POLÍTICA DE PREVENÇÃO E COMBATE À LAVAGEM DE DINHEIRO E FINANCIAMENTO AO TERRORISMO

Elaboração:	Data / Assinatura:
Campos Thomaz e Meirelles Advogados **Sócio**	**27/05/2022**
Revisão:	**Data / Assinatura:**
Alexandre Castilho **Diretor De Compliance** **2GOFINTECH**	**19/07/2022**
Revisão:	**Data / Assinatura:**
Barcellos, Tucunduva - Advogados **Sócio**	**13/10/2022**
Revisão:	**Data / Assinatura:**
Fernando Paixão de Sousa **Diretor Jurídico** **2GOFINTECH**	**01/11/2022**
Revisão:	**Data / Assinatura:**
Alexandre Castilho **Diretor De Compliance** **2GOFINTECH**	**17/11/2022**
Aprovação:	**Data / Assinatura:**
Cyllas Salerno Elia Junior **CEO** **2GOFINTECH**	**21/11/2022**

Av Ibirapuera, 2332, 13º andar - Indianópolis/São Paulo-SP - 04028-900 www.2gobank.com.br CNPJ: 23.819.290/0001-03

HISTÓRICO DO DOCUMENTO:

Data	Versão	Autor	Motivo da Revisão
27/05/2022	1.0	Campos Thomaz e Meirelles Advogados	Versão inicial do documento
19/07/2022	2.0	Alexandre Castilho	Revisão e Atualização da Política
13/10/2022	2.0	Barcelos Tucunduva Advogados	Revisão e Atualização da Política
01/11/2022	2.0	Fernando Paixão	Revisão e Atualização da Política
17/11/2022	2.0	Alexandre Castilho	Revisão Final

SUMÁRIO

1. DEFINIÇÕES

Administradores ou alta Administração: Diretores, Sócios e Conselheiros da **2GOFintech**.

Área de Compliance: Área específica da **2GOFintech**, responsável por garantir o cumprimento da legislação aplicável e procedimentos internos, estabelecendo um programa de conformidade compatível com a natureza, estrutura, perfil de risco e modelo de negócio da **2GOFintech**, bem como criar e gerenciar os riscos relacionados ao combate à corrupção, a lavagem de dinheiro e o Financiamento do Terrorismo, para garantia do padrão ético da **2GOFintech**.

Arranjo de Pagamento: conjunto de regras e procedimentos que disciplina a prestação de determinado serviço de pagamento ao público, pela Lei nº 12.865/2013.

Bacen: Banco Central do Brasil.

Canal de Denúncia: Ferramenta de comunicação para relatos e abertura de ocorrências quando identificada qualquer não conformidade, indícios de corrupção, lavagem de dinheiro e financiamento do terrorismo, ou desvio de conduta ou padrão ético da **2GOFintech**.

Clientes: Usuários finais dos serviços e produtos da **2GOFintech**.

Colaboradores: funcionários da **2GOFintech**, bem como seus prestadores de serviços, profissionais sem vínculo empregatício que sejam contratados de forma esporádica pela **2GOFintech**, seus Administradores e estagiários.

Compliance: Conjunto de regras e procedimentos que visam a conformidade da **2GOFintech** com as leis e normas que lhe são aplicáveis, bem como suas regras e padrões éticos internos para o cumprimento da lei e observância aos princípios da ética, transparência e integridade corporativa.

COAF: Conselho de Controle de Atividades Financeiras, que atua na prevenção e combate à Lavagem de Dinheiro e outras atividades ilícitas.

Financiamento do Terrorismo: Apoio financeiro, por qualquer meio, ao terrorismo ou àqueles que incentivam, planejam ou cometem atos de terrorismo.

Fornecedores: Toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades ou prestam serviços para **2GOFintech**.

Instituição de Pagamento: para fins desta Política, é a **2GOFintech** como emissora de moeda eletrônica, cuja atividade consiste em gerenciar a Conta de Pagamento de Usuários, utilizada para o pagamento de transações pré-pagas.

Know Your Customer/Know Your Client (KYC): Essa expressão sintetiza um conjunto de práticas e informações úteis para que a empresa possa conhecer seu cliente com a finalidade de, mediante diligência prévia, conferir sua reputação, idoneidade e veracidade dos dados cadastrais informados, buscando evitar a prática de lavagem de dinheiro e financiamento do terrorismo.

Know Your Partner ("KYP"): é o processo pelo qual a **2GOFintech** obtém informações dos seus Parceiros de Negócio e Fornecedores, com a finalidade de, mediante diligência prévia, conferir sua reputação, idoneidade e veracidade dos dados cadastrais informados, buscando evitar a prática de Lavagem de Dinheiro e Financiamento do Terrorismo

Know Your Employee ("KYE"): é o processo que visa obter informações dos Colaboradores, com a finalidade de conferir a sua reputação, idoneidade e veracidade dos dados cadastrais informados, buscando evitar a prática de Lavagem de Dinheiro e Financiamento do Terrorismo.

Lavagem de Dinheiro: conjunto de operações comerciais ou financeiras que busca incorporar à economia formal recursos que se originam de atos ilícitos, dando-lhes a aparência legítima

OFAC: Office of Foreign Assets Controls, que consiste no órgão do Departamento do Tesouro dos Estados Unidos da América, que administra e aplica sanções econômicas e comerciais contra países e regimes estrangeiros considerados terroristas, traficantes internacionais de drogas, envolvidos em atividades relacionadas à proliferação de armas de destruição em massa e outras ameaças à segurança nacional, à política externa ou à economia daquele país.

Parceiros de Negócios: Organizações que estabelecem alianças estratégicas e que partilham objetivos comuns com a **2GOFintech**, criando valor e rentabilidade entre si.

Pessoas Politicamente Expostas ("PEP"): São Agentes Públicos que desempenham, ou que tenham desempenhado, nos últimos cinco anos, no Brasil ou em outros países, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo, tudo conforme o definido nos artigos 19 e 27 da Circular no 3.978/2020.

Pix: arranjo de pagamentos, instituído pelo Bacen, que disciplina a prestação de serviços de pagamento relacionados com as Transações de pagamentos instantâneos, no âmbito do arranjo.

Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo: Este documento, aqui definido como "Política".

