POLÍTICA DE PROTEÇÃO DE DADOS

BASE

O Banco RCI Brasil S.A. e as Empresas do Grupo reservam-se no direito de alterar esta Política de Privacidade e Proteção de Dados a qualquer momento, sem aviso. Como esses termos e condições são atualizados regularmente, sugerimos que você consulte esta página ou Política no App sempre que tiver necessidade..

BASE

O Banco RCI Brasil S.A., doravante denominado neste instrumento como "Mobilize Financial Services", juntamente com as "Empresas do Grupo", está comprometido em manter a privacidade dos dados pessoais obtidos no curso de suas atividades empresariais e cumprir as leis e regulamentos aplicáveis sobre o tratamento de dados pessoais ("Dados Pessoais"), incluindo dados sensíveis ("Dados Sensíveis"). Isso inclui, mas não está limitado à Lei Geral de Proteção de Dados, cuja entrada em vigor se deu em setembro de 2020.

A Mobilize Financial Services e as Empresas do Grupo decidiram adotar uma Política de Privacidade e Proteção de Dados para definir técnicas e medidas organizacionais adequadas contra o tratamento não autorizado e ilegal de Dados Pessoais e contra perda ou destruição acidental ou danos aos Dados Pessoais, para assegurar que os Dados Pessoais, incluindo Dados Sensíveis, sejam devidamente protegidos.

Para maiores informações sobre a Política ou sobre como tratamos os seus dados pessoais, você pode entrar em contato com o Encarregado de Dados/DPO.

DEFINIÇÕES

Os termos e expressões a seguir, quando escritos em letras maiúsculas, deverão ter os seguintes significados, conforme definido abaixo:

"Autoridade Nacional de Proteção de Dados" ou "ANPD" significa a autoridade administrativa encarregada da Proteção de Dados Pessoais, que é um órgão da administração pública nacional responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro.

"Comitê de Privacidade e Proteção de Dados" é um comitê especificamente dedicado a lidar com Proteção de Dados, composto por representantes das Empresas do Grupo RCI Brasil e do Encarregado de Proteção de Dados.

"Colaboradores da Mobilize Financial Services" são todos os funcionários das Empresas do Grupo, incluindo diretores, estagiários, aprendizes e qualquer outra pessoa que possua vínculo direto com as empresas do Grupo.

"Controlador de Dados" significa uma pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais.

"Dados Pessoais" significam quaisquer dados relacionados a um indivíduo (pessoa natural) que é ou possa ser identificado a partir dos dados ou a partir dos dados em conjunto com outras informações.

"Dados Sensíveis" significa os dados pessoais 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, ou outros dados específicos considerados sensíveis mediante as leis e regulamentos próprios.

"Empresas do Grupo" significa: (i) Banco RCI Brasil S.A., pessoa jurídica de direito privado com CNPJ/MF 62.307.848/0001-15, com sede na Rua Pasteur, nº 463, 1º Andar, Conjunto 203,

Bairro Batel, Curitiba/PR, CEP 80.250-080; (ii) Administradora de Consórcio RCI Brasil Ltda, pessoa jurídica de direito privado com CNPJ/MF 73.230.674/0001-56, com sede na Alameda Europa, n° 150, Bairro Alphaville, Santana de Parnaíba/SP, CEP: 06541-065; (iii) Corretora de Seguros RCI Brasil S.A., pessoa jurídica de direito privado com CNPJ/MF 04.406.267/0001-34, com sede na Rua Pasteur, nº 463, 1º Andar, Conjunto 203, Bairro Batel, Curitiba/PR, CEP 80.250-080; e (iv) RCI Brasil Serviços e Participações Ltda, pessoa jurídica de direito privado com CNPJ/MF 13.758.102/0001-12 com sede na Rua Pasteur, nº 463, 1º Andar, Conjunto 203, Bairro Batel, Curitiba/PR, CEP 80.250-080.

“Encarregado de Dados” ou “DPO” significa a pessoa que nas Empresas do Grupo é o responsável por coordenar e por assegurar a conformidade com a Política de Privacidade e Proteção de Dados e requisitos legais/regulamentares locais aplicáveis, também, atuará como o canal com os titulares dos dados e a Autoridade Nacional de Proteção de Dados. Informações a seguir.

“LGPD” significa Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709 de 14 de agosto de 2018.

“Open Banking” ou “Sistema Financeiro Aberto” significa o compartilhamento padronizado de dados bancários pessoais e serviços por meio de abertura e integração de sistemas entre clientes e instituições financeiras, de pagamento e demais autorizadas pelo Banco Central do Brasil (BCB), implementada pela Resolução Conjunta nº 1 de 2020 (“Resolução”), entre o BCB e o Conselho Monetário Nacional (CNM).

“Operador de Dados” significa uma pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador de Dados.

