Parabank.
banco digital

POLÍTICA DE PROTEÇÃO GERAL DE DADOS
DEPARTAMENTO DE COMPLIANCE
PARABANK

SUMÁRIO

1. OBJETIVO

A Presente Política de Proteção Geral de Dados tem por objetivo estabelecer diretrizes gerais para a proteção de dados pessoais de seus diretores, colaboradores, clientes, fornecedores e parceiros comerciais no ambiente sistêmico da PARABANK e demais empresas do grupo, sendo que a coleta, manuseio e armazenamento de informações públicas e sensíveis de Pessoas Físicas e Jurídicas fazem parte das atividades operacionais da empresa. Dessa forma apresentamos nesse documento os principais controles adotados com vistas a:

a) Estar em conformidade com as leis e regulamentações aplicáveis de proteção de Dados Pessoais e seguir as melhores práticas de mercado;
b) Proteger os direitos dos diretores, colaboradores, clientes, fornecedores e parceiros comerciais, contra os riscos de violações de Dados Pessoais;
c) Agir com transparência nos processos operacionais da PARABANK e demais empresas do grupo, no que tange o Tratamento de Dados Pessoais; e
d) Promover a conscientização de toda a empresa em relação à proteção de Dados Pessoais e questões de privacidade;

As políticas e procedimentos descritos nesta Política baseiam-se principalmente nas Leis n. 12.965/14 e 13.709/18 e alterações.

2. PÚBLICO ALVO

Todos os diretores, colaboradores, clientes, fornecedores e prestadores de serviços que possuam relacionamento com a PARABANK e demais empresa do grupo, em especial os Departamentos de Recursos Humanos, Cadastro, Tecnologia da Informação, Jurídico e Compliance, por terem responsabilidades diretas com a recepção, análise, tratamento e custódia das informações pessoais dos clientes Pessoa Físicas e Jurídicas.

3. DEFINIÇÃO

A Lei Geral de Proteção a Dados passará a ser aplicável a partir de 1º de janeiro de 2021 e com a aplicação de sanções em agosto de 2021. A presente política demonstra os cuidados e responsabilidades que a PARABANK e demais empresas do grupo possuem com o tratamento de dados pessoais, o que inclui atividades como coleta, armazenamento, utilização, compartilhamento e eliminação de informações relacionadas a pessoas físicas ou jurídicas.

LGPD: Lei Geral de Proteção de dados, que consiste em definir critérios de segurança e procedimentos operacionais para coleta, tratamento e armazenamento de dados públicos ou privados. Além de garantir o respeito à privacidade de terceiros e inviolabilidade da intimidade de nossos clientes. Essas atividades serão reguladas e fiscalizadas pela Agência Nacional de Proteção de Dados.

ANPD: É o órgão regulador e fiscalizador nomeado pelo governo federal para fiscalizar as empresas, quando a adoção das medidas preventivas na utilização de dados pessoais de clientes, aplicar sanções administrativas para empresas que infrinjam as definições descritas na lei e ainda atuação com ações educativas e corretivas no mercado para que as empresas consigam se enquadrar na legislação.

SIGILO BANCÁRIO: As instituições financeiras e demais empresas autorizadas pelo Banco Central a atuar no mercado financeiro, devem manter sigilo em suas operações ativas e passivas e serviços prestados. Os únicos casos em que as informações sobre clientes, serviços ou operações podem ser divulgadas a terceiros, sem representar violação do sigilo bancário, são, com o consentimento expresso do cliente, a troca de informações entre as instituições financeiras para fins de registro, o repasse de informações para empresas de proteção ao crédito, respeitando as legislações vigentes e a ocorrência ou suspeita de que atos ilícitos criminais ou administrativos, nesse caso poderá ser fornecidas às autoridades pertinentes as informações necessárias.

LEI DE PREVENÇÃO À LAVAGEM DE DINHEIRO: A luz da legislação vigente é crime ocultar ou dissimular a natureza, origem, localização, disponibilidade, transação ou propriedade de ativos, direitos ou valores resultantes, direta ou indiretamente, de qualquer crime, bem como seu uso em atividade econômica ou financeira e a participação em um grupo, associação ou escritório sabendo que suas atividades principais ou secundárias são orientadas para a prática de tais atos.