Transações: para fins desta Política, consistem nas movimentações realizadas pelo Cliente de sua conta de pagamento, mediante o aporte, a transferência ou o resgate de recursos financeiros, por qualquer modalidade.

2. INTRODUÇÃO

As diretrizes e procedimentos desta Política foram criados conforme **a Circular do Banco Central do Brasil nº 3.978/2020**, e a presente Política foi elaborada de forma compatível com o porte, a natureza, a complexidade, a estrutura e o modelo de negócio da **2GOFintech**.

As regras aqui definidas devem ser atualizadas pelo diretor de PLDFT e Compliance da **2GOFintech**, nomeado junto ao Bacen, através da análise de eventuais atualizações, revogações ou publicações de novas normas aplicáveis. Os monitoramentos são realizados para acompanhamento de procedimentos e dos controles internos da IP. Assim sendo, não há uma regra de mercado, porém, o controle deve ser periódico.

A Política deve ser divulgada aos Colaboradores da **2GOFintech,** parceiros de negócio e prestadores de serviços terceirizados, mediante linguagem clara e acessível, em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

3. OBJETIVO

Esta Política e Manual de Procedimentos dispõe sobre os conceitos, princípios e diretrizes do Programa de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo da **2GOFintech** e tem como objetivo prevenir e combater a Lavagem de Dinheiro e o Financiamento ao Terrorismo, além de outros crimes envolvendo simulação ou ocultação de recursos financeiros, conforme **Lei nº 9.613/1998**.

Dentre os serviços oferecidos pela **2GOFintech**, como Instituição de Pagamento Emissora de Moeda Eletrônica (IP EME), esta realiza a gestão e custódia de recursos financeiros dos Clientes, que poderão ser indicados por Parceiros Comerciais, possibilitando o recebimento e a realização de pagamentos por meio das Transações.

Assim, os Clientes e Parceiros Comerciais poderão tentar utilizar os serviços prestados pela **2GOFintech** para a prática de crimes relacionados com Lavagem de Dinheiro e Financiamento do Terrorismo, mediante a ocultação ou dissimulação da natureza, origem, localização e movimentação de recursos provenientes de infração penal, com a finalidade de incorporá-los ao sistema financeiro.

A **2GOFintech** irá adotar, por meio de seu Diretor de PLDFT e de sua Área de Compliance, normas internas, padrões, procedimentos, treinamentos, comunicação corporativa e medidas preventivas, corretivas e punitivas, a fim tornar a **2GOFintech**, em todas as áreas, aderente a esta Política.

Ainda, a **2GOFintech** disponibiliza um Canal de Denúncia, que irá realizar o tratamento adequado das ocorrências encaminhadas pelo [e-mail], por meio do(a): recebimento, análise preliminar, classificação, tratamento, monitoramento, investigação, tomada de decisão e reporte das denúncias ao(s) órgão(s) competente(s), até o devido encerramento das ocorrências.

Além do disposto acima, esta Política também tem o objetivo de estabelecer procedimentos para a execução de processos de **KYC, KYP** e **KYE**.

4. APLICABILIDADE

Esta Política é aplicável e abrange todos os departamentos da **2GOFintech**, incluindo seus Administradores e Colaboradores, os quais devem aderir e se obrigar a respeitar aquilo que seja aqui estabelecido.

5. RESPONSABILIDADES

A Área de Compliance por meio do diretor responsável pelo cumprimento das obrigações previstas nesta Política (Diretor de PLDFT), é a responsável por dar o suporte adequado para que as diretrizes desta Política sejam cumpridas pela **2GOFintech**.

Constituem atribuições e responsabilidades da Área de Compliance e ao Diretor de PLDFT, para fins desta Política:

- Gerir e atualizar anualmente os procedimentos dispostos nesta Política, com base na legislação e normas aplicáveis;
- Acompanhar alterações, atualizações, revogações e publicações do ambiente regulatório e prestar informações às demais áreas da **2GOFintech** em relação aos riscos de conformidade;
- Acompanhar e coordenar a atuação dos responsáveis pela execução das atividades diárias e a aderência da **2GOFintech** a esta Política, ao ordenamento jurídico, à regulamentação infralegal, e a todas os documentos internos da **2GOFintech**;

- Garantir que todos os regulamentos internos e externos ao qual a **2GOFintech** se obrigue, sejam cumpridos;
- Promover a cultura organizacional de conformidade, prevenção e combate à Lavagem de Dinheiro e Financiamento ao Terrorismo, contemplando os Administradores, Colaboradores, Fornecedores, Prestadores de Serviços e Parceiros de Negócios;
- Testar e avaliar a aderência da **2GOFintech** às leis, regulamentações, recomendações de órgãos de supervisão e às políticas relacionadas;
- Aplicar e disseminar as diretrizes, códigos e políticas internas da **2GOFintech** relacionadas à ética, conduta e integridade, utilizando mecanismos que assegurem o alcance a todos os Administradores, Colaboradores, Fornecedores, Prestadores de Serviços e Parceiros de Negócios;
- Disponibilizar o acesso a esta Política para todos os Colaboradores da **2GOFintech**, além de realizar treinamentos e dar suporte garantindo a compreensão geral acerca dos temas aqui dispostos;
- Avaliar os riscos de novos Clientes, Parceiros ou Colaboradores, inclusive se estão expostos em listas sancionadoras, incluindo as listas de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, e definir pela sua aceitação ou não, conforme análise de vulnerabilidades;
- Realizar monitoramentos internos;
- Criar e gerenciar os mecanismos de controle voltados à prevenção à Lavagem de Dinheiro e do Financiamento ao Terrorismo;
- Assegurar o cumprimento dos mecanismos de atuação do Canal de Denúncias;
- Monitorar as ocorrências sobre Transações atípicas ou suspeitas identificadas pelas ferramentas tecnológicas da **2GOFintech** ou que sejam comunicadas pelos Colaboradores;
- O enquadramento e monitoramento de PEP, no que couber;
- A análise, identificação, qualificação, classificação de Clientes, bem como dos beneficiários finais, quando aplicável;
- A comunicação com o COAF, Bacen, Ministério da Justiça e Segurança Pública;

- Atuar nos processos de criação de novos produtos na **2GOFintech** para alertar sobre possíveis vulnerabilidades que facilitarão a utilização do novo produto sob um viés ilícito; e

- Adotar regras específicas que regulem situações que comumente envolvem riscos, inclusive relacionados à Lavagem de Dinheiro ou Financiamento ao Terrorismo.