“Titular dos Dados” significa qualquer pessoa natural a quem se referem os dados pessoais que são objeto de tratamento ou a pessoa jurídica a quem se referem os dados, inclusive financeiros e transacionais, objeto do tratamento.

“Tratamento” é qualquer ação tomada tendo por base dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, tratamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

OBJETIVO

O objetivo da Política de Privacidade e Proteção de Dados é definir as principais regras em relação à proteção de dados que são aplicáveis nas Empresas do Grupo para garantir um nível adequado de proteção aos Dados Pessoais tratados.

O objetivo é ajudar cada uma das Empresas do Grupo e suas respectivas áreas internas a estabelecer programas de proteção de dados e cumprir à Lei Geral de Proteção de Dados e toda e qualquer legislação, incluindo regulamentações das autoridades competentes, que direta ou indiretamente estabeleça regras sobre o tema.

ESCOPO

1. Abrangência geográfica

A presente Política de Privacidade e Proteção de Dados aplica-se ao Tratamento de Dados Pessoais coletados e tratados no Brasil, independentemente se o tratamento ocorrer no Brasil ou Exterior.

2. Escopo temporal

Há vários componentes para calcular os períodos de guarda e conservação dos dados, os quais poderão ser alterados de acordo com o tipo e natureza dos dados. Os dados poderão ser conservados pelo período necessário para:

- processar sua inscrição, solicitação, contratação ou reclamação;
- conservar um histórico de sua interação conosco, para o gerenciamento adequado de nosso relacionamento (comercial, gestão de produtos e clientes, atendimento adequado aos clientes);
- Cumprimento de obrigações legais, regulatórias ou contratuais;
- Demais finalidades previstas nesta Política de Privacidade.

Também podemos conservar alguns dos seus dados pessoais em nossos arquivos, para que possamos responder a qualquer processo administrativo, judicial ou arbitral. Isso se aplica durante todo o período de decadência e prescrição especificado na legislação aplicável.

3. Escopo material

a. Escopo das Empresas do Grupo:

A Presente Política de Privacidade e Proteção de Dados aplica-se a todas as atividades de tratamento das Empresas do Grupo, incluindo, mas não limitadas a:

1. oferecimento de produtos ou serviços aos Titulares dos Dados em território nacional;
2. monitoramento do comportamento dos Titulares dos Dados dentro dos limites em que seu comportamento ocorre no território nacional; ou
3. compartilhamento com outras instituições financeiras, conforme expressa solicitação pelos Titulares dos Dados em observância às disposições legais e regulamentares sobre o Open Banking.

b. Escopo dos Dados Pessoais:

Todos os tipos e categorias de Dados Pessoais tratados pelas Empresas do Grupo no curso de suas atividades devem estar contemplados no escopo desta Política de Privacidade e Proteção de Dados. Esses tipos e categorias devem incluir: Dados Pessoais coletados de clientes, clientes prospectados, reclamantes, funcionários das empresas do Grupo, candidatos a empregos, parceiros comerciais, fornecedores e outros terceiros. Incluem:

- Nome
- Nome Social
- Data de nascimento
- Sobrenome
- CPF
- CNPJ
- Carteira de identidade
- Carteira Nacional de habilitação (CNH)
- Carteira de Trabalho e Previdência Social (CTPS)
- Cédula de identidade de estrangeiro (CIE)
- Registro Nacional de Estrangeiros (RNE)
- Protocolo de solicitação da CIE
- Protocolo do pedido de refúgio de que trata o art. 21 da Lei nº 9.474 de 22 de julho de 1997
- Passaporte
- Guia de acolhimento de que trata o § 3 do artº 101 da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da criança e do Adolescente)
- Idade
- Nacionalidade
- E-mail
- Naturalidade
- Nome da mãe

- Nome do pai
- Endereço Residencial
- Endereço Comercial
- Estado Civil
- Sexo
- Telefones residencial
- Telefones comercial
- Telefones celular
- Condição Pessoal (espólio, interdito, deficiente, etc...)
- Renda
- Patrimônio
- IMEI do celular
- Origem racial
- Geolocalização
- Foto
- Filmagens
- Biometria
- Áudio/voz
- Pessoa Politicamente exposta
- Título de eleitor
- Documentos profissionais (CREA, OAB e etc.)
- PIS/NIS - Programa de integração social
- Profissão
- Formação Acadêmica
- IP
- Cookies
- Dados Transacionais de Contas
- Dados Transacionais de Cartão
- Dados Transacionais de Operação de Crédito

Os Dados Pessoais podem ser obtidos:

1. diretamente do titular quando da contratação dos produtos e serviços desta instituição financeira ou em simulações em fase de proposta; ou
2. de fontes externas legítimas, com devido embasamento legal ou contratual; ou
3. em razão de eventual compartilhamento de dados entre as empresas do Grupo RCI Brasil, sua matriz e subsidiárias, montadoras, concessionárias e empresas do Conglomerado Santander, sem prejuízo do disposto na Lei e das hipóteses em que o consentimento for necessário; ou
4. de outras Instituições Financeiras, por decorrência de requerimento pelo Open Banking.