A Lei de Combate à Lavagem de Dinheiro e a regulamentação aplicável do CMN e do Banco Central do Brasil estabeleceram que as instituições financeiras devem, entre outras coisas:

a) Manter registros atualizados relativos a seus clientes permanentes (incluindo seus dados cadastrais, declarações de propósito e natureza das transações, sua capacidade financeira, bem como verificação da caracterização de clientes como indivíduos expostos politicamente);
b) Adotar políticas, procedimentos e controles internos;
c) Registrar transações em moeda nacional e estrangeira, valores mobiliários, metais ou qualquer outro ativo que possa ser convertido em dinheiro, incluindo registros específicos das emissões ou recarga de cartões pré-pagos;
d) Manter registros das transações ou grupos de movimentação de fundos realizados por pessoas físicas ou jurídicas pertencentes ao mesmo grupo ou conglomerado financeiro, em valor total superior a R$ 10.000 em um mês ou que revelem um padrão de atividade que sugira um esquema para evitar identificação, controle e registro;
e) Analisar transações financeiras que possam indicar intenções criminosas; e
f) Manter registros de cada transferência de fundos relacionada a depósitos, transferências e ordens de pagamento em montantes que excedam R$ 2.000,00.

CONTROLADOR: O controlador é quem exerce controle geral sobre os dados capturados dos clientes Pessoa Física ou Jurídica. Ou seja, o controlador terá a responsabilidade de decidir o "porquê" e o "como" da atividade de tratamento de dados, sendo o agente responsável por todo o ciclo de vida dos dados – da sua coleta à sua exclusão.

OPERADOR: O operador é a Pessoa Física ou Jurídica, que realiza o tratamento de dados pessoais em nome do controlador. O operador não controla os dados e não pode alterar a finalidade ou o uso do conjunto particular de dados relacionados a determinado tratamento, devendo tratar tais dados de acordo com as instruções e dentro das finalidades definidas e impostas pelo controlador.

ENCARREGADO: O Encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e O Órgão Fiscalizador e Regulador.

DIGITALIAÇÃO DE DOCUMENTOS: Digitalização e armazenamento dos documentos digitalizados, destaca-se pela necessidade de manutenção dos documentos digitalizados à disposição do Banco Central pelo prazo mínimo de cinco anos, devendo ser considerada a manutenção de cópia de segurança dos documentos digitalizados em local físico distinto do local onde está armazenado o documento digitalizado e a necessidade de utilização de padrão de assinaturas digitais legalmente aceito, a fim de que seja possível verificar a integridade e a autenticidade do documento digitalizado.

DADO PESSOAL: é qualquer informação relacionada a uma pessoa física identificada ou identificável., tal qual RG, CPF, endereço, data de nascimento, mas informações como hábitos de consumo, localização geográfica, perfil comportamental, preferências, históricos de compras e outras informações consideradas com pessoal. São considerados ainda dados pessoais informações sobre navegação na Internet, endereço IP e cookies quando for possível identificar a pessoa ligada aos dados.

DADOS SENSÍVEIS: É considerado dado sensível, o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

DADO ANONIMIZADO: Dado anonimizado é o oposto de dado pessoal, ou seja, é o dado que não pode ser associado a um indivíduo.

TRATAMENTO DE DADOS: Toda operação realizada com dados pessoais, sendo considerada as ações de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

4. DIRETRIZES

A Lei Geral de Proteção de Dados estabelece alguns princípios que se aplicam a todas as atividades de tratamento de dados. São valores gerais que orientam a compreensão, interpretação e aplicação das regras estabelecidas pela legislação e que devem sempre ser considerados quando uma atividade envolver tratamento de dados pessoais.

Os dados pessoais só devem ser coletados e tratados para os propósitos específicos e legítimos que tenham sido informados ao titular de dados e sejam compatíveis com o contexto do tratamento. O tratamento deve ser limitado ao mínimo necessário para aquelas finalidades que foram informadas aos titulares.