As demais áreas da **2GOFintech** deverão comunicar a Área de Compliance sobre quaisquer atividades suspeitas relacionadas à Lavagem de Dinheiro e Financiamento ao Terrorismo.

6. KNOW YOUR PARTNER ("KYP"), KNOW YOUR CUSTOMER ("KYC") e KNOW YOUR EMPLOYEE ("KYE")

Os procedimentos aqui elencados possuem a finalidade de impedir que as atividades da **2GOFintech** sejam, de qualquer forma, utilizadas para a prática de algum dos crimes elencados nesta Política.

Estes procedimentos possuem o viés de garantir a ética e integridade da **2GOFintech** perante os seus Administradores, Colaboradores, Parceiros de Negócios, Clientes, Fornecedores e Prestadores de Serviços, e evitar o envolvimento com pessoas mencionadas em listas sancionadoras, incluindo as listas de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas.

Os dados informados nos procedimentos de KYC e KYP serão confirmados por meio do envio de documentos e/ou mediante consulta em bancos de dados públicos ou privados, tais como *bureaux* de análises de crédito e risco, além de base de dados interna ou que seja compartilhada por outras empresas.

Haverá o armazenamento das informações obtidas nos procedimentos de KYC e KYP, as quais devem ser compatíveis com o perfil de risco definido pela Área de *Compliance*, de acordo com a natureza do negócio e o risco ao qual a **2GOFintech** será exposta.

As informações cadastrais serão arquivadas pelo período mínimo de 10 (dez) anos para o KYC, contados a partir do primeiro dia do ano seguinte após o término do relacionamento com o Cliente, e pelo período mínimo de 10 (dez) anos para KYP e KYE, contados a partir da data de encerramento da relação contratual.

Periodicamente, a **2GOFintech** deverá executar testes para a validação das informações cadastrais fornecidas. Caso existam inconsistências nestas informações, a **2GOFintech** realizará

as devidas tratativas, visando à regularização e sanitização da base de clientes em listas restritivas, e sanitização da base de clientes em lista PEP.

a. KNOW YOUR PARTNER

O **KYP** tem como objetivo estabelecer critérios para contratação ou manutenção de um Parceiro de Negócios, visando o combate a fraudes, crimes relacionados à Lavagem de Dinheiro e Financiamento ao Terrorismo.

Um processo de **KYP** feito de maneira eficiente permite a **2GOFintech** conhecer a identidade do parceiro, entender a natureza das atividades, garantir a legitimidade da fonte de renda, detectar padrões suspeitos ou potencialmente fraudulentos e interromper a fraude antes que ela aconteça. Também, por meio de diligência prévia e periódica, permite assegurar sua identificação, qualificação e classificação, prevenindo a ocorrência de Lavagem de Dinheiro e Financiamento do Terrorismo, e buscando evitar o envolvimento com pessoas mencionadas em listas sancionadoras incluindo as listas de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas

Os procedimentos e diretrizes relacionadas ao **KYP** pela **2GOFintech** são:

- Verificar bons antecedentes de integridade dos Parceiros de Negócios;
- Monitoramento de Parceiros de Negócios relevantes;
- Monitoramento de contratações e rescisões contratuais de Parceiros de Negócios;
- Atualização cadastral;
- Assegurar que os Parceiros de Negócios sejam contratados por exigência legal ou sob a justificativa de se tratarem profissionais qualificados para os serviços, sendo assim adequados para atender as necessidades legítimas da **2GOFintech**;
- Assegurar que os Parceiros de Negócios detenham as habilidades, recursos, experiência, credenciais e qualificações apropriadas para cumprir suas obrigações com relação aos serviços a serem prestados a 2GOFintech;
- Consultar as informações disponíveis em sites especializados em prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo e lista de sanção imposta por resoluções do Conselho de Segurança das Nações Unidas;

- Realizar a análise da situação de crédito e endividamento;

- Prevenir a utilização do sistema financeiro por estes indivíduos para crimes de lavagem de dinheiro, financiamento a atividades terroristas, tráficos de drogas e armamentos e demais atividades criminosas; e

- Prevenir a responsabilização da **2GOFintech** por atos de terceiros, com base na legislação vigente, incluindo a Lei Anticorrupção Lei nº 12.846/2013.

Como parte dos requerimentos regulatórios, os seguintes casos relacionados aos Parceiros Negócios e seus representantes devem ser observados:

- Qualquer negócio realizado por Parceiro de Negócios que seja contrário ao procedimento normal para o tipo de operação de que se trata;

- Parceiros de Negócios possuírem em seus quadros de administração e direção Pessoa Exposta Politicamente (PEP);

- Envolvimento dos Parceiros de Negócios em notícias de mídia sobre corrupção ou outras infrações conexas;

- Fornecimento de auxílio ou informações, remunerados ou não, a terceiro em prejuízo do programa de prevenção à lavagem de dinheiro e combate ao financiamento ao terrorismo da instituição.

- Fornecimento de auxílio ou informações, remunerados ou não, a terceiro em prejuízo do Código de Conduta e Ética da **2GOFintech** e das demais políticas internas correlatas.

Qualquer tipo de comportamento ou antecedente suspeito deve ser investigado, registrado e reportado a Área de Compliance no intuito de mitigar o risco de fraude, corrupção, lavagem de dinheiro ou qualquer outro comportamento potencialmente criminoso por parte dos Parceiros de Negócios.