A Política de Privacidade e Proteção de Dados cobre tanto os tipos de Tratamento automatizados como manuais.

4. Finalidades

Nos termos da Lei Geral de Proteção de Dados, as empresas do Grupo realizam o tratamento de seus dados pessoais com finalidades específicas e de acordo com as bases legais previstas na respectiva Lei, tais como para:

1. o devido cumprimento das obrigações legais, regulatórias e decisões de autoridades, sejam adminisitrativas ou judiciais;
2. o exercício regular de direitos, inclusive de defesa em processo judicial, administrativo ou arbitral;
3. a realização de auditorias;

4. a proteção do crédito;
5. a análise de perfil para concessão de crédito ou gestão de riscos;
6. a execução dos contratos firmados com seus clientes ou execução de ações em virtude de relações pré-contratuais, durante a vigência da contratação ou pós-contratação;
7. atender aos interesses legítimos das empresas do Grupo, de seus clientes ou de terceiros;
8. garantir maior segurança e prevenir fraudes;
9. assegurar sua adequada identificação, qualificação e autenticação, conferindo maior segurança durante a navegação;
10. manutenção e atualização cadastral;
11. prevenir atos relacionados à lavagem de dinheiro e outros atos ilícitos; realizar análises de risco de crédito;
12. aperfeiçoar o atendimento e os produtos e serviços prestados, inclusive para tratamento de reclamações, dúvidas e solicitações, bem como suporte ao titular, pesquisa de satisfação de produtos e serviços e pesquisas de comunicação e marketing de relacionamento;
13. fazer ofertas de produtos e serviços adequados e relevantes aos seus interesses e necessidades de acordo com o seu perfil, inclusive mediante campanhas de marketing ou de simulações;
14. outras hipóteses baseadas em finalidades legítimas, como apoio e promoção de atividades das empresas do Grupo, ou para a prestação de serviços que beneficiem os clientes;
15. analisar dados para aperfeiçoar a usabilidade, experiência e interatividade na utilização dos nossos portais, sites e aplicativos;
16. utilizar cookies, conforme a Política de Cookies
17. no cenário de Open Banking, com seu consentimento, o compartilhamento de seus dados com outras Instituições Financeiras.

Uma vez provido das informações pessoais a respeito do usuário, as empresas do Grupo poderão utilizar, de acordo com o seu interesse legítimo, os dados do usuário para o fim de enviar publicidade, direcionada por e-mail ou por quaisquer outros meios de comunicação e compartilhar com as demais empresas do Grupo, sua matriz e subsidiárias, montadoras ou concessionárias Renault e Nissan, empresas do Conglomerado Santander, para oferta de produtos e serviços de seu interesse. Entretanto, fica reservado ao usuário o direito de, a qualquer momento, inclusive no ato da disponibilização das informações pessoais, informar ao Grupo, por meio dos canais de comunicação disponíveis para o cadastramento de tais informações, do não interesse em receber tais anúncios, inclusive por e-mail (opt-out), hipótese em que o Grupo interromperá tais serviços no menor tempo possível. Para cancelar sua inscrição, consulte as instruções de opt-out presentes no rodapé dos nossos e-mails.

Para qualquer outra finalidade, para a qual o consentimento do titular deve ser coletado, o tratamento estará condicionado à manifestação livre, informada e inequívoca do titular.

As informações de caráter pessoal dos usuários dos Serviços das Empresas do Grupo, entendendo-se por informações pessoais todas aquelas que forem relacionadas a pessoa natural identificada ou identificável, inclusive informações pessoais sensíveis (que tratem 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), como: o nome completo do usuário, endereço físico e eletrônico, número de telefone, RG, CPF, biometria, número de cartão de crédito, situação financeira e patrimonial, preferências e padrões de acesso ("informações pessoais") e CNPJ ao tratarmos de pessoa jurídica não são divulgadas exceto nas hipóteses expressamente mencionadas nesta Política.

Tais informações são coletadas por meio dos canais de atendimento e armazenadas utilizando-se rígidos padrões de sigilo e integridade, bem como controles de acesso físico e lógico, observando-se sempre os mais elevados princípios éticos e legais.

