O presente "Modelo Global de Gestão de Riscos de Branqueamento de Capitais e Financiamento do Terrorismo" institui os princípios seguidos pela MaxPay no âmbito da Avaliação dos Riscos inerentes à atividade desenvolvida pela empresa

Modelo Global de Gestão de Riscos de Branqueamento de Capitais e Financiamento do Terrorismo

Versão 09 - Janeiro 2019

MAXPAY
Serviços de Pagamento, Lda

Visto e Aprovado pela Gerência
Data: ____ / ____ / _____

Assinaturas:

_____

_____

Carimbo:

Modelo Global de Gestão de Riscos de Branqueamento de Capitais e Financiamento do Terrorismo

O presente **"Modelo Global de Gestão de Riscos de Branqueamento de Capitais e Financiamento do Terrorismo"** institui os princípios seguidos pela MaxPay no âmbito da Avaliação dos Riscos inerentes à atividade desenvolvida pela empresa, saber:

- Princípios de Aceitação de Clientes;
- Princípios de Identificação de Clientes;
- Princípios de Análise e Monitorização de Entidades de Risco Elevado;
- Princípios de Gestão de Risco de Branqueamento de Capitais e de Financiamento de Terrorismo;
- Princípios de Execução de Ordens;
- Princípios de Conflitos de Interesses.

NOTA: entenda-se no presente contexto que a designação "cliente" compreende todas as entidades utilizadoras dos nossos serviços de pagamento, i.e., e conforme definição:

«Utilizador de serviços de pagamento» a pessoa que utiliza um serviço de pagamento a título de ordenante, de beneficiário ou em ambas as qualidades

Conteúdo

Modelo Global de Gestão de Riscos de Branqueamento de Capitais e Financiamento do Terrorismo

1. INTRODUÇÃO

O presente documento reúne um conjunto de Princípios denominados "Princípios de Compliance" que definem os aspetos básicos de atitude e de atuação dos colaboradores, através dos quais se pretende que as atividades da MaxPay sejam orientadas.

A razão da sistematização adotada para estes Princípios é baseada:

a) por um lado, atenta a necessidade de proporcionar aos colaboradores documentos concisos e mais acessíveis, favorecendo a respetiva utilização;

b) e por outro lado, reconhece-se que a definição sectorial de Princípios de Compliance enfoca mais adequadamente cada uma das realidades especificamente em causa;

Este documento não esgota o universo de instrumentos de Compliance, integrando um sistema de fontes onde se destacam as fontes de origem externa e interna e que serviu de base para a elaboração das normas internas relativas à matéria.

2. PRINCÍPIO DE ACEITAÇÃO DE CLIENTES

2.1. ENQUADRAMENTO

De acordo com os princípios gerais de prevenção e combate ao Branqueamento de Capitais e Financiamento do Terrorismo e em cumprimento da legislação nacional, das boas práticas internacionais e das recomendações do GAFI, e tendo em conta as melhores práticas em termos de atuação nos mercados, a MaxPay implementa princípios, práticas e procedimentos, cumprindo elevados padrões de ética e profissionalismo de forma a evitar que a instituição possa ser utilizada ou sujeita, intencionalmente ou não, a práticas criminosas e de outra natureza que possam sujeitar a MaxPay a níveis de risco operacional ou reputacional significativos.

Os elementos fundamentais dessas práticas incluem as regras de controlo e gestão dos riscos mais relevantes e, especificamente no que respeita ao relacionamento com os clientes, respetivos representantes ou operações, incluem programas de conhecimento dos seus Clientes (KYC - Know Your Customer) e são incluídas em quatro Princípios fundamentais neste domínio:

(1) Princípio de Aceitação de Clientes;
(2) Princípio de Identificação dos Clientes;
(3) Princípio de Análise e Monitorização de Clientes de Risco Muito Elevado e Elevado;
(4) Princípio de Gestão de Risco de Branqueamento de Capitais (Money Laundering) e de Financiamento do Terrorismo (Counter Terrorism Financing).

Neste sentido, a MaxPay:

i. Tem definido o tipo de Clientes que está disposta a aceitar;

ii. Assume como obrigação especial de diligência, procurar obter informações sobre a verdadeira identidade da pessoa por conta e em nome de quem o cliente atua, sempre que exista suspeita fundada de que os montantes tenham uma proveniência decorrente de atividades criminosas, nomeadamente, dos crimes de furto, roubo, burla, fabrico, importação e exportação, comércio de armas e explosivos, terrorismo, extorsão, corrupção, peculato, contrabando, tráfico e consumo de estupefacientes, substâncias psicotrópicas, precursores e preparados ou outras substâncias de efeitos similares

iii. Obtém com objetividade e rigor a sua identificação e mantém atualizados os elementos de identificação e de informação que recolhe no decurso da relação de negócio, uma vez esta iniciada;

iv. Monitoriza as transações processadas pelos clientes de forma a verificar a conformidade daquelas com o perfil expectável do tipo de cliente em causa;

v. Estabelece medidas de gestão de risco e de controlo de procedimentos que envolvem, entre outros aspetos, auditorias e revisões regulares e extensivas.