O processo de seleção e contratação dos Parceiros de Negócios pode seguir os seguintes procedimentos gerais, sem prejuízo de regras específicas determinadas em regulamentos internos da **2GOFintech**, de acordo com a natureza dos serviços e negócios a serem desenvolvidos em cada caso concreto:

- Disponibilização de uma cópia do Código de Conduta e Ética e Políticas de Compliance da **2GOFintech** para os Parceiros de Negócios e das demais políticas aplicáveis;

- Solicitação de documentos mínimos necessários, que devem ser validados pelo Jurídico, juntamente com a minuta do Contrato a ser celebrado;
- Solicitação de esclarecimentos adicionais, caso o departamento responsável pela análise do questionário não classifique as respostas como suficientes;
- Verificação, pelo Jurídico, de existência de cláusula anticorrupção nos contratos com o Parceiro de Negócios; e
- Realização de pesquisa de reputação, incluindo, mas não se limitando a:
    - Procura de dados em diversas listas restritivas pelo mundo, sendo as principais: Office of Foreign Assets Control (OFAC), Organização das Nações Unidas (ONU), Lista de SDN's, União Europeia e Interpol;
    - Antecedentes criminais dos administradores e colaboradores dos Parceiros de Negócios; e
    - Lista PEP (Pessoas Expostas Politicamente).

b. KNOW YOUR COSTUMER

O **KYC** tem como objetivo coletar informações e definir o perfil de Clientes, visando identificar e mitigar fraudes, crime de Lavagem de Dinheiro ou Financiamento ao Terrorismo.

Um processo de **KYC** feito de maneira eficiente permite a **2GOFintech** conhecer a identidade do cliente, entender a natureza das atividades, garantir a legitimidade da fonte de renda, detectar padrões suspeitos ou potencialmente fraudulentos e interromper a fraude antes que ela aconteça. A adoção de diligência prévia e periódica busca assegurar a identificação, qualificação e classificação de tais padrões suspeitos e fraudes, prevenindo a ocorrência de Lavagem de Dinheiro e Financiamento do Terrorismo e buscando evitar o envolvimento com pessoas mencionadas em listas sancionadoras, incluindo as listas de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas.

A **2GOFintech** apenas aceitará potenciais Clientes que desempenhem atividades lícitas e que não sejam contrárias a Legislação Aplicável. O **KYC**, em observância à legislação e regulamentação aplicáveis, visa:

- Verificar bons antecedentes de integridade dos Clientes de Negócios;

- Prevenir a utilização do sistema financeiro por estes indivíduos para os crimes de lavagem de dinheiro, financiamento a atividades terroristas, tráficos de drogas e armamentos e demais atividades criminosas; e

- Prevenir a responsabilização da **2GOFintech** por atos de terceiros, com base na legislação vigente, incluindo a **Lei Anticorrupção Lei nº 12.846/2013**.

Como parte dos requerimentos regulatórios, os seguintes casos relacionados Clientes e seus representantes devem ser observados:

- Qualquer negócio realizado por um Cliente que seja contrário ao procedimento normal para o tipo de operação de que se trata;

- Fornecimento de auxílio ou informações, remunerados ou não, a terceiro em prejuízo do programa de prevenção à lavagem de dinheiro e combate ao financiamento ao terrorismo da instituição;

- Fornecimento de auxílio ou informações, remunerados ou não, a terceiro em prejuízo do Código de Conduta e Ética da **2GOFintech** e das demais políticas internas correlatas;

- O cadastro é parte inerente ao processo de **KYC**.

Qualquer tipo de comportamento ou antecedente suspeito deve ser investigado, registrado e reportado ao setor de Compliance no intuito de mitigar o risco de fraude, corrupção, lavagem de dinheiro ou qualquer outro comportamento potencialmente criminoso por parte dos Clientes.

Os relatórios emitidos para determinados fins de verificação serão devidamente armazenados pela Compliance.

c. KNOW YOUR EMPLOYEE

O procedimento de **KYE** serve para gerir a contratação e monitoramento de Colaboradores da **2GOFintech** de forma a prevenir e reduzir o risco de práticas ilícitas de qualquer natureza, incluindo, a prevenção e combate à Lavagem de Dinheiro e o Financiamento do Terrorismo.

O **KYE** de Colaboradores é referente a criação de uma conta de pagamento em nome do Colaborador, dessa forma, este também se torna um Usuário / Cliente **2GOFintech**.

Dentre as diretrizes a serem seguidas relacionadas ao **KYE**:

- Ciência e adesão de todos os Colaboradores às regras, normativos, diretrizes e treinamentos da **2GOFintech**;
- Implementação de procedimento para a seleção de Colaboradores;
- Monitoramento do comportamento e conduta dos Colaboradores em atividades que exercerem para a **2GOFintech**;
- Treinamentos e aculturamento de Colaboradores sobre ética, integridade e prevenção à Lavagem de Dinheiro, Financiamento ao Terrorismo, corrupção e fraudes em geral;
- Avaliação das transferências dos Colaboradores entre áreas da **2GOFintech**, bem como eventuais desligamentos;
- O cadastro (item 7, abaixo) é parte inerente ao processo de **KYE.**

A **2GOFintech**, por meio de sua área de Recursos Humanos, estabelece critérios e processos para a seleção e contratação de Colaboradores que possuam perfil condizente com esta Política, visando o cumprimento das responsabilidades que lhe forem atribuídas no exercício de suas atividades.

O monitoramento dos Colaboradores será realizado nos termos da Lei nº 9.613/1998, em especial – e no que couber - de seus artigos 9º, 10 e 11. Deve haver isonomia de tratamento nessa conduta, abrangendo todos os Colaboradores, sendo vedado o monitoramento com fins discriminatórios. A **2GOFintech** deverá comunicar previamente ao Colaborador este monitoramento, mediante a entrega desta Política ou menção expressa em seu contrato de trabalho.

7. CADASTRO

O Cadastro dos Clientes da **2GOFintech** é fundamental para adoção de procedimentos de **KYC**, **KYE** e **KYP**. É pelo cadastro e processo de conhecimento dos clientes (**KYC**) que identificamos e evitamos fraudes, corrupção, lavagem de dinheiro e terrorismo.

O **KYE** de Colaboradores se soma ao **KYC** na **2GOFintech** devido à criação de conta de pagamento em nome do Colaborador para que este receba seu salário, dessa forma, este também se torna um Usuário / Cliente **2GOFintech**.

Na **2GOFintech**, independentemente do tipo de cliente e seu produto (conta de pagamento; adquirência; unidades de negócio; parceiros white lable; intermediação de compra e venda de

criptoativos) os processos de cadastro e **KYC** são realizados para todos de forma igual, sendo os dados elencados abaixo obrigatórios para o cadastro de todos os tipos de clientes.