PRINCÍPIOS PARA O TRATAMENTO DE DADOS

Princípios Gerais

O Tratamento de Dados Pessoais executado sob o controle das Empresas do Grupo será feito de acordo com as leis aplicáveis e com as disposições desta Política de Privacidade e Proteção de Dados e em particular com as seguintes regras mínimas:

- Quando estabelecido pela Lei Geral de Proteção de Dados, um relatório de impacto à proteção de dados pessoais ("RIPD") deve ser conduzido pelas Empresas do Grupo, incorporando os princípios estabelecidos no art. 6º da Lei Geral de Proteção de Dados Pessoais.
- Os Dados Pessoais devem ser obtidos de forma justa e legal. Se necessário, o consentimento expresso do Titular dos Dados deverá ser obtido. O Titular dos Dados tem o direito à informação sobre os dados tratados, exceto se essas informações não forem necessárias considerando as hipóteses estabelecidas para o seu tratamento. Os Dados Pessoais devem ser coletados apenas para propósitos especificados, explícitos e legítimos e não podem ser tratados de forma incompatível com esses propósitos.
- Os Dados Pessoais apenas serão disponibilizados a terceiros para os ditos propósitos ou de qualquer outra forma permitida pelas leis aplicáveis, incluindo, mas não se limitando às Instituições Financeiras, com expresso consentimento do Titular dos Dados, para os propósitos do Open Banking.
- Os controles e procedimentos técnicos e organizacionais apropriados devem ser implementados para garantir a segurança dos Dados Pessoais e evitar acesso ou divulgação não autorizados, que potencialmente poderiam resultar em alteração, destruição acidental ou ilegal, perda dos dados e contra todas as demais formas ilegais de Tratamento. Considerando as obrigações legais, boas práticas, as medidas de segurança devem ser elaboradas para garantir um nível de segurança apropriado aos riscos representados pelo Tratamento e natureza dos Dados Pessoais a serem protegidos.
- Os Dados Pessoais coletados devem ser adequados, relevantes e não excessivos em relação aos propósitos para os quais são coletados e/ou serão processados.
- Os Dados Pessoais não podem ser retidos por um período maior que o necessário para os objetivos para os quais foram obtidos, a menos que exigido de outra forma pelas leis ou regulamentos aplicáveis ou quando houver consentimento específico indicando um determinado período.
- Devem ser implementados procedimentos para garantir respostas imediatas às indagações dos Titulares dos Dados, assegurando o adequado exercício do direito de acesso, retificação e recusa ao Tratamento (exceto quando a Lei Geral de Proteção de Dados Pessoais autorizar de outra forma).

Os Dados Pessoais apenas devem ser processados se esse Tratamento for baseado em bases legítimas, incluindo, por exemplo, se:

- O Titular dos Dados deu consentimento inequívoco; ou
- O Tratamento é necessário para o desempenho de um contrato no qual o Titular dos Dados é parte ou para executar etapas mediante a solicitação do Titular dos Dados antes de celebrar um contrato; ou
- O Tratamento é necessário para conformidade com uma obrigação legal com a qual o Controlador dos Dados está sujeito; ou
- O Tratamento é necessário para proteger os interesses vitais do Titular dos Dados; ou

- O Tratamento é necessário para o desempenho de uma tarefa executada no interesse público ou no exercício de uma autoridade oficial investida no Controlador dos Dados ou em um terceiro para o qual os Dados Pessoais foram divulgados; ou
- O Tratamento é necessário para objetivos de interesses legítimos almejados pelo Controlador dos Dados ou por Terceiro ou Partes para as quais os Dados Pessoais foram divulgados, exceto quando esses interesses são sobrepostos pelos interesses dos direitos e liberdades fundamentais do Titular dos Dados; ou
- O Tratamento é necessário para cumprimento da vontade do Titular de Dados Pessoais no compartilhamento de informações com outras Instituições Financeiras, de acordo com as disposições do Open Banking e demais parâmetros legais e regulamentares estabelecidos para esta finalidade, assegurado o direito do Titular de dados de cancelamento da autorização a qualquer momento.

Dados Sensíveis

O Tratamento de Dados Sensíveis somente poderá ocorrer nas seguintes hipóteses:

1. Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
2. O Tratamento é necessário para os objetivos de executar as obrigações e direitos específicos do Controlador dos Dados no campo da legislação trabalhista dentro da extensão da legislação aplicável para as proteções adequadas;
3. O Tratamento é necessário para proteger a vida ou da incolumidade física do titular ou de terceiros;
4. O Tratamento é realizado no exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
5. O Tratamento é realizado para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
6. O Tratamento relaciona-se com Dados Sensíveis que foram tornados públicos pelo Titular dos Dados; ou
7. O Tratamento é permitido de outra forma mediante lei própria.

Obrigações de Sigilo Bancário

Para as atividades específicas e previstas pela Lei Complementar 105/2001 devem ser observados o sigilo bancário das operações. Embora tecnicamente essas obrigações possam não estar formalmente descritas nas hipóteses da Lei Geral de Proteção de Dados, dependendo da característica dos dados e do seu tratamento e com o objetivo de adotar um procedimento adequado para proteção de dados, eventualmente, entidades não bancárias das Empresas do Grupo poderão adotar medidas mais conservadoras na realização do tratamento dos dados pessoais.