Precedendo a coleta, armazenamento ou qualquer tipo de utilização de dados de cliente é necessário informar e solicitar autorização de manuseio desses dados, tornando claro que os dados serão tratados e para quais finalidades e o porquê do tratamento.

4.1. Transparência e Livre Acesso

Garantir que os titulares de dados pessoais tenham acesso a informações claras e facilmente acessíveis sobre como seus dados são tratados, por quem e para quais finalidades. Isso pode ser feito de diversas maneiras, conforme a natureza do tratamento.

Manter clara, objetiva, sucinta e específica nas políticas de privacidade ou em outros materiais semelhantes, e facilitar o acesso a esses materiais para os titulares de dados, além de disponibilizar um canal de comunicação acessível para que os titulares de dados possam esclarecer suas dúvidas e solicitar informações.

4.2. Segurança

A PARABANK e demais empresas do grupo ao tratar dados pessoais de seus clientes, implementa medidas técnicas e administrativas capazes de proteger esses dados de acessos não autorizados, perda, destruição, alteração, ou divulgação indevida, bem como possui procedimentos de prevenção para quaisquer incidentes que possam causar danos aos titulares de dados. Isso pode incluir, por exemplo, controles de acessos, técnicas de criptografia, revisão de arquitetura de sistemas, separação de bancos de dados, entre outros.

4.3. Discriminação

Os dados coletados não serão em hipótese alguma utilizadas para fins discriminatórios, ilícitos ou abusivos.

4.4. Correção de Dados e Atualização

A PARABANK e demais empresas do grupo, preocupados com a segurança e veracidade das informações de seus clientes, além de aderir as legislações vigentes permite que seu cliente titular dos dados tenha o direito à correção deles, ou retificação das informações a seu respeito. Esse direito é derivado do princípio da qualidade dos dados, previsto no artigo 6º, V, da LGPD, pelo qual garante-se aos titulares.

4.5. Confirmação do Tratamento dos Dados e Direito de Acesso

A PARABANK e demais empresas do grupo deixam claros aos seus clientes que possuem direito à confirmação da existência de tratamento de seus dados pessoais e que esses são ou não objeto de tratamento por agente controlador.

O titular de dados pessoais tem assegurado o acesso aos seus dados pessoais tratados pelo controlador. Ou seja: o titular pode exigir do controlador cópia dos dados pessoais de sua titularidade que são objeto de tratamento por esse controlador. Esse direito deriva do princípio do livre acesso, previsto no artigo 6º, IV, da LGPD, pelo qual garante-se aos titulares a “consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”.

4.6. Anonimização, bloqueio ou eliminação de dados

O cliente titular das informações, pode exigir que dados pessoais tidos como desnecessários, excessivos ou tratados em desconformidade com a atual legislação sejam anonimizados, bloqueados ou eliminados. limitando do tratamento dos dados ao mínimo necessário para a realização das finalidades definidas pela PARABANK e demais empresas do grupo, tendo apenas abrangência aos dados pertinentes, proporcionais e não excessivos. Dessa forma a PARABANK e demais empresas do grupo, irá aceitar a solicitação imposta pelo cliente, apresentando-lhe evidências de que realizou as atividades necessárias para garantias as restrições dos dados.

O cliente poderá exigir, mediante requerimento expresso, a eliminação dos dados pessoais tratados com o seu consentimento, exceto nas hipóteses previstas na legislação que prevê o armazenamento contínuo dos dados dos clientes por obrigação legal ou regulatória, estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

4.7. Portabilidade dos dados

A PARABANK e demais empresas do grupo possibilitam ao titular dos dados receber seus dados pessoais de modo estruturado (formato interoperável ou de uso corriqueiro), com a possibilidade de leitura automática por outros computadores, podendo o cliente fornecer esses dados para outro fornecedor de serviço ou produto.

4.8. Consentimento ao fornecer os dados

A PARABANK e demais empresas do grupo devem solicitar o consentimento formal do cliente ao fornecer seus dados pessoais, conforme definido em legislação, para que seus dados sejam manuseados, tratados e armazenados, contudo na impossibilidade do consentimento, o cliente não poderá concluir seu cadastro ou utilizar determinado produto ou serviço da empresa.