2.2. OBJECTIVO DO PRINCÍPIO DE ACEITAÇÃO DE CLIENTES

No âmbito dos procedimentos de combate ao branqueamento de capitais e ao financiamento do terrorismo e no cumprimento dos normativos regulamentares e das recomendações das entidades internacionais relevantes, a MaxPay desenvolve princípios e procedimentos claros de aceitação de Clientes, incluindo a descrição dos tipos de clientes que provavelmente possam envolver um risco mais elevado para a própria empresa.

No âmbito destes Princípios e Procedimentos são tomados em consideração fatores relevantes para a definição do nível de risco dos clientes, designadamente, o país de nacionalidade e/ou de origem, o perfil profissional/profissão e a sua eventual participação em atividades políticas, as transações que com ele podem estar associadas.

Neste sentido, este documento tem como objetivo definir o conjunto de critérios que devem orientar a empresa na aceitação ou recusa de relacionamento com potenciais clientes, na definição de critérios de aceitação condicionada de clientes e na definição de critérios de classificação do nível de risco dos clientes.

2.3. CATEGORIAS DE POTENCIAIS CLIENTES CUJA ACEITAÇÃO DEVE SER RECUSADA

Tendo como objetivo proteger a MaxPay de práticas que possam colocar em risco as suas atividades e de forma a proteger a sua reputação, a MaxPay recusa o estabelecimento e/ou manutenção com quaisquer potenciais/já existentes clientes que se enquadrem em alguma das seguintes categorias:

i) Pessoas cuja reputação, na comunicação social ou no mercado, surge habitualmente associada a atividades criminosas;

ii) Pessoas cuja atividade ou modo de vida levante suspeitas relativamente à origem do respetivo património;

iii) Pessoas que não colaborem com a MaxPay na disponibilização da informação requerida;

iv) Bancos de Fachada (instituição financeira que não tem presença física e que não se encontra integrado em nenhum grupo financeiro regulamentado no país).

Relativamente às entidades cuja aceitação como cliente seja recusada, a MaxPay prepara um processo de recusa que inclui todas as informações recolhidas sobre a entidade, bem como uma nota fundamentada dos motivos que originaram a não-aceitação. O processo é elaborado pelo Compliance Officer que equacionará, em face das informações recebidas, possíveis ações subsequentes no âmbito da legislação em vigor.

Do processo acima referido, poderá resultar a elaboração de uma Declaração de Identificação de Pessoas Designadas (DIPD), cuja submissão deve ocorrer sempre que a identidade de um cliente potencial, cliente, ou qualquer outra pessoa, grupo ou entidade envolvida numa relação de negócio ou numa operação se considere que corresponde ou seja suspeita de corresponder à identidade de uma pessoa, grupo ou entidade designada.

2.4. CATEGORIAS DE POTENCIAIS CLIENTES CUJA ACEITAÇÃO DEVE SER CONDICIONADA A PROCESSO ESPECIAL DE AUTORIZAÇÃO

A MaxPay tem um processo especial de aceitação de potenciais clientes, fazendo depender de especial autorização por parte da Gerência da empresa a aceitação de clientes que se enquadrem em alguma das seguintes categorias:

i) Pessoas relativamente às quais a MaxPay tenha classificado com nível elevado de risco de branqueamento de capitais;

ii) Pessoas Politicamente Expostas, nos termos do número seguinte.

O processo de aceitação condicionada abrange os casos em que o potencial Cliente seja gestor, acionista ou proprietário de qualquer entidade que prossiga qualquer das atividades vindas de enunciar.

2.5. PESSOAS POLITICAMENTE EXPOSTAS

O processo de aceitação condicionada de clientes referido no número anterior abrange, de forma especial:

i) As Pessoas Politicamente Expostas (PEP) que pretendam ser clientes da MaxPay no País;

ii) Os membros da família dos PEP, incluindo as pessoas que com estes convivam em situação de facto;

iii) Outras pessoas, que reconhecidamente tenham com os PEP ou respetivos familiares estreitas relações de natureza comercial ou societária;

iv) Outras pessoas titulares de outros cargos públicos relevantes;

Por PEP «Pessoas politicamente expostas» entendem-se as pessoas singulares estrangeiras que desempenham, ou desempenharam até há um ano, cargos de natureza política ou pública, bem como os membros próximos da sua família e pessoas que reconhecidamente tenham com elas estreitas relações de natureza societária ou comercial. Para os efeitos previstos na presente lei, consideram-se:

i. Altos cargos de natureza política ou pública:

1) Chefe de Estado;

2) Chefe de Governo;

3) Membros do Governo, designadamente ministros, secretários de Estado e vice-ministros;

4) Deputados ou membros de câmaras parlamentares;

5) Magistrados de tribunais superiores e de outros órgãos judiciais de alto nível, cujas decisões não possam ser objeto de recurso, salvo em circunstâncias excecionais;

6) Membros de órgãos de administração e fiscalização de bancos centrais;

7) Chefes de missões diplomáticas e postos consulares;

8) Oficiais de alta patente das Forças Armadas e da Polícia;

9) Membros dos órgãos de administração e de fiscalização de empresas públicas e de sociedades anónimas de capitais exclusiva ou maioritariamente públicos, institutos públicos, fundações públicas, estabelecimentos públicos, qualquer que seja o modo da sua designação, incluindo os órgãos de gestão das empresas integrantes dos sectores empresariais e locais;

10)Membros dos órgãos executivos de organizações de Direito Internacional.

ii. Membros próximos da família:

1) Cônjuge ou pessoas com as quais se encontrem a viver em união de facto;

2) Os pais, os filhos e os respetivos cônjuges ou pessoas com as quais se encontrem a viver em união de facto;

iii. Pessoas que reconhecidamente tenham com elas relações de natureza societária ou comercial:

1) Qualquer pessoa singular, que seja notoriamente conhecida como proprietária conjunta com o titular do cargo de natureza política ou pública de uma pessoa coletiva, de um centro de interesses coletivos sem personalidade jurídica ou que com ele tenha relações comerciais próximas;

2) Qualquer pessoa singular que seja proprietária do capital social ou dos direitos de voto de uma pessoa coletiva ou do património de um centro de interesses coletivos sem personalidade jurídica, que seja notoriamente conhecido como tendo como único beneficiário efetivo o titular do alto cargo de natureza política ou pública.