Subcontratação de operadores

Nos casos nos quais o Tratamento for realizado por um operador em nome das empresas do Grupo, esta empresa deverá escolher um subcontratado que tenha condições técnicas de segurança e organizacionais suficientes para garantir que o Tratamento será Executado de acordo com esta Política de Privacidade e Proteção de Dados e as empresas do Grupo devem garantir que os subcontratados concordem por escrito e cumpram essas medidas. Deverá ser assinado um contrato que estipule em particular que o subcontratado atuará apenas conforme as instruções das Empresas do Grupo.

Transferências de Dados para fora do Brasil

As Empresas do Grupo devem garantir que transferências de Dados Pessoais para fora do território nacional observem o estabelecido na Lei Geral de Proteção de Dados Pessoais:

- Transferindo os dados para países ou organismos internacionais que proporcionem grau de proteção de dados adequados conforme previsto na legislação brasileira;
- Comprovando que o operador internacional ofereça garantias do cumprimento dos princípios e direitos dos titulares na forma prevista na lei.

Responsabilização e Prestação de Contas

Todas as Empresas do Grupo devem ser capazes de demonstrar as medidas tomadas para garantir a conformidade com a LGPD, bem como demonstrar a eficácia destas medidas.

DIREITOS DOS INDIVÍDUOS EM RELAÇÃO AOS DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais define que os indivíduos devem receber informações sobre o Tratamento dos Dados Pessoais no momento da coleta dos dados, embora possa haver exceções a esta regra. O tipo exato de informações a serem fornecidas variará dependendo da operação, contrato ou serviço, mas geralmente inclui, no mínimo:

- Nome do Controlador dos Dados, que será uma das empresas do Grupo I, já qualificadas nesta política;
- Tipos de dados coletados;
- Objetivos da coleta e tratamento dos Dados Pessoais;
- Destinatários dos Dados Pessoais;
- Informações sobre os direitos de acesso, correção, atualização, retirada de consentimento ou exclusão dos Dados Pessoais dos Titulares dos Dados, e como exercer esses direitos.

Estas informações poderão ser encontradas, nos termos de uso de site ou aplicativos das Empresas do Grupo, contratos firmados com os consumidores e outras informações disponíveis nos canais oficiais de cada uma das Empresas do Grupo.

No que diz respeito a LGPD, o Consentimento será necessário para realização de alguns tratamentos específicos, como compartilhamento com outras Instituições Financeiras no Open Banking, caso não exista outra base legal para utilização dos dados coletados.

No caso de um Tratamento de Dados Pessoais, os Titulares dos Dados possuem os seguintes direitos dentre outros previstos na legislação brasileira:

- Confirmação da Existência de Tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses de guarda legal previstas na Lei;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, incluindo, mas não se limitando à Instituições Bancárias, cujo compartilhamento decorreu do Open Banking;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento, nos termos da LGPD.

As Empresas do Grupo empreenderão todos os esforços para atender tais pedidos no menor espaço de tempo possível. No entanto, mesmo em caso de requisição de exclusão, será respeitado o prazo de armazenamento mínimo de informações de usuários, determinado pela legislação brasileira, dentre outras determinações legais aplicáveis.

As Empresas do Grupo são individualmente autorizadas a acessar seus dados, bem como a compartilhá-los entre as Empresas do Grupo, com a sua Matriz e subsidiárias, com as Montadoras e Concessionárias Renault e Nissan, bem como com as empresas do conglomerado Santander, com o objetivo de lhe oportunizar ofertas exclusivas e em caso de necessidade responder as suas solicitações.

Dentro do possível, os seus dados pessoais serão hospedados em servidores localizados no Brasil e eventualmente na Área Econômica Europeia.

Quanto ao Open Banking, é também direito do Titular de Dados consultar os Dados Pessoais recebidos de outras Instituições Financeiras. Porém, em caso de dúvidas, o seu contato deve ocorrer diretamente com a Instituição Financeira de origem dos Dados, a quem poderá solicitar, a qualquer momento, o cancelamento desta autorização.

AÇÕES PARA IMPLEMENTAÇÃO

Programa de treinamento

As Empresas do Grupo responsabilizam-se em implementar programas de treinamento sobre proteção de Dados Pessoais aos Funcionários da Mobilize envolvidos no Tratamento de Dados Pessoais em relação aos princípios contidos nesta Política de Privacidade e Proteção de Dados Pessoais.

Os princípios gerais para treinamento e aumento de conscientização serão elaborados de forma conjunta e quando possível serão compartilhados exemplos práticos através de sessões de conscientização (e-learning, presencial etc) que serão realizadas por cada Empresa do Grupo em linha com as leis e processos aplicáveis.

