitas a medidas de embargo ou congelamento de fundos/recursos económicos e ativos financeiros (Listas de Sanções ONU, UE, UKSL, OFAC).

3.3 - PERFIL DO CLIENTE

A Empresa adota procedimentos adequados destinados a definir o perfil de risco de branqueamento de capitais e de financiamento do terrorismo (PR) atribuível a cada cliente, com base na informação adquirida e nas análises efetuadas, tendo como referência tanto os elementos de avaliação indicados na Provisão como outros elementos que possam ser adotados pela própria Empresa ao longo do tempo (o chamado perfil).

Com base no perfil do cliente, que também é realizado periodicamente, a Empresa aplica medidas padrão ou aprimoradas, que incluem o envolvimento de funções de responsabilidade proporcionais ao nível de risco identificado do cliente. O parecer prévio da Função de Combate ao Branqueamento de Capitais é exigido de acordo com as responsabilidades definidas no

documento interno "Procedimentos Internos de Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo".

A classificação de clientes para due diligence simplificada é autorizada pela Função de Combate ao Branqueamento de Capitais, a pedido do Responsável da Unidade Operacional de Negócio.

Nesse caso, o âmbito e a frequência dos requisitos são reduzidos, expirando a verificação após 8 anos, independentemente da classificação de risco, a menos que as condições para a aplicação da devida diligência simplificada deixem de ser cumpridas.

Adicionalmente, a Empresa implementou um procedimento informático para avaliar o perfil de risco do cliente e definir consistentemente um prazo de reavaliação adequado ao nível de risco calculado; a periodicidade da reavaliação depende do processo identificado na última avaliação realizada ou, na ausência de questionário KYC, do perfil de risco do cliente, conforme especificado abaixo:

<table>
<tr><th>Classe de risco (RP)</th><th>Pontuação</th><th>Processo de due diligence</th><th>Função de validação</th><th>Frequência de reavaliação</th></tr>
<tr><td>Clientes classificados como sujeitos a due diligence simplificada</td><td>NA</td><td>Simplificado</td><td>Aceitação automática/Gerente de Unidade de Negócio (*)</td><td>8 anos</td></tr>
<tr><td>Imaterial</td><td><=5</td><td rowspan="2">Padrão</td><td rowspan="2">Aceitação Automática</td><td>8 anos</td></tr>
<tr><td>Baixo</td><td>>=6 e <=12</td><td>6 anos</td></tr>
<tr><td>Médio</td><td>>=13 e <=24</td><td rowspan="2">Aprimorado</td><td rowspan="2">Gerente de Unidade de Negócios (**)</td><td>2 anos</td></tr>
<tr><td>Alto</td><td>>=25</td><td>1 ano</td></tr>
<tr><td colspan="2">No caso de elementos de risco específicos (***)</td><td>Aprimorado</td><td>Função de validação AML</td><td>1 ano</td></tr>
</table>

(*) fornecido caso a pontuação de risco calculada ou resultante do KYC realizado seja pelo menos média. (**) fornecido mesmo na presença de elementos de risco definidos que mantenham o perfil de risco abaixo da média.
(***) prestados mesmo na presença de Pessoas Jurídicas com PR >39, caso exerçam atividades comerciais relacionadas com compra de ouro, jogos e apostas e recolha e eliminação de resíduos (códigos ATECO de alto risco) e/ou sejam objeto de auditorias/investigações.

3.4 - FERRAMENTAS PARA APOIAR A DUE DILIGENCE

A Companhia implementou ferramentas tecnologicamente avançadas para apoiar os processos de combate à lavagem de dinheiro, juntamente com as aplicações tradicionais já em uso:

- Automação Robótica de Processos (RPA) aplicada a atividades de coleta de dados nas áreas de due diligence de clientes e reporte de transações suspeitas;
- Motor de Inteligência Artificial, baseado em componentes estatísticas e indicadores preditivos (Predict Index AML, Reputational Index e Criminal Infiltration Index) construídos com técnicas de Data Analytics, aplicados ao processo regular de avaliação de clientes;
- Plataforma de inteligência Cogito, aplicativo utilizado para coleta de notícias, documentos e informações textuais para busca de notícias adversas sobre clientes sujeitos a due diligence;
- Rozes, ferramenta de inteligência de dados que, ao analisar demonstrações financeiras em tempo real, permite identificar empresas cujo balanço e indicadores financeiros

sejam semelhantes aos encontrados em empresas sujeitas a infiltrações criminosas.