Independentemente do processo especial de KYC aplicável a estas categorias de clientes, a aceitação de PEP como Cliente da MaxPay depende sempre da autorização da Gerência da empresa.

2.6. CRITÉRIOS PARA A ATRIBUIÇÃO DE GRAU DE RISCO NO MOMENTO DA ACEITAÇÃO DE CLIENTES

São nomeadamente fatores suscetíveis de agravar o grau de risco especificamente aplicável a determinado potencial Cliente:

i) A geografia de residência ou de atividade do potencial Cliente, ou a origem/destino dos fundos pretendidos movimentar no âmbito de relação de negócios ou de uma transação ocasional;

ii) A sujeição do Cliente a processo condicionado de aceitação, nos termos do nº 2.4 supra;

iii) A circunstância de determinada entidade, pela respetiva atividade/profissão, estar sujeita à aplicação da legislação preventiva de branqueamento de capitais;

iv) A presença de quaisquer outros fatores ou circunstâncias que, para o efeito, hajam sido definidos pelo Compliance Officer.

Para efeitos do parágrafo antecedente:

A. São nomeadamente geografias de risco

i) todas aquelas objeto de embargos ou outro tipo de sanções decretados por quaisquer entidades de Direito Internacional com competência na matéria ou ainda

ii) todas aquelas insuscetíveis de poder ser qualificadas, em matéria de branqueamento de capitais ou de financiamento do terrorismo, como tendo regime equivalente ao nacional ("país terceiro equivalente"), e em especial os países considerados pelo GAFI como "High Risk and non-cooperative jurisdictions";

B. Sem prejuízo de outras, estão sujeitas à aplicação especial atenção preventiva de branqueamento de capitais as seguintes entidades, atividades ou profissões:

-entidades financeiras;
-concessionários de exploração de casinos;
-entidades que exerçam atividades de mediação imobiliária;
-comerciantes que transacionem em numerário;
-revisores e técnicos oficiais de contas, auditores, consultores fiscais;
-notários, conservadores de registos, advogados, solicitadores, em prática individual ou em sociedade que intervenham em operações tipificadas na legislação preventiva de branqueamento de capitais;
-outros prestadores de serviços.

A atribuição do grau de risco é efetuada de forma automática e em função dos critérios definidos pelo Compliance Officer, considerando os vários fatores relevantes, o qual tem a responsabilidade do combate ao branqueamento de capitais.

2.7. ELEMENTOS FUNDAMENTAIS NOS PRINCÍPIOS DE IDENTIFICAÇÃO E DE CONHECIMENTO DOS NOVOS CLIENTES (KYC)

A MaxPay exige a verificação da identidade do Cliente e, sendo o caso, dos respetivos representantes e/ou beneficiários efetivos, para efeitos da aceitação de qualquer Cliente e a realização de qualquer transação ocasional.

A MaxPay nunca permite a realização de quaisquer transações sem que se ache cabalmente verificada a identidade do Cliente.

No âmbito do processo de identificação e de conhecimento do Cliente, a MaxPay avaliará necessariamente, sem prejuízo de outros aspetos relevantes:

i) A finalidade e o propósito da(s) transação(ões) pretendidas efetuar;

ii) O perfil transacional expectável;

iii) As fontes de rendimento;

iv) A coerência e consistência de toda a informação existente sobre o Cliente.

3. PRINCÍPIO DE IDENTIFICAÇÃO DE CLIENTES

3.1. ENQUADRAMENTO

No cumprimento da legislação, em matéria de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo, a MaxPay implementa um conjunto de Princípios e procedimentos que previnem a utilização das suas operações para práticas de natureza criminosa e que possam ser indutoras de riscos operacionais e reputacionais acrescidos.

Neste sentido, o ato de identificação dos Clientes é um elemento da maior relevância na construção do processo de KYC – Know Your Customer que a MaxPay implementa no seu seio, de forma a proteger-se contra os riscos reputacional, operacional e legal e, ao mesmo tempo, como instrumento necessário para o cumprimento dos requisitos legais relativos ao branqueamento de capitais e financiamento do terrorismo.

3.2. OBJECTIVO E ÂMBITO DE APLICAÇÃO

Do conjunto dos Princípios implementados de forma a promover elevados padrões éticos e profissionais na sua atuação, inclui-se o Princípio de Identificação de Clientes, em que ficam

estabelecidos os elementos fundamentais a respeitar nos procedimentos de identificação dos seus clientes, seus representantes e beneficiários efetivos, que em conjugação com a aplicação dos princípios de KYC - Know Your Customer criam condições para uma correta aplicação da Princípio de Aceitação de Clientes e sua subsequente monitorização.

