MANUAL DE BOAS PRÁTICAS PARA APLICAÇÃO DA

LEI GERAL DE PROTEÇÃO DE DADOS

ACREFI
A CASA DO CRÉDITO DESDE 1958

ACREFI
A CASA DO CRÉDITO DESDE 1958

Presidente
Hilgo Gonçalves

Diretor Superintendente
Carlos Alberto Marcondes Machado

Coordenação
Cintia M. Ramos Falcão
Consultora Jurídica

Colaboração
Beatriz Gazoli – Ramos Falcão Consultoria
Cláudia Maciel Polonio – BMW Financeira S/A CFI
João Dias Jr. – Finamax S/A Crédito, Financiamento e Investimento
Miriam Lunaro Battistin Trevisan – Portoseg S/A Crédito, Financiamento e Investimento

Elaboração
Pinheiro Neto Advogados
Agosto/2019

Direção de Arte
Rogério Callamari Macadura
(Purim Comunicação Visual)

Impressão
Pancrom Indústria Gráfica

ÍNDICE

APRESENTAÇÃO

A ACREFI – Associação Nacional das Instituições de Crédito, Financiamento e Investimento, que congrega as empresas desses setores da economia, tem entre seus pilares compartilhar conhecimento. Com essa postura, a entidade está convicta de que contribui de maneira decisiva para o constante aperfeiçoamento do setor financeiro e, por extensão, da economia brasileira.

Nessa linha, estamos apresentando este Manual de Boas Práticas para Aplicação da Lei Geral de Proteção de Dados, esmiuçando de maneira mais didática os detalhes dessa legislação, tão importante para todas as empresas e para os cidadãos. De fato, não é comum que tenhamos uma legislação tão abrangente e que impacte tanto o dia a dia das companhias de todos os setores como a LGPD. Neste texto, desenvolvido pela ACREFI em parceria com o Pinheiro Neto Advogados, foi dada especial atenção aos pontos relevantes da legislação referentes às especificidades de nossos associados, e também para as empresas, e cidadãos, visando com isto aumentar a abrangência de conhecimento.

O *timing* de publicação deste Manual também é relevante. A previsão é que a LGPD entre em vigor em agosto de 2020, mas as empresas precisam ser ágeis , sendo recomendável que comecem de imediato o ajuste de seus negócios às novas normas, evitando imprevistos de última hora. Essa situação reforça a importância deste texto e mostra mais uma vez o compromisso da ACREFI de estar sempre ao lado de seus associados, promovendo o desenvolvimento de suas atividades.

Hilgo Gonçalves
Presidente da ACREFI

SOBRE ESTE MANUAL

Este manual foi desenvolvido pela Associação Nacional das Instituições de Crédito, Financiamento e Investimento (ACREFI) em parceria com Pinheiro Neto Advogados e busca apresentar pontos de atenção e aspectos da Lei nº 13.709, de 14 de agosto de 2018, conhecida como **Lei Geral de Proteção de Dados ("LGPD")** relevantes às sociedades de crédito, financiamento e investimento, tendo em vista as obrigações já aplicáveis em decorrência das obrigações já existentes na (i) Lei Complementar nº. 105, de 10 de janeiro de 2001 ("Lei de Sigilo Bancário"); (ii) Lei nº. 9.13, de 3 de março de 1998 ("Lei de Combate à Lavagem de Dinheiro"); (ii) Resolução do Conselho Monetário Nacional ("CMN") nº. 4.474, de 31 de março de 2016 ("Resolução 4474/16"); e (iv) Resolução CMN nº. 4.658, de 26 de abril de 2018 ("Resolução 4658/18") e, em conjunto com Lei de Sigilo Bancário, Lei Combate à Lavagem de Dinheiro, Resolução 4474/16 e Resolução 4658/18, a "Regulamentação Setorial").

Este manual tem um caráter meramente informativo e não substitui nem deve ser entendido como aconselhamento jurídico.

CAPÍTULO I

FOTOS DEPOSITPHOTOS

VISÃO GERAL DA LGPD E DA REGULAMENTAÇÃO SETORIAL

LGPD:

A LGPD passará a ser aplicável em agosto de 2020. Ela traz mudanças profundas nas condições para o tratamento de dados pessoais, o que inclui atividades como coleta, armazenamento, utilização, compartilhamento e eliminação de informações relacionadas a pessoas naturais identificadas ou identificáveis.