Além disso, no âmbito das ferramentas avançadas acima mencionadas, foram identificados determinados "eventos desencadeadores", destinados a interceptar eventos relativos ao cliente e/ou relacionamentos relacionados, determinando uma variação no prazo de validade da "Avaliação do Cliente - KYC", por exemplo:

- em caso de alteração dos dados cadastrais do beneficiário efetivo e do representante legal;
- em caso de alteração do Perfil de Risco devido à presença de determinados fatores de risco elevado entre os previstos na Provisão;
- no caso de um beneficiário efetivo assumir a função de PEP, ou do registo de um novo beneficiário efetivo de PEP;
- em caso de delegação a pessoa física da relação de clientela dada a pessoa enquadrada como PEP;
- em caso de discrepância entre o beneficiário efetivo inscrito no registo e as provas colhidas em extratos da Câmara de Comércio;
- em caso de controlos de segundo nível pela Função AML.

A responsabilidade pelo processo de due diligence de um cliente cabe à unidade de gestão de relacionamento do cliente, que normalmente lida com o estabelecimento de novos relacionamentos contínuos, executa quaisquer transações ocasionais, reavalia periodicamente os clientes existentes e garante o monitoramento contínuo do relacionamento com o cliente.

3.5 - OBRIGAÇÕES DE ABSTENÇÃO

A Empresa abstém-se de estabelecer, executar ou continuar o relacionamento, operações e serviços profissionais (a chamada obrigação de abstenção) no caso de uma impossibilidade objetiva de realizar a devida diligência do cliente, avaliando se deve reportar uma transação suspeita à UIF.

Nos casos em que a abstenção não seja possível, por existir uma obrigação legal de execução da operação que não pode ser adiada ou se a sua recusa puder dificultar a investigação, a Empresa é, no entanto, obrigada a comunicar imediatamente a operação suspeita.

Além disso, se após uma avaliação mais aprofundada ou a jusante do processo de devida diligência reforçada, surgirem elementos de alto risco que possam afetar o perfil jurídico e/ou reputacional da Empresa, a Empresa reserva-se o direito de limitar ou terminar a relação comercial com o cliente. Essas limitações podem dizer respeito, ou seja, ao acesso do cliente a determinados tipos de produtos ou resultar na interrupção dos serviços oferecidos pela Empresa em conexão com a conta/relacionamento.

As medidas de vigilância do cliente adotadas pela Empresa não impedem/negam, no entanto, o acesso a serviços financeiros a clientes ou categorias inteiras de clientes de alto risco que teriam direito a eles nos termos da legislação em vigor, exceto nos casos expressamente previstos pelo Decreto Legislativo 231/07, no que diz respeito à proibição de manter relações com determinados tipos de entidades.

A Empresa não estabelece relações de correspondente com um banco de fachada e abstém-se de estabelecer relações com entidades que permitam o acesso a relações de correspondente com um banco de fachada. Não deve estabelecer relações comerciais com entidades cuja estrutura de propriedade (societária, fiscal e financeira) seja caracterizada por um elevado grau de opacidade que impeça a identificação clara do beneficiário efetivo ou da natureza e finalidade da estrutura.

Para este fim, a Empresa toma todas as medidas para garantir que não colabora deliberada e conscientemente com instituições financeiras que, por sua vez, operam com bancos de fachada.

Além disso, a Empresa abstém-se de estabelecer ou continuar relações comerciais com pessoas particularmente expostas ao risco de branqueamento de capitais/financiamento do terrorismo, tais como:

- Sociedades fiduciárias com sede num país indicado pelo GAFI como de maior risco de branqueamento de capitais ou que não adotem medidas consistentes com as obrigações impostas pelo Decreto Legislativo 231/07 ou pelas Diretivas Europeias;
- Trusts para os quais não estão disponíveis informações adequadas, precisas e atualizadas sobre o beneficiário efetivo do trust e a sua natureza e finalidade;
- Empresas de apostas, incluindo jogos on-line, cassinos e operadores de bingo para os quais não foram emitidas e/ou verificadas autorizações e/ou licenças exigidas pela legislação italiana e internacional;
- Entidades afiliadas e agentes de prestadores de serviços de pagamento (referidos na definição do art.1 c. 2 letra nn) e instituições de moeda electrónica que não cumpram o disposto no Capítulo V do Decreto Legislativo 231/07 nos artigos 43.º e seguintes;
- Sociedades por quotas ou sociedades controladas por ações ao portador, sediadas em Países de alto risco;
- Clientes que atuam na produção e venda de maconha light ou em locais de entretenimento adulto, caso não consigam verificar as autorizações exigidas por lei.

