



**Política de Prevenção de Branqueamento de Capitais e
do Financiamento do Terrorismo**

Aviso nº1/2022 do Banco de Portugal

- **Ficha Técnica**

Título do documento: Política de Prevenção e Branqueamento de Capitais e do Financiamento de Terrorismo

Estado: Não Revogado

Tipo de Documento: Política

Área Funcional Responsável: Departamento de Legal & Compliance

- **Aviso**

A Eupago – Instituição de Pagamento, Lda. rege-se por uma política de monitorização e melhoria contínua das suas políticas e procedimentos. Desta forma, a informação contida na presente Política está sujeita a atualização, sendo reservado ao Departamento de Legal & Compliance o direito de proceder à referida atualização.

- **Histórico de Versões/Revisões**

Versão	Data	Descrição	Autor
1.0	Dezembro de 2023	Versão original da Política	Departamento de Legal & Compliance

• Índice

Introdução	4
Âmbito	4
Descrição	5
Compliance	5
Capítulo I - Deveres preventivos do BC/FT	6
A. Dever de Identificação	6
B. Dever de Diligência	6
C. Dever de Controlo	7
D. Dever de Recusa	7
E. Dever de Conservação	7
F. Dever de Exame	8
G. Dever de Diligência Reforçada	8
H. Dever de Comunicação	9
I. Dever de Abstenção	9
J. Dever de Colaboração	10
K. Dever de Segredo	10
L. Dever de Formação	10
Capítulo II - Medidas de Know Your Customer (KYC)	10
A. Conhecimento e Monitorização do Cliente	11
B. Monitorização de dados do Cliente	12
Capítulo III - Mecanismos de Controlo Interno	13
Capítulo IV - Sistemas de Informação	13
Capítulo V - Incumprimento da Política	13
Capítulo VI - Responsabilidade contraordenacional	14
Capítulo VII - Normativos internos relacionados	14
Glossário	15
Lista de Siglas e Abreviaturas	17

● **Introdução**

A prevenção do branqueamento de capitais e financiamento de terrorismo é um objetivo chave para a Eupago – Instituição de Pagamento, Lda., como parte dos padrões de ética e segurança e valores para o desenvolvimento da sua atividade. É, assim, considerada elemento fundamental para a preservação da sustentabilidade, solidez, reputação e confiança na instituição.

Desta forma, a presente Política define os princípios base e o modelo operacional para a prevenção do branqueamento de capitais e do financiamento de terrorismo que regem a atividade da instituição.

Para o efeito, esta Política define os padrões de implementação das recomendações emitidas pelo Grupo de Ação Financeira Internacional (doravante GAFI); em cumprimento com o preceituado da Lei n.º 83/2017, de 18 de Agosto, que estabelece as medidas de combate ao branqueamento de capitais e ao financiamento do terrorismo (doravante BCFT), bem como das regras e regulamentos do Banco de Portugal, nomeadamente o Aviso n.º 1/2022 (que revoga o Aviso n.º 2/2018).

Por fim, importa realçar que as disposições definidas nesta Política não se sobrepõem ou tão pouco substituem as disposições legais e regulamentares emitidas pelas autoridades competentes.

● **Âmbito**

A presente Política é aplicável a todos os colaboradores da Instituição, sendo que os respetivos atos e procedimentos, atuais ou futuros, devem ser adotados, adaptados e elaborados em conformidade com esta Política e com a legislação relacionada, sendo-lhes exigido um escrupuloso cumprimento dos procedimentos internamente instituídos e a todo e qualquer processo integrante da atividade da Instituição cuja execução se encontre, direta ou indiretamente, sujeita aos requisitos legais e regulamentares vigentes sobre a prevenção do BCFT. A presente Política abrange e vincula:

- i. A Instituição;
- ii. Os titulares dos órgãos sociais;
- iii. Colaboradores da direção de topo, onde se incluem os titulares de funções essenciais;
- iv. Todos os restantes colaboradores da Instituição, permanentes ou eventuais, mandatários e outras pessoas singulares ou coletivas que lhes prestem serviço a título permanente ou ocasional, direta ou indiretamente, independentemente da natureza do vínculo subjacente; e,
- v. Terceiros que, por solicitação expressa da Instituição ou por força da relação estabelecida, tenham aderido expressamente à presente Política ou sejam legalmente obrigados ao cumprimento da mesma.