É respeitado alguns requisitos para que o consentimento seja considerado válido:

a) **Livre:** o consentimento deve refletir uma manifestação livre da vontade do titular, sendo eu este não pode ser compelido a consentir com o tratamento.
b) **Informado:** o titular deve ter recebido informações claras, objetivas e suficientes para decidir de maneira consciente se concorda com o tratamento de seus dados pessoais para as finalidades descritas pela PARABANK e demais empresas do grupo.
c) **Inequívoco:** o consentimento deve ser demonstrado de maneira inequívoca. Isso pode ser feito por escrito ou por outros meios que demonstrem a vontade do titular, desde que não deixem dúvidas da sua autorização direta. Consentimentos implícitos, que não tenham sido registrados, ou que deixem por algum motivo dúvidas sobre a vontade do titular, serão desconsideradas e entendidas como não consentimento, ou seja, o cliente não terá continuidade no cadastro ou utilização de determinados produtos ou serviços.

A PARABANK e demais empresas do grupo poderão utilizar e tratar dados de clientes (Pessoa Física ou Jurídica) sem seu consentimento expresso, respeitando a legislação vigente, sempre que:

a) **Obrigação legal ou regulatória:** se uma lei ou uma regulamentação definida por órgãos reguladores exigir determinada atividade de tratamento de dados, não é preciso solicitar a autorização do titular de dados.
b) **Quebra de Sigilo Bancário:** Para executar um contrato ou procedimentos preliminares relacionados a um contrato celebrado com o titular de dados pessoais. Por exemplo, para entregar um produto ou um serviço adquirido após a conclusão da compra, naturalmente é preciso conhecer o nome completo, o endereço e outras informações de contato do consumidor.
c) **Cumprimento de Processos Judiciais:** Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, o armazenamento ou outra forma de tratamento de dados pessoais para utilização em eventual processo judicial é possível, independente de autorização do titular.
d) **Interesses Legítimos do Controlador:** Desde que o tratamento de dados não ofereça um risco importante aos direitos e liberdades fundamentais dos titulares de dados, contudo a LGPD exige a análise do impacto à privacidade do titular de dados e a documentação dessa análise quando se utiliza o legítimo interesse.

4.9. Governança

A PARABANK e demais empresas do grupo em conformidade com a Lei Geral de Proteção a Dados - LGPD e para garantir o efetivo cumprimento das suas disposições, adota programa de governança em privacidade de dados, especialmente as obrigações de controles internos, prevenção à lavagem de dinheiro e política de segurança cibernética previstas pelos Reguladores.

O Programa de Governança da PARABANK define critérios e procedimentos internos para o tratamento de dados pessoais, normas de segurança da informação, padrões técnicos, alocação de responsabilidades e obrigações aos diversos colaboradores envolvidos nas atividades operacionais, táticas e estratégicas de

tratamento (Alçada de Poderes), ações educativas, mecanismos internos de supervisão e mitigação de riscos, procedimentos de resposta a incidentes de segurança.

Todos os processos, decisões e ações relacionados à governança de dados pessoais na empresa são documentados e mantidos em arquivo para futuras apresentações aos órgãos reguladores.

5. RESPONSABILIDADE

5.1. Diretoria de Riscos, Compliance e PLD

O Departamento de Compliance possui competência e independência para apurar quaisquer denúncias ou suspeitas de inconformidade praticadas pela PARABANK e demais empresas do grupo, referente as diretrizes estabelecidas na presente Política.

Será responsável ainda por:

a) Revisar e recomendar a aprovação desta Política e suas alterações ao Diretores Executivos e Conselho;

b) Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades, cível e legalmente;

c) Definir e aprovar a estrutura de governança para os assuntos de privacidade e proteção de dados;

d) Fazer o monitoramento permanente e efetivo da implementação das iniciativas de privacidade, incluindo os eventos relacionados a vazamento de Dados Pessoais;

e) Garantir os recursos necessários para a implementação e gerenciamento das iniciativas de privacidade;

f) Reportar aos Diretores Executivos e Conselho, todos os eventos relacionados a vazamento de Dados Pessoais e as decisões tomadas para corrigir o problema e mitigar o risco.