A Companhia utiliza todas as informações adquiridas durante o processo de due diligence sobre seus clientes e suas transações para determinar se uma transação ou relação comercial está, direta ou indiretamente, ligada a pessoas ou entidades envolvidas em lavagem de dinheiro, financiamento do terrorismo ou no desenvolvimento de armas de destruição em massa, e de forma alguma apoia transações envolvendo armas controversas e/ou proibidas por tratados internacionais,
por exemplo armas nucleares, biológicas e químicas, bombas de fragmentação, armas contendo urânio empobrecido, minas terrestres antipessoal.

No que diz respeito à produção, trânsito e/ou comercialização de materiais de armamento diferentes dos acima mencionados, a Empresa poderá apoiar transações que tenham sido devidamente autorizadas pelas autoridades competentes e estejam em conformidade com a legislação aplicável e vigente.

3.6 – RELATÓRIO DE TRANSAÇÕES SUSPEITAS

Sempre que a Empresa suspeite ou tenha motivos razoáveis para suspeitar que uma operação

de branqueamento de capitais ou de financiamento do terrorismo foi ou está a ser conduzida ou tentada:

- submete um relatório de transação suspeita à Unidade de Inteligência Financeira (UIF), se a transação tiver sede em Itália;

- se a transação tiver sede noutro País, cumpre o disposto na legislação local e, quando esta preveja a aplicação de medidas equivalentes às previstas na legislação da UE, informa prontamente o Responsável pelo Combate ao Branqueamento de Capitais, tomando todas as precauções necessárias para proteger a identidade das pessoas que denunciam a transação suspeita.

A Empresa implementou procedimentos e processos para monitorar, identificar e relatar atividades suspeitas de acordo com o prazo e os métodos exigidos pela legislação aplicável.

Os colaboradores comunicam prontamente qualquer conhecimento ou suspeita de branqueamento de capitais, financiamento do terrorismo ou outras atividades criminosas, ou rendimentos de atividades criminosas, independentemente da sua dimensão, de acordo com o modelo organizacional e modos de funcionamento atualizados previstos no regulamento interno de referência. Até que o processo de reporte esteja concluído, a Empresa abstém-se de executar a transação, a menos que tal seja impossível por existir uma obrigação legal de aceitar a escritura ou a execução da operação não possa ser adiada devido à condução normal dos negócios ou quando possa obstruir as investigações. Nestes casos, o relatório é apresentado imediatamente após a execução da transação.

Os motivos de suspeita incluem as características, dimensão e natureza da operação, a tentativa de divisão da operação e qualquer outra circunstância que chegue ao conhecimento dos colaboradores em consequência das suas funções, tendo também em conta o âmbito financeiro e a natureza do negócio realizado pelo sujeito da operação suspeita, com base nos elementos adquiridos nos termos da legislação anti-branqueamento de capitais (por exemplo, durante a devida diligência).

Para limitar o risco de envolvimento da Empresa – mesmo que não intencional – nas atividades ilegais acima mencionadas, é ativado um processo reforçado de due diligence nos acordos de transferência de fundos onde os intervenientes envolvidos neste tipo de transação (originador, beneficiário, os bancos envolvidos na transferência de fundos) podem levar à suspeita de branqueamento de capitais, financiamento do terrorismo ou violações de restrições internacionais aplicáveis a determinados bens, pessoas ou entidades.

A jusante do processo de comunicação, a Empresa poderá limitar e/ou interromper a relação comercial com os clientes, em particular quando tal relação possa constituir um risco legal ou de reputação significativo para Rox Pay S.r.l.

3.7 – RETENÇÃO DE DADOS

A Empresa retém todos os documentos e regista todos os dados obtidos através do processo de devida diligência do cliente, garantindo a rastreabilidade das transações dos clientes para facilitar as funções de controlo do Banco de Itália e da UIF, incluindo inspeções.

Para o efeito, a Rox Pay S.r.l., como intermediária financeira com sede em Itália, criou um Arquivo Electrónico Único (Archivio Unico Informatico ou AUI) que lhe permite fornecer informações ao Banco de Itália e à UIF de acordo com as normas técnicas especificadas no Anexo 2 das Disposições sobre retenção de dados. Este arquivo armazena eletronicamente todos os dados de identificação e outras informações relacionadas a relacionamentos comerciais contínuos e transações de clientes, conforme exigido pela legislação aplicável.