- **Descrição**

A presente Política define os papéis e responsabilidades no que toca à prevenção destes crimes, identifica a missão da instituição e o papel dos departamentos nestes domínios e estabelece o modelo operacional e as funções de controlo (processos-chave adotados, atividades de filtering e monitorização) bem como apresenta mecanismos informáticos implementados para prevenção, mitigação e combate destes mesmos crimes.

- **Compliance**

O não cumprimento das normas estabelecidas nesta Política, dará origem a procedimentos disciplinares que poderão no seu limite levar à rescisão do contrato por justa causa. A monitorização do cumprimento das normas definidas nesta Política é da responsabilidade do Departamento de Legal & Compliance.

POLÍTICA DE PREVENÇÃO DE BRANQUEAMENTO DE CAPITAIS E DO FINANCIAMENTO DO TERRORISMO

● Capítulo I - Deveres preventivos do BC/FT

A Lei n.º 83/2017, de 18 de agosto, estabelece medidas de natureza preventiva e repressiva de combate ao BCFT. Deste modo, as entidades financeiras e os seus Colaboradores estão obrigados, no exercício da respetiva atividade, ao cumprimento dos seguintes deveres preventivos:

A. Dever de Identificação

Impõe-se um dever de verificar a identidade dos seus clientes (existentes e potenciais), e confirmar os seus dados e dos respetivos representantes, quando aplicável.

Obriga-se ao cumprimento de procedimentos neste âmbito sempre que se verifique qualquer destas situações:

- a) Se estabeleça uma relação de negócio;
- b) Se suspeite que as operações possam estar relacionadas com um caso de branqueamento de capitais ou financiamento de terrorismo; ou
- c) Existam dúvidas sobre a veracidade ou adequação dos dados de identificação dos clientes previamente obtidos.

Sobre esta matéria, consultar a *Política de Identificação e Aceitação de Clientes* que contém todo o processo desenvolvido pela instituição de forma a cumprir este dever de identificação.

B. Dever de Diligência

Atenta a atividade desenvolvida pela Eupago e os riscos inerentes, importa analisar todas as informações relativas à natureza e finalidade da relação de negócio a estabelecer ou já estabelecida com o Comerciante, bem como sobre a origem e o destino dos fundos.

Esta análise deverá ser realizada nos momentos já identificados no ponto anterior, isto é:

- a) Sempre que se estabeleça uma relação de negócio;
- b) Caso se suspeite que as operações possam estar relacionadas com um caso de branqueamento de capitais ou financiamento de terrorismo; ou
- c) Sempre que existam dúvidas sobre a veracidade ou adequação dos dados de identificação dos clientes previamente obtidos.

Sobre esta matéria, consultar a *Política de Identificação e Aceitação de Clientes* que contém todo o processo desenvolvido pela instituição por forma a cumprir este dever de diligência.

C. Dever de Controlo

Em respeito por este dever, a Eupago dispõe de um conjunto de políticas, procedimentos e controlos adequados à gestão eficaz dos riscos de Branqueamento de Capitais e Financiamento do Terrorismo e ao efetivo cumprimento das normas legais e regulamentares sobre esta matéria.

D. Dever de Recusa

Quanto a este dever, implica uma recusa em iniciar uma relação de negócio, isto é, em prestar serviços de pagamentos, quando se verifique qualquer uma destas circunstâncias:

a) Não se obtenham os elementos identificados e respetivos meios comprovativos necessários do Comerciante, Representante Legal ou Beneficiário Efetivo, incluindo a informação necessária para aferição da qualidade destes e a estrutura de propriedade do Comerciante;

b) Informação sobre a natureza, objeto e finalidade da relação de negócio;

c) Não seja possível dar cumprimento aos procedimentos de identificação e diligência, incluindo os procedimentos de atualização de dados.

Na eventualidade de uma conta ser recusada, a Instituição preenche um “Relatório de Conta Recusada”, que deve ser anexado à ficha de conta de cada cliente ou potencial cliente. Neste relatório são especificados os motivos da recusa e, se se verificou ou não, motivo para participação ao Procurador-Geral da República e à Unidade de Informação Financeira (UIF).