Este princípio determina que:

i) Os princípios básicos a que deve obedecer a identificação de todas as entidades com quem a MaxPay se relaciona em termos de negócio cumprem obrigatoriamente com os requisitos do legalmente estabelecido;

ii) O conjunto de documentos a obter por parte dos clientes/potenciais clientes que realizem transações com a MaxPay, nos termos legalmente definidos;

iii) Os requisitos de qualidade exigíveis a todos os documentos apresentados à MaxPay, comprovativos dos diversos elementos que os clientes visam atestar;

iv) A regularidade da atualização dos documentos inerentes ao Princípio de Identificação de Cliente em poder da MaxPay, relativamente aos clientes com quem tem relações continuadas de negócio e os períodos mínimos de manutenção e arquivo daqueles documentos.

Todos os colaboradores da MaxPay estão sujeitos ao cumprimento deste princípio, segundo os mais elevados padrões de ética e respeito pela confidencialidade da informação manuseada no desempenho das suas funções.

3.3. VERIFICAÇÃO DA IDENTIDADE

3.3.1. Princípios básicos

A identificação dos Clientes, no âmbito da atuação da MaxPay, implica o conhecimento de um conjunto de características, a seguir detalhadas, que estão muito para além dos elementos de identificação pessoal, em sentido estrito. Deste modo, o Princípio de Identificação de Clientes tem que ser entendido sempre na perspetiva lata potenciadora da anulação dos riscos antes referidos, e não numa abordagem minimalista e estrita, que não seja capaz de evitar as perdas resultantes desses riscos.

Os princípios da veracidade, da comprovação, da especialidade e da atualidade são elementos fundamentais do princípio de identificação de Clientes. Neste sentido, independentemente da tipologia e qualidade dos documentos requeridos aos Clientes para confirmação da sua identidade, em sentido lato, o princípio da veracidade refere a necessidade de, em cada momento, se conhecer

que não existe qualquer suspeita de que os elementos e informações que estão a ser fornecidos à MaxPay sejam falsos, nem procuram esconder realidades que, de outra forma, pudessem obstar a que a relação de negócio se estabelecesse nos moldes propostos.
O ato de identificação e comprovação dos elementos de identificação não se esgota no momento do estabelecimento da relação inicial: este ato corresponde a um processo permanente de atualização das novas realidades e características de identificação dos Clientes e de comprovação desses mesmos elementos sempre que a caducidade dos documentos se aproxima.

3.3.2. Elementos a obter

A própria legislação nacional, Instrutivos e Avisos publicados pelo Banco Nacional de Angola estabelecem um conjunto de deveres de identificação que são integrados na operação diária de todos os funcionários, rigorosamente seguidos no momento em que se torna necessária a identificação dos Clientes e escrupulosamente espelhados/refletidos no sistema informático de suporte à operativa da MaxPay (Trader).

A MaxPay nos seus normativos internos e em consonância com a legislação em vigor, estabelece os elementos fundamentais a obter no início do relacionamento de negócio e a manter com cada um dos Clientes com quem se relaciona.

Os elementos fundamentais do ato de identificação dos clientes são os detreminados na legislação em vigor a cada momento, transcritos/sistematizados no Manual de Procedimentos da MaxPay e refletidos no sistema informático da empresa.

Complementarmente, no âmbito da constituição do processo de KYC-Know Your Customer, a MaxPay deve ainda obter informação clara e verdadeira sobre:

i) a finalidade da relação de negócio que se pretende estabelecer;

ii) a origem e o destino dos fundos que se quer movimentar, quando e sempre que legalmente exigível;

iii) as fontes de rendimento e de património do Cliente, criando a convicção da sua licitude e

iv) o perfil transacional expectável, de forma a aferir o respetivo grau de risco de branqueamento de capitais ou o enquadramento do Cliente na Princípio de Aceitação de Clientes definida.

No caso de tal ser entendido relativamente aos Clientes e às transações que pela sua natureza ou características possam suscitar um maior risco de branqueamento de capitais ou financiamento do

terrorismo, a MaxPay promove um conjunto de procedimentos especiais e prepara um processo de KYC e acompanhamento/diligência reforçados. Estão nesta situação, designadamente, as relações estabelecidas com Pessoas Politicamente Expostas (PEP).

3.3.3. Qualidade dos documentos exigíveis

Os documentos e elementos de confirmação das informações de identificação definidos pelas leis, pelos regulamentos e pelos normativos internos aplicáveis serão sempre documentos originais, quer porque foram emitidos originariamente pelas entidades com capacidade para tal, quer porque resultam de cópias devidamente autenticadas com força pública.

No caso de documentos com origem fora do país (emitidos por outros países) deve ser reforçado o cuidado na análise da sua veracidade e da natureza respetiva. Os documentos apresentados devem ser originais ou, tal como quanto aos documentos nacionais, cópias devidamente autenticadas por entidades com natureza pública neste domínio.

Em caso algum, serão aceites documentos que apresentem rasuras, estragos ou danos visíveis em partes fundamentais ou, por qualquer razão, possam sugerir a suspeita de falsificação ou violação de elementos.

No caso de documentos redigidos em língua estrangeira deverá ser solicitada uma tradução oficial.