Neste sentido, em resposta às recentes atualizações introduzidas pelas "Disposições sobre

Retenção de Dados e Acesso a Documentos, Dados e Informações" e pelas "Disposições sobre Transmissão Agregada de Dados", a Empresa decidiu adotar determinados princípios de isenção de obrigações de registo conforme expressamente previstos. Em particular, os dados e informações relativos às operações realizadas por intermediários bancários e financeiros, que se enquadrem nos casos especificados no artigo

O artigo 8º das Disposições sobre Conservação de Dados e o artigo 3º das Disposições sobre Dados Agregados não são registados no Arquivo Electrónico Único.

Em relação aos requisitos de due diligence do cliente, a Empresa retém cópias ou registros de todos os documentos exigidos por um período de dez anos após o término do relacionamento comercial.

Quanto às transações e relações comerciais em curso, todas as provas e registos de apoio, por exemplo, documentos originais ou cópias admissíveis em processos judiciais, são conservados por um período de dez anos após a execução da transação ou após o término da relação comercial.

3.8 – MEDIDAS RESTRITIVAS DE REGARGÃO DE PREVENÇÃO

Dada a natureza, dimensão e complexidade do seu negócio, bem como a gama e tipo de serviços prestados, a Empresa está exposta ao risco de violação de medidas restritivas.

De forma a manter um sistema organizativo e processual que visa garantir o cumprimento das medidas restritivas internacionais comunitárias e nacionais, o risco de incumprimento das medidas restritivas é avaliado pela Função de Combate ao Branqueamento de Capitais com base em fatores geográficos, de clientes, de produtos/serviços e de canais de distribuição, assegurando a monitorização constante da eficácia do sistema, garantida também através da realização periódica de um exercício de autoavaliação, que permite a identificação de eventuais ações corretivas em resposta à deteção de problemas críticos existentes e/ou à adoção de medidas adequadas de prevenção e mitigação de riscos.

A Companhia estabeleceu procedimentos e processos para monitorar, identificar e reportar atividades que violem medidas restritivas, com prazos e métodos consistentes com os requisitos legais.

Os controlos existentes sobre pessoas/entidades e transações são realizados através de um processo de triagem automatizado, que é realizado tanto diariamente como durante a fase de onboarding, através de listas específicas – atualizadas duas vezes por dia – relativas a clientes, contrapartes, países e transações.

Existem processos para monitorar fluxos de entrada ou saída com países e/ou entidades sujeitas a sanções financeiras internacionais, com responsabilidades definidas entre os departamentos competentes.

É garantido que o pessoal seja adequadamente treinado e informado sobre as políticas, procedimentos e controles para cumprir as medidas restritivas.

4 – LISTA DE PROCESSOS CHAVE

4.1 – GESTÃO DE RISCOS DE LAVAGEM DE DINHEIRO E FINANCIAMENTO DO TERRORISMO

O processo de "Gestão do Risco de Lavagem de Dinheiro e Financiamento do Terrorismo" é o processo pelo qual as seguintes atividades são realizadas dentro da Companhia, a fim de mitigar o risco de não cumprimento dos requisitos de combate à lavagem de dinheiro e ao

financiamento do terrorismo:

- Identificar o risco de incumprimento dos requisitos ABC-CFT através da supervisão contínua das alterações na legislação e da avaliação dos impactos nos processos e procedimentos empresariais, bem como da identificação e avaliação dos riscos ABC-CFT utilizando uma abordagem baseada no risco;