As diretrizes da **2GOFintech** para o credenciamento ou atualização de cadastro de Clientes e coleta de informações e documentos são:

Documentos e Informações obrigatórias		
Pessoa Física	**Pessoa Jurídica**	**Sócios de Pessoa Jurídica**
Nome completo	Contrato Social	Nome completo
CPF	CNPJ	CPF
RG	Inscrição Estadual	RG
Endereço completo	Endereço completo	Endereço completo
Endereço de e-mail	Inscrição Municipal	Endereço de e-mail
Telefone	Razão Social	Gênero
Celular	Nome Fantasia	Celular
Gênero	Endereço de e-mail	Data de Nascimento
Estado Civil	Telefone	Nacionalidade
Data de Nascimento	Celular	Nome da Mãe
Escolaridade	-	Nome do Pai
Cidade e UF de Nascimento	-	-
Nacionalidade	-	-
Nome da Mãe	-	-
Nome do Pai	-	-

Em atendimento a Resolução **BCB 96/2021** as contas de pessoa físicas não poderão ter o CPF/MF com o status de SUSPENSO, CANCELADO ou NULO assim como para pessoas jurídicas, o CNPJ/MF, com o status de INAPTA, BAIXADA ou NULA. Caso, em já sendo clientes da **2GOFintech** por razões alheias tiverem seus status modificado para os acima explicados, as respectivas contas deverão ser bloqueadas e encerradas imediatamente, observando os requisitos e procedimentos do Termos de Uso das plataformas, aplicativos e site **2GOFintech**.

KYC na prática

a. Análise das informações cadastrais do Cliente:

O primeiro passo é a análise da veracidade dessas informações. É usada uma plataforma de busca, que faz a pesquisa em mais de 200 fontes e retornam vários dados desse documento (nome completo, nome da mãe, data de nascimento, endereços cadastrados, situação dos

documentos entre várias outras informações pertinentes), sendo necessário apenas digitar algum documento ou anexar uma foto desse documento. Além da plataforma escolhida como primária, fazemos outras buscas visado assegurar a credibilidade dos documentos e estabelecer o risco do cliente.

O setor de compliance coleta esses dados, informados pelo cliente e os que retornaram da plataforma, e faz uma comparação das informações analisando se as que foram prestadas equivalem com as que retornaram da plataforma ou de outros meios de verificação. Caso sejam divergentes, é orientado ao funcionário responsável que não prossiga com o cadastro, pois a probabilidade de ser um cadastro falso é grande.

Os funcionários e parceiros White Label da **2GOFintech** deverão pesquisar nas respectivas juntas comerciais os documentos acostados ao sistema e anexar a plataforma as informações e documentos constantes das juntas comerciais, receita federal, conselho de contadores e outros que se façam necessários para a exatidão do perfil de cada cliente, conforme anexo desta política.

O cadastro deve ser preenchido a dar visibilidade e veracidade das informações do cliente. As informações do cadastro devem ser preenchidas com exatidão, não sendo permitido ao operador de cadastro inserir informações que não sejam condizentes com a realidade. A falta de transparência ou uso de informações equivocadas poderá acarretar na demissão do funcionário ou na rescisão do contrato de White Label, e demais sanções a serem aplicadas de acordo com o Contrato de Parceria White Label da **2GOFintech**.

b. DEFININDO UM PERFIL PARA O CLIENTE

Para definir um perfil para o Cliente é necessário compilar todos os dados e analisar criteriosamente, e buscar entender qual atividade o cliente exerce, seu faturamento, localidade entre outras informações. Esses dados são necessários para realizar a identificação, qualificação e classificação dos Clientes nos termos desta Política e da legislação em vigor, pois no primeiro momento é preciso entender o perfil dos clientes, visando começar nossa relação da melhor maneira possível, oferecendo serviços que realmente são necessários e úteis para eles.

O grau de risco de cada cliente é atribuído ao conjunto de informações e fatores descritos na política de gerenciamento de risco da **2GOFintech**.

A **2GOFintech**, suas empresas coligadas, filiais e/ou subsidiárias não manterão negócios com clientes dos países constantes da lista de restrições/sanções do departamento de Estado Norte Americano.

c. RELACIONAMENTO COM O CLIENTE

Essa etapa, diferentemente das duas últimas, não é feita de forma rápida, pois se baseia na relação contínua entre a **2GOFintech** e o cliente. Com a oportunidade de acompanhar a rotina financeira desse cliente, e entendendo muito mais a fundo o seu dia a dia, fica muito mais fácil definir quais produtos e serviços oferecer a eles, e qual a dinâmica das suas transações e negócios. É intuitivo dizer que conhecendo a rotina dos clientes, é mais fácil direcionar promoções, campanhas, produtos e serviços para eles. Além de ser possível analisar transações que estão dentro ou fora do perfil dos clientes.

8. LIMITE DE MOVIMENTAÇÃO FINANCEIRA PARA CLIENTES

A **2GOFintech** prevê que a concessão de limites de crédito em conta de pagamento deve ser compatível com o perfil de risco do titular da conta. A **2GOFintech** entende que, em se tratando de limites de seus clientes: "*Seus limites de movimentação são calculados automaticamente e revisados de forma periódica ou a pedido. Eles podem aumentar ou diminuir de acordo com o histórico de movimentação da sua conta ou da necessidade da sua operação*".

9. PESSOAS EXPOSTAS POLITICAMENTE (PEP)

São Pessoas Expostas Politicamente os Agentes Públicos que desempenham ou tenham desempenhado, nos últimos cinco anos, no Brasil ou no exterior, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e pessoas de seu relacionamento próximo.

A **2GOFintech** realiza a pesquisa através de empresas especializadas nesse ramo de pesquisa com serviço notoriamente reconhecido no mercado, que verificam os dados cadastrais deClientes para identificação de Pessoa Exposta Politicamente, conforme explicado no item 11. abaixo.

O monitoramento de clientes PEP deve ser realizado continuamente visando a integridade da **2GOFintech** e as diretrizes desta Política.

A **2GOFintech** realiza o acompanhamento financeiro de seus Clientes e realiza análises com base em lista de Pessoas Expostas Politicamente para indicação de operações atípicas ou suspeitas que possam configurar ou configurem em Lavagem de Dinheiro.

10. ANÁLISE DE LISTAS RESTRITIVAS (OFAC e Conselho de Segurança da ONU)

Para identificação e análise de integridade dos Clientes, verificação de identidade, compreensão das atividades exercidas pelo Cliente, conhecimento de origem e destino dos recursos, a **2GOFintech** realiza a análise de listas restritivas, além de outras pesquisas e checagens listadas no item 11. desta Política.