O longo período entre a data de publicação da LGPD (agosto/2018) e o início da sua vigência (agosto/2020) deriva da complexidade das ações que precisam ser tomadas pelas empresas para adaptação aos novos parâmetros legais.

No final do ano de 2018, foi criada a Autoridade Nacional de Proteção de Dados ("ANPD"), por meio da Medida Provisória nº 869/2018, convertida na Lei 13.853/2019.

A ANPD terá um papel tríplice de:

(i) fiscalização - poderá editar normas e procedimentos, deliberar sobre a interpretação da LGPD e requisitar informações relacionadas ao tratamento de dados pessoais;

(ii) sanção - terá poderes para instaurar processo administrativo quando houver descumprimento à LGPD e terá competência exclusiva para aplicar as sanções previstas na LGPD; e

(iii) educação - irá difundir o conhecimento sobre a LGPD e medidas de segurança, apresentando diretrizes para interpretação da lei, estimulando padrões para serviços e produtos que facilitem o controle de titulares sobre seus dados pessoais e elaborando estudos sobre melhores práticas nacionais e internacionais de proteção de dados pessoais, entre outros.

REGULAMENTAÇÃO SETORIAL:

Lei de Sigilo Bancário

Instituições financeiras, incluindo-se aí as sociedades de crédito, financiamento e investimento, devem manter sigilo em suas operações ativas e passivas e serviços prestados. Os únicos casos em que as informações sobre clientes, serviços ou operações de instituições financeiras e instituições de pagamento brasileiras podem ser divulgadas a terceiros, sem constituir violação do sigilo, são os seguintes:

(i) revelação de informações sigilosas com o consentimento expresso dos interessados;

(ii) a troca de informações entre as instituições financeiras para fins de registro;

(iii) o fornecimento a entidades de proteção ao crédito das informações com base em dados dos registros de emitentes de cheques bancários sacados de contas sem fundos suficientes e de devedores inadimplentes; e

(iv) a ocorrência ou suspeita de que atos ilegais criminais ou administrativos foram realizados, caso em que as instituições financeiras e as empresas de cartões de crédito podem fornecer às autoridades pertinentes as informações relacionadas a tais atos criminosos quando necessário para a investigação de tais atos.

A Lei de Sigilo Bancário também permite que o Banco Central do Brasil ou a Comissão de Valores Mobiliários troquem informações com autoridades governamentais estrangeiras, desde que um tratado específico tenha sido previamente assinado.

Lei de Combate à Lavagem de Dinheiro

Nos termos da Lei de Combate à Lavagem de Dinheiro, 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:

(i) 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);

(ii) adotar políticas, procedimentos e controles internos;

(iii) 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;

(iv) 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;

(v) analisar transações ou propostas cujas características possam indicar intenções criminosas; e

(vi) manter registros de cada transferência de fundos relacionada a, entre outras, (a) depósitos, transferências e cheques e (b) emissão de cheques e ordens de pagamento em montantes que excedam R$ 1.000.

Resolução 4474/16

A Resolução 4474/16 dispõe sobre a digitalização e a gestão de documentos digitalizados relativos às operações e às transações realizadas pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Entre os requisitos previstos na Resolução para digitalização e armazenamento dos documentos digitalizados, destaca-se (i) a necessidade de manutenção dos documentos digitalizados à disposição do Banco Central pelo prazo mínimo de cinco anos; (ii) a exigência de produção e manutenção de cópia de segurança dos documentos digitalizados em local físico distinto do local onde está armazenado o documento digitalizado; e (iii) 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.

Ressaltamos, ainda, que os procedimentos e as tecnologias utilizadas na digitalização de documentos (por exemplo produção e armazenamento), bem como o procedimento de descarte de documentos, devem ser descritos em manual específico da instituição, o qual deve assegurar a autenticidade, confidencialidade, integridade e disponibilidade das informações.

Além disso, destacam-se as obrigações de (i) manutenção de documentos digitalizados e suas respectivas cópias de segurança no Brasil; e (ii) averiguação se o descarte de documentos poderá afetar de maneira negativa, direta ou indiretamente, a tutela judicial e extrajudicial dos direitos que decorram dos documentos, inclusive no que diz respeito à produção de provas.

Resolução 4658/18

O gerenciamento de risco cibernético e o processamento de dados em nuvem das instituições autorizadas a funcionar pelo Banco Central do Brasil passaram a ser regulamentados pela Resolução 4658/18.