- Gestão e mitigação do risco de branqueamento de capitais e financiamento do terrorismo através da implementação e monitorização de ações de mitigação do risco de incumprimento previstas no Plano Anual (Plano AML) ou identificadas pela Governação da Sociedade aplicadas por todas as funções de negócio relevantes na implementação de procedimentos (regulamentos internos, aplicações informáticas, processos operacionais, controlos);
- Verificações de conformidade (ex-ante e ex-post) nas áreas regulatórias atribuídas pela propriedade, através da definição e monitorização de indicadores de risco e da sua evolução ao longo do tempo. O objectivo é detectar possíveis situações de incumprimento, bem como realizar as actividades de controlo ex-ante e ex-post;
- Prestar aconselhamento e apoio em questões de LBC/CFT, participando em equipas de trabalho multifuncionais e prestando apoio quer às estruturas empresariais, quer aos Órgãos de Gestão de Topo em questões e processos empresariais onde o risco de branqueamento de capitais e financiamento do terrorismo seja relevante, realizando os cumprimentos previstos nos regulamentos de supervisão e realizando uma avaliação preliminar de conformidade nesta área na oferta de novos produtos/serviços;
- Monitorização e controlo do risco de LBC/CFT através da análise dos fluxos de informação recebidos do Nível I e de outras funções de controlo relacionadas com requisitos operacionais de combate ao branqueamento de capitais e através da implementação de controlos de monitorização de risco e da verificação constante da sua adequação;
- Realizar a autoavaliação de LBC através da realização de atividades preliminares necessárias ao preenchimento dos chamados Questionários "Sistêmico" e "Operacional", bem como à determinação do risco residual;
- Reportar aos Órgãos Sociais e às Autoridades de Supervisão, nomeadamente preparando-se para reportar anualmente aos Órgãos Sociais e ao Conselho Fiscal bem como preparar-se para reportar periodicamente as atividades desenvolvidas e quaisquer solicitações específicas das Autoridades de Supervisão;
- Fornecer cursos de formação específicos em matéria de LBC/CFT, organizando um plano de formação adequado em conjunto com as restantes funções corporativas responsáveis pela formação. O objetivo é conseguir uma formação contínua dos funcionários e colaboradores.

As regras e responsabilidades específicas da Companhia em relação a este processo estão detalhadas no regulamento interno
documento, "Procedimentos Internos de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo".

4.2 – GESTÃO DAS RELAÇÕES COM AS AUTORIDADES DE SUPERVISÃO NO COMBATE AO BRANQUEAMENTO DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO

O processo de Gestão de Relacionamento Regulatório AML/CFT é o processo pelo qual as atividades são realizadas dentro da Empresa para gerenciar, analisar, direcionar e monitorar todas as comunicações com reguladores sobre assuntos relacionados ao combate à lavagem de dinheiro e ao financiamento do terrorismo. O objetivo é fiscalizar essas atividades, incluindo o arquivamento de documentos em um único repositório.

As seguintes atividades são realizadas como parte deste processo:

- Gestão das relações com Autoridades de Supervisão (Anti-Lavagem de Dinheiro), gerindo, analisando e endereçando comunicações e solicitações de Autoridades de Supervisão relativas à conformidade no terreno;
- Gestão dos relatórios de Supervisão de combate à lavagem de dinheiro, através da elaboração do fluxo e envio dos relatórios de Supervisão de combate à lavagem de dinheiro;

- Tratamento de procedimentos administrativos relacionados com combate ao branqueamento de capitais através do exame de reconvenções relativas a processos administrativos notificados à Empresa pelas autoridades competentes (GdF e UIF), bem como representação da Empresa perante o MEF, sendo responsável pelo recenseamento dos processos na respetiva aplicação e pela afetação à Provisão para Riscos e Encargos e eventuais pagamentos de sanções, em coordenação com a Função Orçamental.

As regras e responsabilidades específicas da Companhia em relação a este processo estão detalhadas no documento interno "Procedimentos Internos de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo".

4.3 – GESTÃO DE REQUISITOS OPERACIONAIS DE COMBATE À LAVAGEM DE DINHEIRO E FINANCIAMENTO DO TERRORISMO

O processo de Gestão de Requisitos Operacionais AML/CFT é o processo pelo qual as seguintes atividades são realizadas dentro da Empresa, a fim de cumprir os requisitos regulamentares:

- limitar a utilização de numerário e títulos ao portador, cumprindo os requisitos regulamentares relativos às limitações à utilização de numerário e obrigações/títulos ao portador;
- gerir as obrigações adequadas de due diligence do cliente, executando as atividades de due diligence do cliente (ou due diligence reforçada) nos casos estabelecidos pela lei italiana (Decreto Legislativo 231/07 e alterações subsequentes) dependendo do perfil de risco dos clientes, apoiando a Rede da Empresa no cumprimento das obrigações exigidas pelas leis e regulamentos vigentes, e prestando apoio às estruturas da Empresa na gestão das relações com clientes e contrapartes bancárias e financeiras, a fim de permitir o estabelecimento e manutenção de relacionamentos;
- gerir as obrigações de comunicação de transações suspeitas, realizando as atividades de comunicação de transações suspeitas, executando as delegações de autoridade do Conselho de Administração (ex art. 36 Decreto Legislativo 231/07) e monitorizando os pedidos recebidos da UIF;
- gerir as obrigações relativas ao financiamento do combate ao terrorismo, definindo a metodologia de triagem destinada a garantir a implementação de medidas restritivas da União e nacionais, verificando a transposição das atualizações da Lista de Sanções, bem como reportando às Autoridades competentes (nacionais e de supervisão) sobre medidas restritivas (UIF, MAECI e MEF) sobre medidas de congelamento de capitais (ex-Decreto Legislativo 109/07) e realizando os requisitos operacionais necessários;
- gerir as obrigações de retenção de dados, verificando a fiabilidade do Sistema de Informação através da atualização do Archivio Unico Informatico (AUI), fazendo quaisquer revisões, enviando periodicamente dados agregados à UIF e transmitindo à UIF e ao Banco de Itália as notificações exigidas pelos regulamentos;
- monitorar a implementação adequada de sanções financeiras internacionais (embargos financeiros);
- monitorização contínua dos clientes com maior risco de branqueamento de capitais e financiamento do terrorismo, monitorização de pedidos de investigação adicional de clientes que potencialmente expõem a Empresa a elevados riscos de branqueamento de capitais, ativando, sempre que necessário, o processo de avaliação de transações suspeitas e o processo de triagem de clientes que potencialmente expõem a Sociedade a elevados riscos de branqueamento de capitais.