Sobre esta matéria, consultar a *Política de Identificação e Aceitação de Clientes* que contém todo o processo desenvolvido pela instituição por forma a cumprir este dever de recusa.

E. Dever de Conservação

No cumprimento deste dever, todo o arquivado será conservado por um período de 7 anos, a contar do momento da identificação e do termo das relações, em formato digital nos nossos servidores, e em formato papel nos arquivos da empresa. Estes arquivos estão localizados na sede da instituição.

Deste modo, os originais, cópias, referências ou quaisquer suportes duradouros dos documentos comprovativos e dos registos das operações são conservados por pelo menos 7 anos a contar da execução das operações.

F. Dever de Exame

Neste capítulo, impõe-se uma obrigação de examinar com especial cuidado e atenção, intensificando e adequando o grau e a natureza do seu acompanhamento, quando se detetem condutas, atividades ou operações, cujos elementos caracterizadores as tornem suscetíveis de poderem estar relacionadas com fundos, ou outros bens que provenham de atividade criminosa ou estar relacionados com financiamento ao terrorismo.

Para o efeito, relevam os seguintes elementos caracterizadores a serem tidos em consideração:

- a) A natureza, finalidade, frequência, complexidade, invulgaridade e a atipicidade da conduta, da atividade ou das operações;
- b) Aparente inexistência de um objetivo económico ou de um fim lícito associado à conduta, à atividade ou às operações;
- c) Os montantes, a origem e o destino das operações;
- d) O local de origem e o destino das operações;
- e) Os meios de pagamento utilizados;
- f) A natureza, a atividade, o padrão operativo, a situação económico-financeira e o perfil do Comerciante;
- g) O tipo de transação, produto, estrutura societária ou centro de interesses coletivos sem personalidade jurídica que possa favorecer especialmente o anonimato;
- h) Entre outras.

Esta monitorização das operações é efetuada pelos Colaboradores, suportados por mecanismos de controlo interno, através da estrutura informática.

Remete-se para o *Manual de Mecanismos de Prevenção de BCFT*, onde se descrevem os processos internos adotados.

G. Dever de Diligência Reforçada

Atenta a natureza da atividade desenvolvida pela Eupago, impõe-se um dever especial de diligência reforçada. Assim, a par de toda a documentação entregue pelo Comerciante, são solicitados documentos ou informações suplementares para verificar ou certificar os dados fornecidos por este.

A Eupago e os seus Colaboradores devem, ainda, dedicar particular atenção a PEP e titulares de outros cargos políticos ou públicos, sendo que nestes casos poderá ser necessário:

- a) Obter autorização da hierarquia imediata antes de estabelecer relações de negócio com tais Comerciantes;
- b) Efetuar um acompanhamento contínuo acrescido da relação de negócio, através de uma análise dos movimentos de conta.

H. Dever de Comunicação

No âmbito deste dever, a Eupago informa, de imediato, o Procurador-Geral da República e a Unidade de Informação Financeira, sempre que exista uma suspeita fundamentada ou conhecimento de operações que indiciem a prática do crime de branqueamento ou do financiamento do terrorismo.

Cumpra ao Departamento de Legal & Compliance efetuar estas comunicações, após análise da operação ou dos documentos identificativos do Comerciante, mediante a submissão do relatório próprio com a anexação de todas as informações disponíveis. Caso se aplique, deverá também anexar o “Relatório de Conta Recusada”.

Caso algum cliente ou um potencial cliente conste da lista consolidada dos indivíduos, grupos e entidades sujeitos a medidas restritivas/ sanções impostas quer a nível nacional, quer a nível internacional, a Eupago está obrigada a comunicá-lo às autoridades nacionais competentes: à Direção-Geral de Política Externa do Ministério dos Negócios Estrangeiros e ao Gabinete de Planeamento, Estratégia, Avaliação e Relações Internacionais do Ministério das Finanças (Lei n.º 97/2017, de 23 de agosto).