4. PRINCÍPIO DE ANÁLISE E MONITORIZAÇÃO DE ENTIDADES DE RISCO ELEVADO E MUITO ELEVADO

4.1. ENQUADRAMENTO

O Princípio de Aceitação de Clientes da MaxPay remete a atuação da empresa para as melhores práticas em termos de atuação nos mercados, as quais vinculam a empresa a elevados padrões de ética e deontologia profissional.

A adoção de medidas eficazes de Know Your Customer (KYC) constitui uma parte essencial de gestão de risco de branqueamento de capitais e financiamento do terrorismo por parte do MaxPay, minimizando riscos significativos, especialmente no que concerne ao risco reputacional.

4.2. OBJECTIVO/ÂMBITO DO PRINCÍPIO DE ANÁLISE E MONITORIZAÇÃO DE CLIENTES DE RISCO ELEVADO E MUITO ELEVADO

O presente documento tem como objetivo definir o conjunto de critérios que deverão orientar a MaxPay acerca dos procedimentos de aceitação, análise e monitorização daqueles que são os clientes considerados de alto risco exigindo um intensivo “customer due diligence” (CDD) ou a aplicação de

medidas reforçadas de "vigilância" e monitorização contínua, com base na avaliação de risco, devendo ainda abranger os mecanismos de controlo de execução que garantam a efetiva implementação dos procedimentos, tais como o processo de identificação e registo dos beneficiários efetivos e das Pessoas Expostas Politicamente (PEP), a filtragem de operações e ainda a monitorização de transações dos Clientes através dos aplicativos informáticos da MaxPay, com o objetivo último de mitigar o risco da MaxPay ser utilizada intencionalmente ou involuntariamente para as atividades de branqueamento de capitais.

4.3. METODOLOGIAS E PROCEDIMENTOS UTILIZADOS NA ANÁLISE E MONITORIZAÇÃO DE CLIENTES DE RISCO ELEVADO E MUITO ELEVADO

Uma abordagem baseada no risco é o método utilizado pela MaxPay com o intuito de identificar, gerir e mitigar o risco de branqueamento de capitais e financiamento do terrorismo e inclui métodos e sistemas de controlo adequados para avaliar e prevenir os mesmos. Ao mesmo tempo, complementarmente, contribui para a redução do risco de fraude, reduzindo o potencial de perdas financeiras assumido.

Assim, relativamente aos Clientes identificados com risco elevado, a MaxPay:

i) Define no seu Princípio de Aceitação, categorias de Clientes em que o estabelecimento de relações de negócio deva ser recusado ou condicionado a processo especial de autorização, estando nesta última incluídas as Pessoas Politicamente Expostas. Estas, em observância ao expresso na lei, e desde que averiguado o seu estatuto deverão ser submetidas a um processo KYC com informação detalhada, estando previsto a obrigatoriedade de requerer autorização da Gerência;

ii) Desenvolve uma operativa de validação de clientes, que consiste na confirmação por parte do Compliance Officer, da conformidade documental do processo de Cliente;

iii) O sistema informático possibilita a qualquer Colaborador comunicar ao Compliance Officer situações ou operações com elevado índice de suspeição, merecedoras por natureza de acompanhamento especialmente determinado. A informação deste repositório e a sua consulta estão disponíveis apenas para Colaboradores do Compliance Officer, na proporção das suas funções.

4.4. CRITÉRIOS DE ATUAÇÃO NA ANÁLISE E MONITORIZAÇÃO DE CLIENTES DE RISCO ELEVADO E MUITO ELEVADO

4.4.1. Abertura/cadastro de cliente de Risco Elevado e Risco Muito Elevado

Dado que uma parte da avaliação e prevenção dos riscos atrás referidos se baseiam na monitorização contínua do Cliente e das suas atividades, com base em critérios de risco estabelecidos, a MaxPay define que são submetidas a avaliação rigorosa do Compliance Officer todo o início de estabelecimento de relações de negócio de clientes cujo risco seja classificado como elevado, independentemente de outros critérios que possam vir a ser definidos a cada momento.

No caso dos PEP, a não obtenção ou recusa no fornecimento dos elementos considerados necessários, deverão determinar a recusa por parte da MaxPay da aceitação da relação comercial, devendo a ocorrência originar a constituição de um processo de análise aprofundado.

4.4.2. Pessoas politicamente expostas (PEP)

Sempre que se constate o estatuto de "PEP" de um cliente (conforme definido em 2.5), serão adotados procedimentos enunciados seguidamente.

Relativamente às operações realizadas com pessoas politicamente expostas e no seguimento do Dever de Diligência Reforçada, ao iniciar uma relação comercial, no âmbito do desenvolvimento da relação de negócio ou na execução de qualquer operação, a MaxPay:

a) Questionará o Cliente por forma a determinar se o mesmo se enquadra na classificação de PEP;

b) Na presença de um PEP, assegurará um processo reforçado de diligência com o objetivo de obter informações detalhadas acerca da origem do património e dos fundos envolvidos, devendo ser claramente indicados, entre outros:

i) O motivo de estabelecimento de relação de negócio;
ii) A origem dos fundos;
iii) Montante exato do(s) valor(es) que vão ser transacionados;
iv) Discriminação do rendimento.