Cada Empresa do Grupo deve definir como executar o controle do nível de treinamentos concluídos com êxito. Além disso, cada Empresa do Grupo determinará a periodicidade das atualizações do treinamento, o treinamento sobre proteção de Dados Pessoais de Funcionários da Mobilize recém contratados como parte da sessão de indução ao unirem-se à Empresa do RCI, bem como um treinamento anual especialmente dirigidos aos Funcionários do RCI que são mais intimamente envolvidos com aspectos críticos dos Dados Pessoais.

As Empresas do Grupo podem considerar incluir o seguinte no programa de treinamento: (i) Sumários dos principais conceitos, (ii) Apresentação dos critérios para o tratamento com base na LGPD; (iii) Síntese das bases legais para o tratamento de Dados Pessoais; (iv) Ilustrações da aplicação dos princípios na prática, (v) Uma visão geral das políticas e procedimentos relevantes das Empresas do Grupo, ou (vi) Um estudo de caso interativo que exige que os funcionários lidem com um problema de proteção de dados, como uma solicitação do Titular dos Dados para acessar todos os Dados Pessoais relacionados a ele. Em todos os casos, o foco do treinamento deve ser nos requisitos previstos na LGPD.

Governança

O Grupo Globalmente possui uma Organização/Governança de Privacidade de Dados com (i) um modelo de governança de Privacidade de Dados aprovado pelo Comitê de Gerenciamento, (ii) um Administrador de Proteção de Dados do Grupo, (iii) um Comitê de Direção de Privacidade de Dados do Grupo, (iv) uma rede de Correspondentes de Proteção de Dados coordenada pelo Administrador de Proteção de Dados do Grupo.

O DPO Global determina a estratégia de proteção e privacidade de Dados Pessoais do Grupo RCI de acordo com os objetivos estratégicos e garante que as Empresas do Grupo façam a adesão às disposições aplicáveis dos regulamentos de proteção de dados e privacidade.

Localmente um Comitê de Privacidade deverá ser constituído por representantes das Empresas do Grupo RCI Brasil e o Encarregado de Dados localmente será responsável, em conjunto com todas as áreas das respectivas empresas, pela implementação das diretrizes e obrigações fixadas na LGPD.

Controle

Considerando potenciais consequências graves decorrentes da violação da Lei Geral de Proteção de Dados Pessoais, as Empresas do Grupo RCI Brasil devem implementar programas de conformidade e controles relacionados que sejam elaborados de forma cabível para prevenir, detectar, monitorar e abordar violações em potencial.

REGISTRO DE RECLAMAÇÕES

As empresas do Grupo devem ter um processo interno, centralizado ou não, para registros de reclamações sobre o tratamento dos dados pessoais. No caso de uma reclamação, os Titulares dos Dados, considerando a realização de um Tratamento ilegal ou inapropriado de seus Dados Pessoais que seja incompatível com a Política de Privacidade e Proteção de Dados, poderá peticionar para:

- O Encarregado de Dados Pessoais das Empresas do Grupo ; e/ou
- A Autoridade Nacional de Proteção de Dados.

Todas as empresas do Grupo RCI devem ter em seus sites da internet ferramentas práticas que permitam aos Titulares dos Dados registrarem reclamações, incluindo pelo menos uma das abaixo:

- Link da internet para um formulário de reclamação;
- Endereço de e-mail;
- Telefone;
- Endereço postal.

A menos que fique comprovado ser particularmente difícil encontrar as informações necessárias para conduzir a investigação, as reclamações devem ser investigadas da maneira mais rápida possível, com a conclusão em no máximo até 1 (um) mês e dando visibilidade dos próximos passos em até 05 (cinco) dias úteis ao titular dos dados pessoais.

ASSISTÊNCIA MÚTUA E COOPERAÇÃO COM A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

As Empresas do Grupo cooperarão com a Autoridade Nacional de Proteção de Dados (ANPD) em qualquer problema em relação à Proteção de Dados, dentro dos limites previstos na LGPD e sem renunciar a quaisquer defesas e/ou direitos de recurso disponíveis ao Controlador de Dados:

- Disponibilizando o pessoal necessário para o diálogo com a ANPD;
- Revisando de forma proativa, procedimentos internos considerando quaisquer diretrizes estabelecidas pela ANPD;
- Respondendo as solicitações por informações ou reclamações;
- Aplicando as recomendações relevantes ou diretrizes estabelecidas.

As Empresas do Grupo acordam em observar uma decisão da ANPD, dentro dos limites estabelecidos na LGPD e regulamentos aplicáveis, sem renunciar a quaisquer defesas e/ou direitos de recurso disponíveis ao Controlador de Dados.