As autoridades nacionais competentes estão, ainda, incumbidas de informar e prestar esclarecimentos a qualquer pessoa ou entidade em matéria de medidas restritivas. Com efeito, e em caso de dúvidas acerca da aplicação de medidas restritivas, a Eupago deverá entrar em contacto com as autoridades competentes.

Quando exista notícia ou suspeita de que houve ou está em curso um ato ou omissão idónea a configurar a violação de uma medida restritiva existe o dever de denúncia junto do Procurador-Geral da República e das autoridades nacionais competentes.

Contactos das Autoridades:

- Unidade de Informação Financeira – uif.comunicacoes@pj.pt
- Procuradoria-Geral da República – correio.dciap@pgr.pt
- Direção-Geral de Política Externa do MNE - pesc@mne.pt
- Gabinete de Planeamento, Estratégia, Avaliação e Relações Internacionais do MF - dmspl@gpeari.gov.pt

I. Dever de Abstenção

A Eupago deve abster-se de executar operações sempre que saibam ou suspeitem estarem relacionadas com a prática do crime de branqueamento ou de financiamento do terrorismo.

Assim, sempre que se constate que uma determinada operação evidência fundada suspeita de constituir crime, a instituição abstém-se de a executar até que a UIF ou a PGR expressamente autorize a execução da mesma..

Para comunicar à UIF ou à PGR a operação suspeita, e solicitar a autorização prévia, devem ser utilizados os contactos enumerados no ponto anterior.

J. Dever de Colaboração

A Eupago colabora com as autoridades competentes e presta assistência, sempre que tal seja requerido.

A Eupago responde a todos os pedidos de informação das autoridades competentes (DCIAP-PGR / UIF-PJ), Autoridades Judiciais e Policiais, Autoridade Tributária e Aduaneira, e Autoridades Setoriais e, de forma célere, fornece os dados solicitados, colaborando, deste modo, para a descoberta da verdade e transparência do sistema.

K. Dever de Segredo

Define que não podem ser reveladas informações a clientes ou a terceiros, nomeadamente as relativas a comunicações efetuadas, em curso ou que irão ser efetuadas às autoridades competentes, ou sobre pedidos de informação destas, ou que se encontra em curso investigações, inquéritos, averiguações, análises ou procedimentos legais pelas autoridades referidas.

Impõe necessária prudência junto dos clientes e de outras entidades relacionados com a execução de operações especialmente suspeitas, evitando quaisquer diligências que por qualquer razão, possam suscitar a suspeição de que estão em curso quaisquer procedimentos que visem averiguar suspeitas de práticas relacionadas com o BCFT.

A fim de fazer cumprir, e de demonstrar a importância do dever de segredo, o não cumprimento do mesmo, implicará a instauração de um Procedimento disciplinar que pode terminar com despedimento por facto imputável ao trabalhador.

L. Dever de Formação

A Eupago organiza e incentiva a frequência de todos os Colaboradores em ações específicas e regulares de formação que os habilitem a reconhecer operações que possam estar relacionadas com BCFT e a atuar de acordo com a Lei e normas regulamentares que a concretizem.

A par disso, é disponibilizado a todos os Colaboradores da Eupago a presente Política para integral conhecimento dos procedimentos internos implementados e dos riscos adjacentes à atividade desenvolvida

● Capítulo II - Medidas de Know Your Customer (KYC)

O conhecimento do cliente (*know your customer* – doravante, KYC) é um dos pilares fundamentais na aferição da apetência do cliente para a realização de operações de branqueamento de capitais e na consequente definição do seu perfil de risco.

A adoção de medidas eficazes de KYC constitui uma parte essencial da gestão do risco de branqueamento de capitais e financiamento do terrorismo pelo que, neste âmbito, a Eupago:

- Classifica todos os clientes constantes na sua base de dados em função do seu perfil de risco de branqueamento de capitais;
- Ajusta os níveis de vigilância (simplificada ou reforçada) em função do perfil de risco de branqueamento de capitais do cliente;
- Define processos específicos com vista à monitorização de clientes e contas que possam constituir um risco mais alto na ótica do branqueamento de capitais e do financiamento do terrorismo;
- Procede à confirmação periódica dos dados dos clientes.