5.2. Diretoria Executiva

Aprovar esta Política e suas futuras alterações e responsabilizar-se pelo uso adequado de Dados Pessoais de clientes utilizados na atividade operacional da PARABANK e demais empresas do grupo.

A Diretoria Executiva será responsável por aprovar a medida disciplinar proposta pelo Departamento de Compliance ou pelo Comitê de Auditoria em casos de infrações cometidas perante as diretrizes estabelecidas na presente Política.

5.3. Responsável pela Privacidade Corporativa

O Comitê de Privacidade tem por responsabilidade garantir o cumprimento da presente Política, bem como fiscalizar intempestivamente os procedimentos operacionais adotados para a coleta, manutenção e descarte de dados pessoais de clientes, bem como:

a) Responsabilizar-se pelo uso adequado de Dados Pessoais em suas atividades;

b) Promover o conhecimento adequado de todos os colaboradores que se utilizam dos dados pessoais dos clientes, em relação à importância da proteção de Dados Pessoais e das atividades internas inerentes as iniciativas de privacidade;

c) Revisar anualmente, ou em prazo menor quando necessário, as iniciativas de privacidade adotadas pela PARABANK e demais empresas do grupo

d) Discutir e tomar decisões técnicas sobre novas atividades de Tratamento de Dados Pessoais, com base nos relatórios de impacto à proteção de Dados Pessoais;

e) Decidir sobre as medidas técnicas a serem aplicadas para eventos alto risco, assim como as medidas disciplinares;

f) Validar a aderência aos requisitos da legislação e da regulamentação aplicáveis, além de garantir privacidade como um padrão e a incorporação no desenho das medidas de segurança;

g) Auxiliar operacionalmente o monitoramento do cumprimento das regras internas e manutenção de KPIs (Key Performance Indicator) relacionados à proteção de dados e privacidade;

h) Auxiliar na condução periódica de avaliações de privacidade, identificando a evolução do programa e os gaps remanescentes e/ou novos;

i) Implantar planos de ação para correção de gaps das iniciativas de privacidade;

j) Emitir relatórios de impacto à proteção de Dados Pessoais (DPIA – Data Protection Impact Analysis) e auxiliar o Departamento de Compliance na tomada de decisão de alinhamento e melhorias desta Política;

k) Monitorar as requisições ou solicitações dos Titulares de Dados Pessoais a fim de garantir que sejam respondidas dentro do prazo; e

l) Garantir a manutenção das evidências de execução e implementação das iniciativas de privacidade;

5.4. Departamento de Segurança da Informação

O Departamento de Segurança da Informação será responsável pelo uso adequado de Dados Pessoais em suas atividades, além de analisar violações e vazamentos de Dados Pessoais bem como efetuar a coleta de evidências técnicas;

Deverá ainda executar de forma contínua o monitoramento e implementação de medidas de segurança para garantir o cumprimento da legislação e da regulamentação aplicáveis, publicações de avisos de privacidade em websites e programas externos e manter atualizada a Documentação Orientadora relativa à Segurança da Informação que estejam na sua competência;

5.5. Departamento de Auditoria Interna e Comitê de Auditoria

A atividade de auditoria interna que atua como a terceira linha de defesa faz parte do sistema de controles internos e tem como objetivo testar a qualidade do sistema de controles internos e assegurar se são suficientes para mitigar ameaças operacionais, incluindo os riscos de não conformidades.

O respectivo comitê será composto pelo responsável executivo da área de auditoria interna, diretor de riscos, compliance e PLD, diretor executivo e convidados quando necessário e terá a responsável por apurar denúncias de violação aos termos desta Política quando as pessoas envolvidas forem um ou mais membros da Diretoria ou alta gestão da empresa, bem como propor a medida disciplinar cabível.