Refira-se por último que considerando o risco acrescido de branqueamento ou de financiamento do terrorismo, devido ao seu perfil ou à natureza das operações que possam ser desenvolvidas, os PEP são objeto de um acompanhamento contínuo acrescido por parte da MaxPay ao longo da relação de negócio, que se aplica a quem, tendo deixado de ter a qualidade de PEP, continue a representar um risco acrescido para o MaxPay.

A MaxPay estende ainda, na generalidade e proporcionalmente, as diligências supra enunciadas para as Pessoas Expostas Politicamente aos titulares de elevados cargos públicos.

4.4.3. Beneficiários efetivos

Entende-se como BEF, abreviatura da designação "Beneficiário Efetivo", as pessoas singulares proprietárias últimas ou detentoras do controlo final de um cliente ou as pessoas no interesse da qual é efectuada uma operação.

4.4.4. Gestão de risco e execução das operações

As operações detetadas cuja desconformidade não seja justificada ou em que existam relevantes indícios ou suspeitas de ilícito originam por parte da MaxPay, independentemente de outras medidas, uma atuação imediata sobre o cliente.

As ações a desenvolver incluem, sem prejuízo de outras medidas adequadas, a comunicação às autoridades prevista na Lei, mediante a elaboração de uma Declaração de Operação Suspeita (DOS) – i.e., sempre que se saiba, suspeite ou existam razões suficientes para se suspeitar que teve lugar, está em curso ou foi tentada uma operação suscetível de configurar a prática do crime de branqueamento de capitais ou de financiamento do terrorismo.

4.4.5. Ações de controlo ativo reforçado

A MaxPay define um conjunto de procedimentos que pretendem assegurar a monitorização e acompanhamento especialmente atento de entidades consideradas de risco elevado.

Além das situações anteriormente enumeradas, sempre que tome conhecimento através de fontes de informação consideradas com a credibilidade suficiente, no âmbito da prevenção e combate ao branqueamento de capitais e financiamento do terrorismo e de forma a preservar e defender a sua reputação, reservar-se-á o direito de, entre outras acções possíveis:

i) Suspender transações em que existam dúvidas relevantes da sua legitimidade ou conformidade, não procedendo à sua execução sem que estejam reunidas as condições consideradas necessárias;

ii) Proceder a diligências reforçadas e ao exame de operações solicitando documentação comprovativa da justificação económica apresentada, procedendo à sua recusa no caso da informação e documentação consideradas necessárias não ser facultada;

iii) Proceder à devolução de transações à sua origem sempre que entenda não estarem reunidas as condições de conformidade legal ou regulamentar, bem como aquelas, cujo envolvimento possam entender colocar em perigo a sua reputação;

iv) Recusar a execução de transações nas quais entenda estarem a ser violados princípios e valores genericamente aceites pelo sistema financeiros como fazendo parte integrante das boas práticas recomendadas;

v) Recusar o estabelecimento de relações comerciais sempre que entendam ser tal estabelecimento potencialmente provocador de danos reputacionais para o MaxPay;

vi) Comunicar às autoridades competentes qualquer operação ou situação suspeita, sempre que os indícios que contribuíram para a formação dessa convicção não sejam anulados pelas informações ou documentação disponibilizada pelos Clientes.

A MaxPay continuará a adotar progressivamente as medidas e Princípios que entenda serem as adequadas à preservação da sua imagem e do seu ativo reputacional, reafirmando o seu forte empenho na prevenção e combate ao branqueamento de capitais e financiamento do terrorismo.

5.PRINCÍPIO DE GESTÃO DE RISCO DE BRANQUEAMENTO DE CAPITAIS E DE FINANCIAMENTO DE TERRORISMO

5.1. ENQUADRAMENTO

A MaxPay aceita de forma séria e responsável o desafio do combate ao branqueamento de capitais e financiamento ao terrorismo, dedicando esforços em ações e instrumentos de combate a este crime, na convicção que este tipo de atitude estará sempre associada aquilo que se considera ser a defesa da integridade da MaxPay e da sua reputação, bem como a manutenção de elevados padrões de ética profissional.

A MaxPay dá prioridade máxima aos Princípios direcionados para a prevenção do seu envolvimento ou utilização em possíveis ações de branqueamento de capitais e financiamento do terrorismo, que possam prejudicar a sua reputação e estabilidade.

Assim sendo, a MaxPay adota medidas internas, procedimentos e programas de formação e controlo destinados a garantir a conformidade de todos os seus Colaboradores com o enquadramento legal existente sobre a matéria.

5.2. OBJECTIVO E ÂMBITO DO PRINCÍPIO DE GESTÃO DE RISCO DE BRANQUEAMENTO DE CAPITAIS E DE FINANCIAMENTO DE TERRORISMO

Prevenir o uso do sistema financeiro para efeitos do branqueamento de capitais e financiamento do terrorismo é um dos meios mais eficazes de oposição ao crime organizado e uma ferramenta importante na identificação e combate á atividade criminal.

A MaxPay considera ser um dever de todos os seus Colaboradores, na sua atividade diária e no âmbito das suas funções, agir em conformidade com a legislação sobre branqueamento de capitais assim como com as orientações e Princípios internos da MaxPay nesta matéria, no sentido de prevenirem a utilização dos serviços disponibilizados para efeitos de branqueamento de capitais e financiamento do terrorismo.