De acordo com a legislação aplicável, a Eupago efetua as diligências idóneas e suficientes com o objetivo de assegurar a atualidade, exatidão e completude da informação relativa aos clientes, representantes e beneficiários efetivos.

Ao implementar medidas de KYC adequadas, a Eupago procede à detalhada identificação de cada cliente, ao conhecimento da natureza das atividades económicas por si desenvolvidas e, ainda, às diligências necessárias para o conhecimento efetivo das estruturas de propriedade e controlo das pessoas coletivas.

A implementação de políticas e medidas KYC assume, assim, a função essencial de identificar, avaliar e monitorizar o risco do cliente em matéria de BCFT, permitindo uma avaliação mais eficiente dos riscos e tornando-se numa importante ferramenta para manter a confiança, estabilidade e reputação da Eupago.

A. Conhecimento e Monitorização do Cliente

A Eupago tem políticas e procedimentos internos que asseguram o cumprimento do dever de identificação dos seus clientes e efetua, com recurso a ferramentas informáticas, a monitorização das transações realizadas pelos seus clientes que são filtrados com regularidade por confronto com listagens relevantes para identificação de sancionados e PPE/Titulares de outros cargos políticos ou públicos.

São várias as fontes de informação utilizadas para criar uma lista interna de PPE/Titulares de outros cargos políticos ou públicos.

A par disso, a Eupago recorre ao serviços de plataformas externas que prestam um serviço de validação e verificação de dados, para auxiliar na filtragem e monitorização dos Clientes e manter atualizados os registos de PEP's e de outras pessoas ou organizações que constam das listas de restrições da ONU, Conselho Europeu, etc.

Para além destas listas, a atualização da lista interna de PPE/Titulares de outros cargos políticos ou públicos, é efetuada através de “media clipping” e das respostas dadas ao questionário efetuado pela Eupago aos potenciais clientes, sempre que se pretende estabelecer uma relação de negócio.

NOTA: PEP's e titulares de outros cargos públicos ou políticos são monitorizados de maneira reforçada, atenta a qualidade que assumem. Esta monitorização é efetuada através do Sistema de Perfis de Risco, com base na avaliação de risco realizada.

Consideram-se titulares de outros cargos políticos ou públicos, as pessoas singulares que, não se subsumem na qualidade de “pessoa politicamente exposta”, mas que desempenham ou tenham desempenhado, nos últimos 12 meses - em território nacional, os seguintes cargos:

- enunciados no art.º 2.º, n.º 3 da Lei n.º 52/2019, de 31 de julho;
- membro do órgão representativo ou executivo da área metropolitana ou de outras formas de associativismo municipal.

B. Monitorização de dados do Cliente

Por forma a garantir que os dados dos clientes se encontram atualizados, sempre que é inserido um documento/dado associado a uma conta, é também adicionada a data de expiração do mesmo. Esta data de expiração pode ser:

- Expiração documento de identificação;
- Expiração Certidão Permanente;
- Data de fim de mandato de órgãos de administração ou equivalente.

Para todos os dados que não contenham uma data de expiração, como por exemplo o comprovativo de morada, a data a inserir no sistema é o de:

- 1 Ano após o início da relação de negócio para clientes de risco Elevado;
- 3 Anos após o início da relação de negócio para clientes de risco Médio;
- 5 Anos após o início da relação de negócio para clientes de risco Baixo.

Todos os dias o sistema informático identifica os documentos a expirar no mês seguinte, por forma a permitir a adoção dos procedimentos necessários à atualização da informação. Não obstante, são efetuadas diligências de atualização dos dados constantes dos seus registos sempre que:

- Existam razões para duvidar da sua veracidade, exatidão ou atualidade;
- Existam suspeitas da prática dos crimes de branqueamento ou de financiamento do terrorismo, sem prejuízo do cumprimento do respectivo dever de comunicação;
- Exista conhecimento da ocorrência de, pelo menos, um dos seguintes factos relacionados com o cliente, o seu representante ou o beneficiário efetivo, consoante os casos:

- i) Alteração do órgão de administração ou órgão equivalente;
- ii) Alteração da natureza da atividade ou do modelo de negócio;
- iii) Alteração da lista de assinaturas autorizadas para a movimentação de contas;
- iv) Modificação na estrutura de participações, domínio ou controlo, quando suscetível de induzir a uma alteração do beneficiário efetivo.