Se a ANPD solicitar informações ou de qualquer outra forma exercer seu direito de investigação, o Encarregado de Dados deve ser informado sem demora por qualquer representante das

Empresas do Grupo RCI Brasil. Então o Encarregado de Dados / DPO deve atuar como o coordenador primário para formular uma resposta apropriada à indagação, tendo como suporte os colaboradores e/ou prestadores de serviços potencialmente envolvidos, bem como, os administradores e/ou responsáveis. Além disso, o DPO atuará como o contato direto e primário em relação a ANPD.

OPEN BANKING

O Open Banking destina-se à melhor experiência no uso de produtos e serviços financeiros, mais adequados e personalizados, através de plataforma segura de comunicação entre as Instituições Financeiras, incluindo a Mobilize Financial Services..

O compartilhamento de informações apenas se dará a partir do consentimento do Titular dos Dados, através de manifestação prévia e inequívoca, feita por meio eletrônico, após a solicitação por meio da Instituição receptora de dados, isto é, a Instituição Bancária de destino que irá receber os dados. A solicitação de compartilhamento de dados compreenderá as etapas de consentimento, autenticação e confirmação. Assim, é o Titular de Dados quem decidirá quando e com quem deseja compartilhar seus Dados Pessoais.

Com este consentimento, poderão ser compartilhadas informações como, mas não se limitando a:

- Dados transacionais de contas;
- Dados transacionais de cartão;
- Dados transacionais de operação de crédito;
- Seguros;
- Produtos com natureza de investimento;
- Cadastro próprio e de seus representantes.

Em atenção ao art. 10 da Resolução Conjunta nº 1 de 2020 do BCB e CNM, o compartilhamento terá prazo de validade compatível com as finalidades desse tratamento, tendo como limite o prazo de 12 meses. Além disso, o Titular dos Dados poderá solicitar, a qualquer momento, o cancelamento do consentimento fornecido.

É também direito do Titular de Dados consultar os Dados Pessoais recebidos de outras Instituições Financeiras. Porém, em caso de dúvidas, o seu contato deve ocorrer diretamente com a Instituição Financeira de origem dos Dados Pessoais.

ATUALIZAÇÃO DA POLÍTICA

Sempre que as empresas do Grupo entenderem necessário, a Política de Privacidade e Proteção de dados poderá sofrer alterações que serão publicadas em nossos Sites e Aplicativos ou serem comunicadas de qualquer outra forma a você, sem aviso prévio.

O Encarregado de Dados/DPO deve assegurar revisões e atualizações regulares da Política de Privacidade e Proteção de Dados, por exemplo, como consequência de alterações maiores na estrutura corporativa e no ambiente regulatório.

Neste sentido, o Encarregado de Dados/DPO deve auxiliar a definir e atualizar as medidas técnicas e organizacionais a serem implementadas ao coletar, tratar e/ou usar Dados Pessoais em conformidade com os requisitos legais. Tais medidas organizacionais e/ou técnicas podem apenas entrar em vigor após o Encarregado de Dados revisar e aprovar sua compatibilidade com esta Política de Privacidade e Proteção de Dados.

IMPLEMENTAÇÃO - NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS - REVISÃO – RELATÓRIO

<u>Implementação</u>

Cada Empresa do Grupo é a única responsável por assegurar que tenha um programa apropriado e efetivo de proteção de dados. Para facilitar a operação adequada desses programas, o DPO supervisionará a implementação e operação em andamento dos programas de conformidade de proteção de dados das Empresas do Grupo. O programa de conformidade de proteção de dados estará sujeito a auditorias internas periódicas que testarão a eficácia dos programas de conformidade de proteção de dados.

Notificação de violação de Dados Pessoais

Quando os Dados Pessoais dos Titulares dos Dados estiverem comprometidos, os responsáveis pelas Empresas do Grupo deverão notificar o DPO/Encarregado de Dados imediatamente. Então a Empresa do Grupo envolvida, juntamente com o Encarregado de Dados, deve notificar a Autoridade Nacional de Proteção de Dados sem demora e em um prazo razoável contado da ciência do incidente de segurança.

A Comunicação deverá mencionar no mínimo a descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, os motivos da demora, no caso da comunicação não ter sido realizada imediatamente, e as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial ou eventualmente o sigilo bancário.

Relatório

É esperado que as Empresas do Grupo relatem as informações relacionadas com violações de segurança de dados, qualquer auditoria ou exame da Autoridade Nacional de Proteção de Dados ao Encarregado de Dados/DPO Global do Grupo.