5.3. MÉTODOS E PROCEDIMENTOS DE PREVENÇÃO DO BRANQUEAMENTO DE CAPITAIS E DO FINANCIAMENTO DO TERRORISMO

5.3.1. Normativos internos

As medidas detalhadas de natureza preventiva estão refletidas nos diversos documentos existentes de procedimentos internos. Todos os Colaboradores deverão agir de acordo com estes documentos, bem como os princípios e procedimentos normalizados neles definidos – Código de Conduta, Manual de Procedimentos.

5.3.2. Due Diligence/Know Your Costumer (KYC)

A MaxPay adota todos os procedimentos necessários no sentido de determinar a verdadeira identidade dos seus Clientes, representantes e/ou beneficiários efetivos (Princípio de Identificação de Clientes), assim como de obter toda a informação relevante e pertinente à abertura e manutenção de uma relação comercial.

No âmbito do processo de identificação e conhecimento do Cliente, a MaxPay avalia necessariamente, sem prejuízo de outros aspetos que possam ser considerados relevantes:

i) A finalidade e o propósito da relação que se pretende estabelecer;
ii) O perfil transacional expectável;
iii) As fontes de rendimento dos Clientes;
iv) A coerência e consistência de toda a informação existente.

Os princípios de Due Diligence são aplicados não só aos procedimentos de identificação de Clientes mas também à deteção, monitorização e acompanhamento de transações que não sejam conformes ao seu perfil.

Todos os registos e evidências documentais são mantidos em vários suportes, pelo prazo legalmente definido.

5.3.3. Risk Based Approach

A MaxPay desenvolve um sistema de classificação de risco de branqueamento de capitais/financiamento do terrorismo (risco BC/FT) aplicável a todos os Clientes, o qual se baseia na ponderação das características do Cliente, conhecidas no decurso do procedimento KYC (antiguidade, atividade profissional, país, tipo de nacionalidade, estatuto PEP, operações/perfil transacional expectável).

A MaxPay atribui a cada Cliente um dos níveis de risco ajustado e diferenciado, a saber:

-Nível de Risco 1 - Muito Reduzido
-Nível de Risco 2 - Reduzido
-Nível de Risco 3 - Médio
-Nível de Risco 4 - Elevado
-Nível de Risco 5 - Muito Elevado

Foi ainda claramente definido um Princípio de Aceitação de Clientes, que estipula os princípios orientadores sobre o tipo de Clientes com que está disposta a iniciar ou manter relações de negócio, designadamente para efeitos de risco de branqueamento (BC).

Embora as orientações acerca da matéria de branqueamento de capitais e financiamento do terrorismo sejam aplicadas a todos os novos Clientes, são as mesmas de igual forma aplicadas aos Clientes existentes com base em critérios ponderados de materialidade e risco.

Sendo o processo de classificação de risco BC/FT dos Clientes dinâmico, os procedimentos adequados deverão ser aplicados a todos os Clientes existentes conforme o risco que lhes for atribuído ou que vejam o seu risco agravado de acordo com os critérios decididos em sintonia com a legislação e regulamentação em vigor, em cada momento, relativa a esta matéria. É necessário garantir que todas as operações de clientes já existentes sejam continuamente monitorizadas e qualquer padrão incomum ou não adequado no funcionamento das mesmas desencadeie um processo de reavaliação da classificação do Cliente com base na atualização do respetivo “due dilligence”.

Os processos de defesa reputacional da MaxPay e de combate ao branqueamento de capitais e ao financiamento do terrorismo, enquadrados numa lógica de diferenciação e graduação do risco BCFT, apenas se tornam verdadeiramente eficazes com a aplicação das Princípios de classificação, análise e monitorização que permitam perceber, em permanência, o nível de risco da entidade.

5.3.4. Metodologia utilizada no processo de monitorização e controlo

Esta abordagem baseada no risco, como método utilizado pela MaxPay com o intuito de identificar, gerir e mitigar o risco de branqueamento de capitais e financiamento do terrorismo, inclui métodos e sistemas de controlo adequados para avaliar e prevenir a concretização daquele risco.

Para isso:

i) Com base nos normativos legais e em fatores que contribuem para a definição do nível de risco, a MaxPay procede à classificação dos Clientes através de notação de Risco BC/FT, considerando a existência dos níveis de risco, processo em permanente atualização e que permite a classificação de todos os clientes, fator preponderante e com impacto direto em todas as atividades de monitorização e controlo baseado no risco;
ii) Com base na utilização do sistema informático da empresa, procede-se, em tempo real, à monitorização de alertas de entidades ("black-lists"/entidades designadas), com o objetivo de verificar a "coincidência" ou não, com as entidades constantes naquelas listas. No caso de se verificar a concordância exata com alguma das entidades constantes nas listas internacionais e mandatórias, a MaxPay não estabelece qualquer relação de negócio; nos restantes casos, em que não se verifique concordância absoluta, procede-se a diligências reforçadas de controlo;

iii) A MaxPay mantém um investimento contínuo na formação de todos os seus funcionários, incluindo ações presenciais, genéricas ou específicas, o fornecimento de informação regular através da divulgação da informação na rede interna.

5.3.5. Monitorização e controlo

O objetivo do controlo implementado é proteger a MaxPay dos diversos riscos e monitorizar de forma permanente a execução das operações, assegurando a sua conformidade com o enquadramento legal, os Princípios e procedimentos internos pré-definidos tendo em conta o perfil do Cliente envolvido, permitindo a deteção de transações com indícios ou suspeitas relevantes para efeitos de branqueamento de capitais e financiamento do terrorismo.