As regras e responsabilidades específicas da Companhia em relação a este processo estão detalhadas no regulamento interno

documento, "Procedimentos Internos de Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo".

5 - QUADROS ORGANIZACIONAIS E ÓRGÃOS DE CONTROLE

Para gerir eficazmente o risco de branqueamento de capitais e financiamento do terrorismo, bem como de violação das Medidas Restritivas, a Empresa identificou as funções, recursos e procedimentos organizacionais que são consistentes e proporcionais ao tipo e dimensão da atividade desenvolvida, à complexidade organizacional, bem como às características operacionais.

É assegurada a monitorização dos riscos relativos ao branqueamento de capitais e ao financiamento do terrorismo:

- pela Função Anti-Lavagem de Dinheiro da Rox Pay S.r.l., cuja responsabilidade é atribuída ao Chefe da Função AML que reporta diretamente ao Diretor-Presidente.
- Pelo Membro do órgão de administração responsável pelo Combate ao Branqueamento de Capitais, com responsabilidade atribuída ao CEO, que é o principal ponto de contacto entre o Chefe da Função de Combate ao Branqueamento de Capitais e o Conselho de Administração e garante que o Conselho dispõe das informações necessárias para compreender plenamente a relevância dos riscos de branqueamento de capitais para os quais a Rox Pay S.r.l. está exposto.

O monitoramento dos riscos relacionados à violação de Medidas Restritivas:

- é assegurada pelo Quadro Superior responsável pelas Medidas Restritivas, cuja responsabilidade é atribuída ao Chefe do Departamento AML, que supervisiona a adequação e eficácia das políticas, procedimentos internos e controlos relativos à gestão de Medidas Restritivas, sanções e embargos. O Quadro Superior propõe, em colaboração com as funções relevantes da empresa, as alterações organizacionais e processuais necessárias e/ou adequadas para garantir a monitorização adequada do risco de violação de medidas restritivas, sanções e embargos.

De acordo com a regulamentação em vigor, a Sociedade estabeleceu a sua estrutura organizacional e governo societário de forma a proteger os interesses da Sociedade e, ao mesmo tempo, assegurar uma gestão sã e prudente e evitar o risco - mesmo que involuntário - de qualquer envolvimento direto em atos de branqueamento de capitais e/ou financiamento do terrorismo.

Para o efeito, de acordo com o Sistema de Controlo Interno adotado pela Sociedade, o Conselho de Administração e os Revisores Oficiais de Contas estão envolvidos na mitigação dos riscos acima referidos através de tarefas e responsabilidades claramente definidas.

Além disso, a Companhia estabeleceu uma unidade centralizada para a gestão do sistema interno de denúncia de infrações, com a responsabilidade de supervisionar as atividades de recebimento, análise e avaliação de alertas encaminhados pelos colaboradores por meio do procedimento de Denúncia.

6 – REVISÃO E ATUALIZAÇÃO DA POLÍTICA

A Função de Combate ao Branqueamento de Capitais revê a política pelo menos anualmente, atualiza-a se e quando necessário e prepara o texto para aprovação pelo Conselho de Administração sob proposta do Diretor Geral.

Quaisquer alterações à Política aprovadas pelo Conselho de Administração da Rox Pay S.r.l. são posteriormente implementados em toda a Companhia por deliberação da alta administração, alinhando responsabilidades, processos e normas internas.