RESPONSÁVEL PELO CONTROLE OU OPERACIONALIZAÇÃO DE DADOS PESSOAIS NO GRUPO RCI BRASIL

Os dados pessoais fornecidos para Empresas do Grupo, a depender do produto e/ou serviço ofertado podem ter uma das empresas abaixo como Controlador ou Operador. Geralmente teremos as empresas listadas a seguir como Controladores de Dados: i) Banco RCI Brasil S.A., pessoa jurídica de direito privado com CNPJ/MF 62.307.848/0001-15, com sede na Rua Pasteur, nº 463, 1º Andar, Conjunto 203, Bairro Batel, Curitiba/PR, CEP 80.250-080; (ii) Administradora de Consórcio RCI Brasil Ltda, pessoa jurídica de direito privado com CNPJ/MF 73.230.674/0001-56, com sede na Alameda Europa, n° 150, Bairro Alphaville, Santana de Parnaíba/SP, CEP: 06541-065; (iii) RCI Brasil Serviços e Participações Ltda, pessoa jurídica de direito privado com CNPJ/MF 13.758.102/0001-12 com sede na Rua Pasteur, nº 463, 1º Andar, Conjunto 203, Bairro Batel, Curitiba/PR, CEP 80.250-080; e como Operador de Dados Pessoais a Corretora de Seguros RCI Brasil S.A., pessoa jurídica de direito privado com CNPJ/MF 04.406.267/0001-34, com sede na Rua Pasteur, nº 463, 1º Andar, Conjunto 203, Bairro Batel, Curitiba/PR, CEP 80.250-080.

O Encarregado de Dados/DPO, Maick Dias, pode ser contatado através do endereço Rua Pasteur, nº 463, 1º Andar, Conjunto 203, Bairro Batel, Curitiba/PR, CEP 80.250-080 e endereço de e-mail: atendimento-clientes@rcibanque.com.

LEI APLICÁVEL E RESOLUÇÃO DE CONFLITOS

Toda e qualquer controvérsia oriunda dos termos expostos na presente Política de Privacidade serão solucionados de acordo com a lei brasileira, sendo competente o foro da cidade de Curitiba, Estado do Paraná, com exclusão de qualquer outro por mais privilegiado que seja.

DISPOSIÇÕES GERAIS

Eventuais omissões ou meras tolerâncias das partes no exigir o estrito e pleno cumprimento desta Política de Privacidade e/ou de prerrogativas decorrentes dele ou da lei, não constituirão

novação ou renúncia, nem afetarão o exercício de quaisquer direitos aqui previstos, que poderão ser plena e integralmente exercidos, a qualquer tempo.

Caso se perceba que uma disposição é nula, as disposições restantes desta Política de Privacidade permanecerão em pleno vigor e um termo válido substituirá o termo nulo, refletindo nossa intenção, tanto quanto possível.

SISTEMA DE INFORMAÇÃO DE CRÉDITO (SCR)

SOBRE

O Sistema de Informações de Crédito (SCR) é um banco de dados que contém informações sobre as operações de crédito contratadas por pessoas físicas e jurídicas perante as instituições financeiras e que por estas são remetidas ao Banco Central do Brasil (BACEN), na condição de administrador do SCR.

O SCR tem por finalidades, (a) prover informações ao BACEN, para fins de monitoramento do crédito no sistema financeiro e para o exercício de suas atividades de fiscalização; e (b) propiciar o intercâmbio de informações entre as instituições financeiras sobre o montante de responsabilidades de clientes em operações de crédito, com o objetivo de subsidiar decisões de crédito e de negócios, conforme a política de crédito das instituições.

Os dados sobre o montante das dívidas do cliente a vencer e vencidas, inclusive em atraso e baixadas com prejuízo, bem como o valor das coobrigações que ele tenha assumido e das garantias que tenha prestado são fornecidos ao BACEN e registrados no SCR, sendo de responsabilidade exclusiva da instituição remetente a inserção de informações que digam respeito ao cliente.

Eventuais solicitações de correções, exclusões, manifestações de discordância e registro de medidas judiciais quanto às informações constantes do SCR deverão ser dirigidas aos canais de atendimento do RCI Brasil, por meio de requerimento escrito e fundamentado e, quando for o caso, acompanhado da decisão judicial.

A consulta sobre qualquer informação constante do SCR dependerá da prévia autorização do cliente/proponente, que se estende às instituições que, nos termos da regulamentação vigente, podem realizar consultas ao SCR e que adquiram ou recebam em garantia, ou manifestem interesse de adquirir ou de receber em garantia, total ou parcialmente, operações de crédito de responsabilidade do cliente.

O cliente/proponente poderá obter esclarecimentos adicionais ou consultar, a qualquer tempo, os dados em seu nome no SCR pelos meios disponibilizados pelo Banco Central, em uma de suas unidades, na central de atendimento ao público (0800 979 2345) ou por meio de acesso ao Registrato do BACEN (www.bcb.gov.br).

Os extratos com os dados são elaborados de acordo com critérios contábeis e metodologia específica estabelecidos pelo BACEN e se referem ao saldo existente no último dia do mês de referência.