● **Capítulo III - Mecanismos de Controlo Interno**

O Departamento de Compliance, em colaboração com a Gerência, é responsável pela definição de políticas e normas internas respeitantes à prevenção do branqueamento de capitais e financiamento do terrorismo.

Deste modo, com vista ao cumprimento do dever de controlo no âmbito do BCFT, foram implementadas um conjunto de medidas de prevenção, mitigação e combate ao BCFT, através da aplicação dos normativos legais e regulamentares em vigor, do reforço de segurança do sistema informático da instituição e da formação contínua de todos os Colaboradores.

Sobre esta matéria, consultar o Manual de Mecanismos de Prevenção de BCFT, que descreve todas as medidas implementadas e o processo de filtering e monitorização adotado pela Instituição.

● **Capítulo IV - Sistemas de Informação**

Para além de permitir a operacionalidade do sistema de pagamentos, o sistema de informação da Eupago permite armazenar e aceder, a qualquer momento, informações relativas à atividade, pois funciona como registo centralizado de Clientes e operações.

O sistema de informação da Eupago:

- Contém o registo centralizado de todas as operações e de clientes;
- Permite o acesso a todos movimentos dos clientes em tempo real, ao histórico de todas as operações realizadas pelos administradores e pelos clientes;
- Permite a análise individual de cada transação de modo que um responsável seja alertado para transações específicas;
- Calcula o volume médio transacionado por cliente;
- Permite o acesso a todas as transações efetuadas ou por efetuar, relativas a um cliente ou a todos;
- Saber com exatidão total e em tempo real os pagamentos efetuados;
- Saber os montantes individuais dos movimentos que constituem o valor global de um pagamento;
- Exportar os movimentos de um ou vários clientes para formato XML, CSV, Excel, etc.

● **Capítulo V - Incumprimento da Política**

O incumprimento da presente Política por parte dos colaboradores da Instituição viola o disposto na Lei, e no Código de Conduta, sujeitando o infrator às regras disciplinares aplicáveis na Instituição e às consequências das responsabilidades civis,

contraordenacionais e criminais. O exercício do poder disciplinar sobre os Colaboradores, quando esteja em causa o incumprimento da presente Política compete ao Conselho de Administração.

- **Capítulo VI - Responsabilidade contraordenacional**

Sem prejuízo da responsabilidade penal pelo crime de branqueamento a que podem estar sujeitas tanto as pessoas singulares como as pessoas coletivas (cfr. artigo 368.º-A e artigo 11.º do Código Penal), ou de outras disposições sancionatórias conexas aplicáveis a cada caso concreto, estão tipificadas contraordenações pelo incumprimento dos deveres e obrigações impostos pela Lei n.º 83/2017, de 18 de agosto, puníveis com coimas e sanções acessórias.

A responsabilidade da pessoa coletiva não exclui a responsabilidade individual das pessoas singulares que sejam titulares de funções de administração, gerência, direção, chefia, fiscalização, representantes, trabalhadores ou demais colaboradores, permanentes ou ocasionais.

- **Capítulo VII - Normativos internos relacionados**

A presente Política deverá ser traduzida em procedimentos que no seu conjunto contribuam para robustecer a efetividade do sistema de prevenção do BCFT de que a Instituição dispõe, pelo que a informação relativa à prevenção do BCFT não se esgota neste documento. Deste modo, a Instituição dispõe de um conjunto de normativos internos, com caráter reservado, que complementam os princípios e objetivos desta Política.