As verificações também são aplicáveis aos Colaboradores da **2GOFintech** e as listas averiguadas são:

- Pesquisa online no Conselho de Segurança das Nações Unidas: https://www.un.org/securitycouncil/sanctions/information
- Pesquisa online na "Sanctions List Search" disponibilizada pela Office of Foreign Assets Control (OFAC): https://sanctionssearch.ofac.treas.gov/

Caso sejam levantados quaisquer indícios de crimes de Lavagem de Dinheiro, Financiamento ao Terrorismo ou outros crimes relevantes, ficará a cargo da Área de Compliance a avaliação de riscos e procedimentos a serem adotados para o imediato bloqueio ou exclusão de Cliente e demissão (sendo funcionário da **2GOFintech**) ou rescisão contratual de terceiros Colaboradores dos quadros da **2GOFintech**.

11. BACKGROUND CHECK E PESQUISA DE MÍDIA NEGATIVA

Após a realização do cadastro do cliente dentro do ambiente da **2GOFintech**, é iniciado o processo de **KYC** realizado pela 2GO Fintech, por meio de empresa(s) especializada(s) contratada(s) especialmente para esse fim.

Este processo é realizado após o preenchimento do CPF/CNPJ e e-mail no sistema de cadastro da **2GOFintech**, e todos os clientes devem passar pelo processo de KYC, não existindo exceções. Além do processo de **KYC**, a **2GOFintech** realiza consultas no TJ, JUCESP, SINTEGRA e Receita Federal.

Caso seja necessário, a diretoria de Compliance analisará os processos que envolvam os clientes ou possíveis clientes para decidir sobre a abertura de conta ou continuidade dos negócios/parceria. A decisão sobre a abertura ou continuidade cabe primeiramente a diretoria de Compliance e em sua falta, a alta administração.

O processo do KYC consiste na condução de prova de vida, envio de selfie e envio de documentos de identificação (documento frente e verso). Além das auto declarações informadas no processo.

As checagens e processos realizados pela 2GO Fintech (e/ou por meio de seus parceiros terceirizados) são, mas não se limitando a:

- Verificação de fraude;
- Verificação de pessoa politicamente exposta;
- Identificação do documento e se ele se encontra legível;
- Identificação de CPF;
- Identificação de selfie (nesse passo o possível cliente deverá segurar o documento apresentado como identificação);
- Facematch;
- Consulta do CPF;
- Nomes equivalentes;
- Óbito;
- Banco de suspeitos do CAF;
- Banco privado de suspeitos da **2GOFintech**;
- Dados oficiais;
- Ações relacionadas ao cliente: Processos; réu em processos; processos criminais;
- Presença em lista de sanções; e
- Exposição política.

Realizamos, por meios próprios e/ou por meio de prestadores de serviços terceirizados, pesquisas de pessoas físicas e jurídicas utilizando os seguintes dados:

- Pessoas Físicas: CPF regular, nome equivalente, antecedência criminal (polícia criminal e federal), número de CPF válido, dados pessoais (nome completo, CPF, data de nascimento, nome da mãe, nome do pai e situação do CPF), endereços e contatos, informações financeiras (estimativa de patrimônio, renda estimada, assistência social, restituições de Imposto de Renda), informações profissionais e acadêmicas.
- Pessoas Jurídicas: Número de CNPJ autêntico, CNPJ ativo na Receita Federal, verificação de protestos financeiros, dados empresarias (razão social, situação, nome fantasia, data

de abertura, CNPJ, regime tributário, Inscrição estadual, porte, atividade econômica principal, natureza jurídica, capital social, CNAE - atividades econômicas secundárias, endereços e contatos da empresa, quadro societário e administrativo, Informações judiciais da empresa, KYC Compliance empresarial, KYC Compliance dos sócios, certidões de regularidade da empresa.

A decisão de aprovação, rejeição ou apontamento de pendências com relação à avaliação da checagem realizada pode ser automatizada, uma vez que os parâmetros já foram definidos pela diretoria de Compliance. Tal decisão (inclusive se automatizada) do processo de KYC é realizada, com base nos seguintes dados: CPF, selfie (*a selfie consiste em uma foto do cliente, segurando o documento, próximo ao rosto. O documento deve aparecer por completo -contendo foto, nome, data de nascimento e CPF, de forma nítida e legível. Se necessário, será solicitado o envio de duas fotos (uma com a frente e outra com o verso do documento), facematch*, óbito, bancos suspeitos, banco privado, documentação inválida e CNPJ inválido e demais parâmetros delimitados pela diretoria de Compliance.

A selfie consiste em uma foto do cliente ou do potencial cliente, segurando o documento, próximo ao rosto. O documento deve aparecer por completo (contendo foto, nome, data de nascimento e CPF), de forma nítida e legível. Se necessário, a **2GOFintech** solicitará duas fotos, uma com a frente e outra com o verso do documento.

Caso o cliente não seja aprovado no processo automatizado de KYC, a área de Compliance poderá realizar uma pesquisa mais aprofundada com relação aos *red flags* apontados pelo sistema automatizado e geradores da não aprovação. Tal procedimento pode ser adotado uma vez que há ocasiões em que o processo sinaliza *red flags* que não possuem muita relevância ou real motivo para o bloqueio de determinado cliente. Nesses casos, o *Compliance* realiza um *background check* de forma manual e mais aprofundado, de modo a investigar a fundo os *red flags* sinalizados no processo de KYC automatizado – sempre objetivando não realizar bloqueios ou negativas de cadastro infundadas.

A Diretoria de Compliance acessará os processos digitais através dos meios legais e de acordo com a sua necessidade para fins de avaliação e contagem nos critérios de gerenciamento de risco.

Nos casos em quem os *red flags* forem disparados o cliente ou o possível cliente poderá ser aceito com a condição *sine qua non* de ser devidamente identificado no Compliance como sendo de alto risco, bem como terá a sua movimentação financeira limitada.