6. SANÇÕES ADMINISTRATIVAS

O descumprimento das disposições legais ou regulamentares internas pode acarretar sanções disciplinares e administrativas, no caso de Diretores e Colaboradores ou o encerramento do relacionamento comercial, no caso de parceiros, fornecedores ou prestadores de serviços.

Quando a área de Compliance tiver conhecimento de situações por parte do colaborador, que representem violação ao estabelecido nesta Política e demais normas internas, a equipe de Compliance, liderada por seu gestor ou Diretor, deverá analisar o caso e tomar as medidas disciplinares cabíveis, conforme abaixo descritas.

O Diretor ou Colaborador será notificado formalmente para apresentar defesa em até 10 (dez) dias úteis contados do recebimento da notificação, sob pena de serem considerados verdadeiros os fatos imputados e aplicadas as penalidades especificadas adiante. Em todos os casos, as notificações serão tratadas com o maior sigilo possível.

Os procedimentos adotados serão conduzidos pelo gestor ou Diretor da área, a quem cabe também a recomendação final das respectivas penalidades para aprovação pela Diretoria da Gestora.

As penalidades aplicáveis resumem-se em advertência, suspensão temporária e afastamento definitivo.

A omissão diante da violação conhecida da lei, de qualquer disposição desta política e demais normas internas, não é uma atitude correta e constitui, em si mesma, uma violação das normas internas, passível de aplicação de:

- **Falta Leve:** será considerada “Falta” a violação de qualquer item desta política e das demais normas internas que regem a PARABANK e demais empresas do grupo que, a critério do Diretor de Risco,

Compliance e PLD, embora tenha ocorrido, não trouxe qualquer prejuízo financeiro, operacional ou à imagem das empresas do grupo.

Penalidade: advertência verbal e anotação no prontuário do Colaborador, mantido para os devidos efeitos de arquivamento ("Prontuário").

- **Falta Grave:** será considerada "Falta Grave" a violação de qualquer item desta política e das demais normas internas, que tenha trazido pequenos prejuízos financeiros, operacionais ou à imagem das empresas do grupo, à critério do Diretor de Risco, Compliance e PLD, ou ainda, se houver reincidência de alguma Falta Leve cometida anteriormente, **por no mínimo 3 (três) vezes em um intervalo de 2 (dois) anos**.

  Penalidade: advertência formal, anotação no Prontuário do Colaborador e aplicação de suspensão das atividades pelo período de até 3 (três) dias úteis, formalizada pelo Departamento de Recursos Humanos.

- **Falta Gravíssima:** será considerada "Falta Gravíssima" a violação de qualquer artigo desta política e das demais normas internas, que apresente prejuízos financeiros, operacionais ou à imagem das empresas do grupo, à critério do Diretor de Risco, Compliance e PLD, ou ainda, se houver reincidência de alguma Falta Grave cometida anteriormente, **por no mínimo 3 (três) vezes em um intervalo de 2 (dois) anos.**

  Penalidade: afastamento definitivo das atividades exercidas perante a empresa (Desligamento).

A aplicação das penalidades acima não isenta, dispensa ou atenua a responsabilidade civil, administrativa e criminal, pelos prejuízos resultantes de seus atos dolosos ou culposos resultantes da infração da legislação em vigor e das políticas e procedimentos estabelecidos neste documento.

7. REFERÊNCIAS

Tipo de documento	Nome do documento
Lei	LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. LEI COMPLEMENTAR Nº. 105, DE 10 DE JANEIRO DE 2001 LEI Nº. 9.613, DE 3 DE MARÇO DE 1998 LEI N. 12.683, DE 9 DE JULHO DE 2012. LEI N. 13.964 DE 24 DE DEZEMBRO DE 2019.
Norma / Regulamento	CIRCULAR BACEN Nº 3.865, DE 7 DE DEZEMBRO DE 2017. CIRCULAR BACEN Nº 3.461, DE 24 DE JULHO DE 2019. CIRCULAR BACEN N. 3.978 DE 23 DE JANEIRO DE 2020.

8. HISTÓRICO

Versão	Descrição da atualização	Data da versão
1.0	Primeira publicação.	01/04/2020