● Glossário

Para efeitos da presente Política, entende-se por:

- **Beneficiário:** A pessoa singular ou coletiva que seja o destinatário previsto dos fundos que foram objeto de uma Operação de Pagamento;
- **Beneficiário Efetivo:** qualquer pessoa singular por conta de quem é realizada uma transação ou atividade ou que, em última instância, detém ou controla o cliente, nos termos previstos na alínea h) do n.º 1 do artigo 2.º da Lei n.º 83/2017, de 18 de agosto;
- **Branqueamento de capitais:** qualquer evento destinado a dissimular a natureza e a origem dos fundos provenientes de atividades ilícitas;
- **Comerciante/Cliente:** qualquer pessoa singular, pessoa coletiva, de natureza societária ou não societária, ou centro de interesses coletivos sem personalidade jurídica que entre em contacto com a instituição de pagamento com o propósito de, por esta, lhe ser prestado um serviço ou disponibilizado um produto, através do estabelecimento de uma relação de negócio;
- **Colaborador:** qualquer pessoa singular que, em nome da instituição de pagamento e sob a sua autoridade ou na sua dependência, participe na execução de quaisquer operações, atos ou procedimentos próprios da atividade prosseguida por aquela, independentemente de ter com a mesma a mesma um vínculo de natureza laboral (colaborador interno) ou não (colaborador externo);
- **Dados Pessoais:** tem o sentido constante da definição inserida no artigo 4.º, 1), do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, ou seja, a informação relativa a uma pessoa singular identificada ou identificável. É considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;
- **Financiamento do terrorismo:** recolha de fundos destinados ao terrorismo, independentemente de esses fundos terem origem em atividades lícitas;
- **Grupo de Ação Financeira Internacional (GAFI) ou Financial Action Task Force (FAFT):** agrupamento governamental internacional de carácter informal, em que a sua ação consiste na formulação de recomendações com vista à prevenção e repressão de branqueamento de capitais, do financiamento do terrorismo, do confisco dos lucros do crime e da cooperação internacional nestas matérias;

- **IBAN:** International Bank Account Number. Elemento de informação que permite identificar, no Espaço Económico Europeu e na Área Única de Pagamentos em Euros (SEPA), a Conta de Pagamento de um Beneficiário de uma operação de pagamento. O IBAN é composto, no máximo, por 34 caracteres. Em Portugal, a construção do IBAN é efetuada fazendo preceder o NIB do prefixo “PT50”;
- **Instituições de pagamento:** As pessoas coletivas a quem tenha sido concedida autorização, nos termos do artigo 10.º do RJPSP, para prestar e executar serviços de pagamento em toda a União Europeia.
- **Operação de Pagamento:** O ato praticado pelo Ordenante ou Beneficiário de depositar, transferir ou levantar fundos, independentemente de quaisquer obrigações subjacentes entre o Ordenante e o Beneficiário.
- **Pessoa Politicamente Exposta (PPE) ou Politically Exposed Person (PEP):** as pessoas singulares que desempenham, ou desempenharam nos últimos doze meses, em qualquer país ou jurisdição, funções públicas proeminentes de nível superior e que, por desenvolverem essa atividade, existe um maior risco de branqueamento de capitais e financiamento ao terrorismo, e, bem assim, os seus representantes, familiares e colaboradores (cfr. alínea cc), do n.º 1 do artigo 2.º da Lei 83/2017, de 18 de agosto;
- **Relações de Negócio:** qualquer relação de natureza comercial entre a instituição de pagamento e os seus clientes que, no momento do seu estabelecimento, se prevê que seja ou venha a ser duradoura, caracterizando-se, designadamente, pela prestação de serviços pela instituição de pagamento aos seus clientes, de forma tendencialmente estável e continuada no tempo e independentemente do número de operações individuais que integrem ou venham a integrar o quadro relacional estabelecido, com respeito pelos princípios previamente designados, entre eles: princípio da confidencialidade, proteção de dados e transparência;
- **Unidade de Informação Financeira:** unidade central nacional com competência para receber, analisar e difundir a informação suspeita de branqueamento ou de financiamento do terrorismo, instituída pelo Decreto-Lei n.º 304/2002, de 13 de dezembro.

● Lista de Siglas e Abreviaturas

Por facilidade de exposição e sem prejuízo da utilização pontual das designações e expressões que visam substituir, ao longo da presente Política, são utilizadas as seguintes siglas e abreviaturas:

- **BdP:** Banco de Portugal;
- **BCFT:** Branqueamento de capitais e financiamento de terrorismo;
- **ENI:** Empresário em nome individual
- **GAFI:** Grupo de Ação Financeira Internacional
- **PPE ou PEP:** Pessoa Politicamente Exposta ou Politically Exposed Person;
- **UIF:** Unidade de Informação Financeira.