A partir de diretrizes próprias, a nova regulamentação direciona as instituições financeiras quanto à forma de elaborar, ou de adequar, os seus controles internos. A "Política de Segurança Cibernética" e os "Planos de Ação" para fins de prevenção e resposta aos incidentes cibernéticos deverão estar finalizados até 6.5.2019, e eventuais adequações não poderão ultrapassar a data limite de 31.12.2021.

Especificamente em relação ao **processamento de dados em nuvem** nessas instituições, a Resolução 4658/18 estabelece que estas devem assegurar que suas políticas, estratégias e estruturas para gerenciamento de riscos previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização de serviços (observando-se aí, inclusive, as diretrizes da LGPD), contemplem a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior.

As instituições financeiras e demais entidades autorizadas, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem:

(i) a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e

“O GERENCIAMENTO DE RISCO CIBERNÉTICO E O PROCESSAMENTO DE DADOS EM NUVEM DAS INSTITUIÇÕES AUTORIZADAS A FUNCIONAR PELO BANCO CENTRAL DO BRASIL PASSARAM A SER REGULAMENTADOS PELA RESOLUÇÃO 4658/18”

(ii) a verificação da capacidade do potencial prestador de serviço de assegurar: a) o cumprimento da legislação e da regulamentação em vigor (o que incluirá a LGPD); b) o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço; c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço; d) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado; e) o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados; f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados; g) a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

CAPÍTULO II

ALGUNS TERMOS E CONCEITOS IMPORTANTES DE COMPREENDER ANTES DE CONTINUAR A LEITURA DESTE MANUAL

Titular: é a pessoa física a quem um dado pessoal se refere.

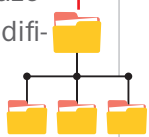
Dado pessoal: é qualquer informação relacionada a uma pessoa física identificada ou identificável. RG, CPF, endereço, data de nascimento são alguns exemplos de dados pessoais, mas informações como hábitos de consumo, localização geográfica, perfil comportamental, preferências, históricos de compras e outras informações semelhantes, quando relacionadas a uma pessoa física identificada ou identificável, são considerados "dados pessoais". Da mesma forma, informações sobre navegação na Internet, como endereço IP e cookies, entre outras, são em geral consideradas dados pessoais sempre que for possível identificar a pessoa relacionada a esses identificadores.

Dado pessoal sensível: é 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. A lei traz exigências adicionais e impõe algumas restrições para o tratamento de dados sensíveis.

Dado anonimizado e pessoa identificável: dado anonimizado é o oposto de dado pessoal, ou seja, é o dado que não pode ser associado a um indivíduo. É importante notar que ainda que um dado não esteja direta e explicitamente associado a uma pessoa identificada, ele pode ser considerado um dado pessoal (e não anônimo) sempre que for possível associá-lo a um indivíduo utilizando os meios técnicos disponíveis na ocasião.

Meios técnicos razoáveis e disponíveis: A LGPD não estabelece de maneira específica quais padrões, meios técnicos ou processos devem ser aplicados para que os dados sejam considerados suficientemente anonimizados. A interpretação sobre o que deve ser considerado "meio técnico razoável" em cada cenário será feita pela Autoridade Nacional de Proteção de Dados e a LGPD indica apenas que a autoridade deve considerar fatores objetivos, tais como custo e tempo necessários, considerando as tecnologias disponíveis e utilzação exclusiva de meios próprios.

Tratamento de dados: é toda operação realizada com dados pessoais – da coleta ao descarte, incluindo o mero armazenamento. A LGPD menciona expressamente diversos outros exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.



"A INTERPRETAÇÃO SOBRE O QUE DEVE SER CONSIDERADO "MEIO TÉCNICO RAZOÁVEL" EM CADA CENÁRIO SERÁ FEITA PELA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E A LGPD INDICA APENAS QUE A AUTORIDADE DEVE CONSIDERAR FATORES OBJETIVOS"

CAPÍTULO III

PRINCÍPIOS GERAIS E MELHORES PRÁTICAS

A LGPD 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 LGPD e que devem sempre ser considerados quando uma atividade envolver tratamento de dados pessoais.