As atividades de monitorização e controlo incluem designadamente as seguintes práticas:

i) Monitorização e controlo de Clientes e transações;
ii) Monitorização e controlo de transações envolvendo países de risco;
iii) Monitorização e controlo de transações fora do comum;
iv) Monitorização da consistência entre as transações e a informação recolhida sobre a atividade do Cliente, perfil de risco e património financeiro numa base permanente. Esta atividade envolve não só transações pontuais mas também a análise temporal do perfil

transacional do Cliente em termos de montantes médios e quantidade de transações executadas;

v) Monitorização e controlo de transações envolvendo entidades sujeitas a sanções e embargos diversos, constantes nas listas de entidades suspeitas (com o objetivo do controlo do cumprimento dessas restrições decretadas internacionalmente);

vi) Controlo da conclusão e atualização da informação e documentos do Cliente que deverão ser mantidos em suporte (papel ou informático), assim como informação adicional que deverá ser incluída em transferências eletrónicas de fundos;

Independentemente dos critérios supre enunciados, deve ser dada especial atenção a todas as condutas e/ou atividades cujos elementos caracterizadores possam agravar o risco ou suscetibilidade de relacionamento com os crimes de branqueamento de capitais ou financiamento do terrorismo, sendo recolhidas informações e evidências documentais, da conformidade e do racional económico das transações submetidas a análise.

A maioria das atividades de monitorização e controlo são executadas pelo Compliance Officer, o qual tem acesso a qualquer tipo de informação do MaxPay.

5.3.6. Comunicação de transações suspeitas

A monitorização e controlo apropriados de Clientes e transações é uma atividade fundamental utilizada pela MaxPay na deteção, identificação e acompanhamento de transações ou atividades atípicas e/ou potencialmente suspeitas.

Havendo a suspeita fundada de que um Cliente ou potencial Cliente está a usar ou pretende usar os produtos ou serviços da MaxPay para branquear fundos provenientes de atividade ilícita ou financiar o terrorismo, a MaxPay toma todas as medidas necessárias para assegurar o integral cumprimento da legislação existente sobre a matéria.

Os Manuais da MaxPay definem os procedimentos a serem adotados pelas várias unidades orgânicas no caso de serem detetadas transações ou atividades que se devam considerar suspeitas. Estas transações ou atividades serão sempre reportadas pelos Colaboradores ou respetivas áreas ao Compliance Officer, a quem compete a sua análise de forma aprofundada.

Neste contexto, as transações consideradas como suspeitas são comunicadas pela MaxPay às autoridades competentes de acordo com os procedimentos legalmente instituídos.

5.3.7. Formação

O objetivo da princípio de formação da MaxPay é não só assegurar a conformidade da MaxPay com o enquadramento legal, mas também desenvolver uma cultura de empresa, aumentando o sentido de responsabilidade de todos os Colaboradores.

Neste contexto, a MaxPay tem implementadas normas rígidas e claras de Formação para todos os Colaboradores, em cumprimento com o estabelecido na legislação

É dada prioridade de formação a todos os Colaboradores que asseguram contacto direto com Clientes, bem como a todos os recém-admitidos.

O objetivo final é a sensibilização de todos os Colaboradores por forma a permitir que quando em presença de uma situação suspeita e com forte probabilidade de configurar crime de branqueamento de capitais ou financiamento do terrorismo, sejam cumpridos todos os deveres que a MaxPay incumbe, solicitando aconselhamento às respetivas hierarquias e ao Compliance Officer sobre os procedimentos a observar, agindo em conformidade com os mesmos e no rigoroso cumprimento das disposições legais a que a MaxPay se encontra obrigado.

5.3.8. Bancos correspondentes

A MaxPay toma as medidas consideradas necessárias de acordo com as boas práticas existentes, quando está em causa o estabelecimento ou a manutenção de relações com Bancos correspondentes, desenvolvendo procedimentos especificamente definidos, no sentido de assegurar a Due Diligence necessária relativamente a estas entidades.

Toda a informação relevante é reunida no sentido de permitir uma decisão fundamentada sobre o estabelecimento de uma relação de correspondência.

6. PRINCÍPIO DE CONFLITOS DE INTERESSES

6.1. ENQUADRAMENTO

A MaxPay tem implementadas medidas a nível organizativo/administrativo eficazes com vista a garantir, com um grau de certeza razoável, a identificação, gestão e controlo dos possíveis conflitos de interesses.

A integridade, a equidade, a imparcialidade e a primazia dos interesses dos Clientes ocupam um lugar principal entre as normas éticas da empresa. A todos os Colaboradores é requerida uma atuação conforme com as normas éticas e recebem a informação, o treino e a orientação apropriada a fim de atuarem de modo eficaz.

6.2. PRINCÍPIO DE CONFLITOS DE INTERESSES

Como qualquer grupo de serviços financeiros, a MaxPay está exposta a potenciais conflitos de interesses que possam surgir nas suas diferentes áreas de atuação. Os princípios de atuação da MaxPay assentam na necessidade de adotar todas as medidas razoáveis para identificar potenciais conflitos de interesses entre a MaxPay e os seus Clientes e entre um e outro Cliente, assim como dispor das regras que permitam assegurar que tais conflitos não afetem adversamente os interesses dos Clientes.