Além dos casos já estipulados como Lavagem de Dinheiro, Financiamento ao Terrorismo e outros, ficam impossibilitados de abrirem conta na 2GOFintech ou permanecerem como

clientes da 2GOFintech as pessoas físicas que tiverem seus nomes envolvidos em crimes contra o sistema financeiro nacional, terrorismo, tráfico de drogas, armas e/ou pessoas. Bem como as pessoas jurídicas que tenham por sócios pessoa físicas que tenham seus nomes expostos/vinculados/relacionados nas condições acima, ou incluídas em listas de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas.

12. PROCEDIMENTO E REGISTRO DAS OPERAÇÕES

Todos os documentos, informações e registros relevantes para os fins mencionados nestaPolítica são arquivados pela **2GOFintech** pelo prazo mínimo de 5 (cinco) anos.

A **2GOFintech** define que as informações, documentos e registro devem prever e permitir a identificação da movimentação financeira completa de cada Cliente, bem como as avaliações de risco realizadas pela **2GOFintech** e informações relevantes de identificação de Clientes.

13. MONITORAMENTO E ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS

A **2GOFintech** realiza o monitoramento de Operações de seus Clientes para verificar se estas estão compatíveis com seu perfil, capacidade financeira e com sua atividade econômica. Este monitoramento é fundamental para a checagem de quaisquer atividades ou situações suspeitas em Operações da **2GOFintech**.

Em casos de Pessoas Expostas Politicamente ou Operações que não sejam possíveis identificar o beneficiário final, serão adotados os seguintes procedimentos para análise: perfil; origem; destino dos recursos e a capacidade financeira dos clientes.

Os parâmetros para o sistema de monitoramento da **2GOFintech** devem ser definidos com base em Matriz de Risco (disposta em Política de Gerenciamento de Riscos da **2GOFintech**) e o prazo de monitoramento de cada tipo de Cliente, que não pode exceder o prazo de quarenta e cinco dias, contados a partir da data da seleção da operação ou situação, ficará a cargo da Área de Compliance.

Nos casos de identificação de risco alto na Matriz de Risco da **2GOFintech**, o monitoramento deve seguir de forma criteriosa e continuamente.

As áreas relacionadas a novos produtos da **2GOFintech** devem, sempre que um novo produto for desenvolvido, pedir aprovação e realizar testes de conformidade com a Área de Compliance para identificação de possíveis riscos de Lavagem de Dinheiro ou Financiamento ao Terrorismo.

Neste sentido, qualquer operação vinculada ao novo produto só poderá ser realizada/comercializada após tal avaliação.

14. BLOQUEIO DE ATIVOS

A **Lei nº 13.810/2019** e a **Resolução BCB nº 44/2020** preveem a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, estabelecidas pelo Conselho de Segurança das Nações Unidas, quando dispostas em Lista da ONU.

A responsabilidade de avaliar os casos e definir o tratamento de cada situação será da Área de Compliance.

A **2GOFintech** irá estabelecer procedimentos para bloquear os ativos e/ou fundos das pessoas ou entidades identificadas nos programas de sanções da ONU, conforme os requerimentos do programa e comunicar as autoridades, conforme aplicável.

Sem prejuízo, Clientes que possuem relações relevantes relacionadas aos crimes de Lavagem de Dinheiro, Financiamento ao Terrorismo, Corrupção e quaisquer outras condutas ilícitas em desacordo com as Políticas da **2GOFintech** devem ser bloqueados e impedidos de realizar qualquer tipo de Operação.

Caso algum Fornecedor, Cliente ou beneficiário final esteja registrado em alguma lista de sanção imposta por resoluções do Conselho de Segurança das Nações Unidas, deverá ser realizado de imediato o bloqueio dos ativos nos termos da Lei nº 13.810/2019, bem como a realização da comunicação do fato ao COAF, ao Bacen, Ministério da Justiça e Segurança Pública e outros órgãos de registro público que forem aplicados.

15. COMUNICAÇÃO AO COAF

Os casos e situações suspeitas que forem identificados em monitoramento realizado pela **2GOFintech** e que apresentarem indícios de Lavagem de Dinheiro ou Financiamento ao Terrorismo serão submetidos para análise de Área de Compliance. Após a análise da Área de Compliance e identificação de ilícitos, será realizada comunicação para registro no site do COAF.

Caso a situação suspeita envolva Pessoa Exposta Politicamente, esta informação também deverá ser reportada no acesso ao sistema do COAF.

A comunicação ao COAF será realizada no prazo legal e sem dar ciência aos envolvidos ou a terceiros. Em caso de inexistência de comunicações em determinado ano, a **2GOFintech** providenciará o envio de declaração negativa, até dez dias úteis após o encerramento do referido

ano, atestando a não ocorrência de operações ou situações passíveis de comunicação ao órgão, na forma da Legislação Aplicável.

A Área de Compliance será a responsável por reportar tal informação e descrever detalhadamente os fatos, indícios e todas as informações relevantes.

A **2GOFintech** adota processos de identificação e mapeamento de Clientes e Fornecedores incluídos nas listas de sanções impostas pelas resoluções da ONU, com o objetivo de cumprir com as seguintes obrigações:

- Garantia da comunicação imediata ao Diretor de PLDFT e de Compliance da **2GOFintech** de qualquer fornecedor, cliente ou beneficiário ("Sancionado") que conste em qualquer lista de sanções que seja aplicável à Lei nº 13.810/2019;

- Realização do imediato encerramento do relacionamento com o Sancionado, bem como do bloqueio para novas transações;

- Adoção das medidas necessárias para a realização da indisponibilidade de ativos de titularidade, direta ou indireta, do Sancionado, na forma e nas condições definidas pelo COAF ou outro órgão com finalidade semelhante;

- Comunicação do fato ao COAF ou outro órgão com finalidade semelhante, Bacen, Ministério da Justiça e Segurança Pública e demais órgãos competentes, conforme aplicável.

Caberá à **2GOFintech** verificar se já foram adotadas as providências correspondentes e adotá-las, caso necessário.

O disposto nesta Política aplica-se às relações de negócio mantidas pela **2GOFintech** e seus Clientes, e às relações que venham a ser iniciadas posteriormente com quaisquer Clientes alcançados pelas determinações de indisponibilidade.

Os procedimentos aqui listados estão integrados nos processos de mapeamento e monitoramento identificados nesta Política.

- Procedimentos a serem adotados pela **2GOFintech** em caso de sanções impostas pelo CSNU.

Para assegurar a efetividade desta Política, a **2GOFintech** adotará os seguintes procedimentos no caso de sanções impostas pelo CSNU:

- Procedimentos de indisponibilidade de ativos de Pessoa Física, Pessoa jurídica e de entidades (proibição de transferir, converter, trasladar, disponibilizar ativos ou deles dispor, direta ou indiretamente);

- Comunicação tempestiva ao Bacen, ao Ministério Público e ao Coaf referente as pessoas investigadas ou acusadas de terrorismo que aparecem nas listas sancionadoras da ONU;

- Acompanhamento de forma direta e atualizada, das informações divulgadas no site do CSNU, https://lnkd.in/dgErmBjp;

- Na detecção de irregularidades, a **2GOFintech** deve assegurar que se mantenham os ativos sob verificação, para efeito de colocá-los em regime de indisponibilidade;

- No caso de constatação de irregularidades, a **2GOFintech** deverá cumprir imediatamente as medidas estabelecidas nas resoluções do CSNU no caso de comunicação por meio do sistema BC Correio, e dirigidas especificamente para pasta Deati/CSNU;

- Ainda, a **2GOFintech** deverá realizar as comunicações para o Ministério da Justiça e Segurança Pública (MJSP) devem ser dirigidas ao endereço institucional de e-mail csnu@mj.gov.br.

O monitoramento de informações abrange inclusões e exclusões de listas de pessoas naturais, pessoas jurídicas, entidades ou ativos sujeitos a medidas de indisponibilidade decorrentes de sanções ou determinações do CSNU ou de seus comitês de sanções.

16. BLOQUEIO DE USUÁRIOS/CLIENTES

Usuários/Clientes podem ser bloqueados ou excluídos nas seguintes hipóteses após a análise da Área de Compliance:

- cadastro não finalizado por causa de incompatibilidade de informações prestadas e documentos enviados;

- estar nas listas restritivas da ONU, OFAC ou da **2GOFintech**

- apresentar transações suspeitas e, após a análise da Área de Compliance, se optar pela comunicação ao COAF;

- Documentação divergente da solicitada;

- Status de CPF/MF e CNPJ/MF contrários a esta Política, procedimentos internos da **2GOFintech**, e requisitos da resolução **Resolução BCB 96/2021 (das diretrizes para abertura, manutenção e encerramento de contas de pagamento)**.

17. COMUNICAÇÃO E TREINAMENTOS

A comunicação desta Política tem o objetivo de realizar a disseminação de padrões de integridade e conduta ética da **2GOFintech**, além de garantir que medidas ou sanções sejam aplicadas quando forem detectadas falhas de conformidade ou crimes de Lavagem de Dinheiro e Financiamento ao Terrorismo.

A Área de Compliance é a responsável por fornecer treinamentos a todos os Colaboradores da **2GOFintech**. Os treinamentos para fins desta Política devem promover o aculturamento dos Colaboradores da **2GOFintech** a fim de que estes saibam detectar operações que caracterizem indícios de ocorrências de crimes de lavagem de dinheiro e financiamento ao terrorismo, além de prever uma familiarização com a legislação em vigor sobre o tema.

Esta Política deverá estar disponível a todos os Colaboradores e Administradores da **2GOFintech** em local de fácil acesso que permita a consulta a qualquer momento.

A área de Compliance é a responsável por elaborar um programa específico de treinamento anual de prevenção à lavagem de dinheiro e financiamento ao terrorismo da **2GOFintech**.

Os treinamentos são atualizados anualmente e são aplicáveis a todos os Colaboradores e Administradores da **2GOFintech**.

18. CICLO DE REVISÃO

A área de Compliance é a responsável pela revisão, alteração e atualização desta Política a cada 12 (doze) meses, ou em tempo menor no caso de alterações regulatórias ou legais.

Esta Política deve ser aprovada pelos Administradores, bem como suas atualizações e revisões.

Quando houver alteração nesta Política, novos treinamentos e comunicações deverão ser realizados pela área de Compliance a todos os Colaboradores da **2GOFintech**.

19. DISPOSIÇÕES FINAIS

Esta Política é aplicável a todos os Clientes, Colaboradores, Administradores, Parceiros de Negócios, Prestadores de Serviços e outros terceiros que possuam relacionamento comercial com a **2GOFintech**.

A **2GOFintech** deverá avaliar a efetividade desta política, seus procedimentos e controles internos, e documentar em relatório específico que deve ser elaborado anualmente, com data-base de 31 de dezembro e encaminhado, para ciência, até 31 de março do ano seguinte ao da data-base, aos Administradores da **2GOFintech**.

O relatório deve conter informações que descrevam: a metodologia adotada na avaliação de efetividade; os testes aplicados; a qualificação dos avaliadores; e as deficiências identificadas, como também, no mínimo, a avaliação: (i) dos procedimentos destinados a conhecer clientes, incluindo a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais; (ii) dos procedimentos de monitoramento, seleção, análise e comunicação ao Coaf, incluindo a avaliação de efetividade dos parâmetros de seleção de operações e de situações suspeitas; (iii) da governança da política de PLDFT; (iv) das medidas de desenvolvimento da cultura organizacional voltadas à PLDFT; (v) dos programas de capacitação periódica de pessoal; (vi) dos procedimentos destinados a KYE e KYP; (vii) e das ações de regularização dos apontamentos oriundos da auditoria interna e da supervisão do Banco Central do Brasil.

A **2GOFintech** deverá elaborar plano de ação destinado a solucionar as deficiências identificadas por meio da avaliação de efetividade acima descrita, documentada por meio de relatório de acompanhamento que será elaborado e encaminhado para ciência e avaliação dos Administradores, até 30 de junho do ano seguinte ao da data-base do relatório de avaliação da efetividade da Política, dos procedimentos e dos controles internos.

A área de Compliance da **2GOFintech** deverá ser consultada em caso de dúvidas ou esclarecimentos sobre o conteúdo desta Política ou sobre sua aplicação.

Os Colaboradores e Administradores da **2GOFintech** devem reportar quaisquer suspeitas ou evidências de atos ilícitos e violações a quaisquer instrumentos normativos da **2GOFintech** utilizando o Canal de Denúncias ou via comunicação direta à área de Compliance.

Canal de Denúncias	compliance@2gofintech.com.br