Entre os princípios mais relevantes às instituições de crédito, financiamento e investimento, estão os seguintes:

Princípios da Finalidade, Adequação, Necessidade

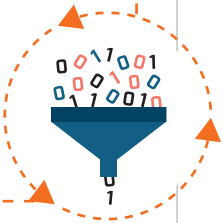
De acordo com esses princípios, dados pessoais só devem ser coletados e tratados para os propósitos específicos e legítimos que tenham sido informados ao titular de dados e sejam compatíveis com o contexto do tratamento. O tratamento deve ser limitado ao mínimo necessário para aquelas finalidades que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

Isso significa que antes de coletar, armazenar ou de qualquer maneira utilizar dados pessoais, é importante verificar:

(i) se o titular daqueles dados foi informado de maneira clara e específica sobre como os dados serão tratados e para quais finalidades – o porquê do tratamento;

(ii) se o tratamento é adequado ao contexto em que os dados foram coletados, ou seja, às expectativas que o titular de dados tinha ao fornecer os seus dados ou torná-los disponíveis; e

(iii) se é realmente necessário tratar aqueles dados para atingir aquela finalidade.



Princípios da Transparência, Livre Acesso

É importante 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. Uma recomendação é sempre utilizar linguagem 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 disso, é também necessário oferecer um canal de comunicação acessível para que os titulares de dados possam esclarecer suas dúvidas e solicitar informações.

Princípios da Segurança e Prevenção

Ao tratar dados pessoais, é importante implementar medidas técnicas e administrativas capazes de proteger esses dados de acessos não autorizados, perda, destruição, alteração, ou divulgação indevida, bem como prevenir 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.

Princípio da Não discriminação

O tratamento de dados pessoais não deve ser realizado para fins discriminatórios, ilícitos ou abusivos.

Melhores práticas: alguns exemplos

Utilize recursos audiovisuais. Para que as informações fiquem mais atrativas e compreensíveis, considere a adoção de vídeos, imagens e infográficos para ilustrar processos e tratamentos de dados pessoais. Recursos interativos também podem ser interessantes.

Clareza e objetividade são essenciais. Procure sempre oferecer informações de forma simples e direta, evitando ambiguidades e termos muito técnicos em seus documentos e políticas.

Seja flexível. Sempre que possível, dê liberdade para o usuário concordar ou não com o fornecimento de seus dados pessoais e gerenciar suas escolhas de privacidade, preferencialmente por meio de painéis de controle *(dashboards)* ou ferramentas similares. Não deixe as *checkboxes* pré-marcadas. Não colete dados excessivos ou desnecessários.

Seja disponível. Crie um canal de atendimento e de comunicação para que os usuários entrem em contato de maneira fácil e simplificada para tirar dúvidas sobre o tratamento de dados pessoais.

“É TAMBÉM NECESSÁRIO OFERECER UM CANAL DE COMUNICAÇÃO ACESSÍVEL PARA QUE OS TITULARES DE DADOS POSSAM ESCLARECER SUAS DÚVIDAS E SOLICITAR INFORMAÇÕES”

CAPÍTULO IV

DIREITOS DOS TITULARES DOS DADOS PESSOAIS

O artigo 17 da LGPD estabelece categoricamente que **"toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei"**. Ou seja, dados pessoais são de titularidade da pessoa natural a quem dizem respeito, e, portanto, não pertencem aos agentes de tratamento

O artigo 18 da LGPD estabelece diversos direitos que o titular possui e pode exercer, em relação aos agentes de tratamento, a qualquer momento e mediante requerimento expresso, que deve ser atendido sem custos para o titular, em prazos e termos a serem futuramente definidos em regulamento, a saber:

Direito de confirmação do tratamento: O titular tem direito à confirmação da existência de tratamento, ou seja, direito de saber se seus dados pessoais são ou não objeto de tratamento por um determinado controlador. Esse direito deriva do *princípio da transparência* previsto no artigo 6º, inciso VI da LGPD, pelo qual garante-se aos titulares *"informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".*

Direito de acesso: 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".*

Correção de dados incompletos, inexatos ou desatualizados: Um dos principais direitos do titular de dados pessoais é o direito à correção, 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 "exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento".

Anonimização, bloqueio ou eliminação de dados: O titular pode exigir que dados pessoais tidos como desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD sejam anonimizados, bloqueados ou eliminados. Esse direito deriva do princípio da necessidade, previsto no artigo 6º, inciso III da LGPD, pelo qual garante-se a *"limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados".*

Portabilidade dos dados a outro fornecedor de serviço ou produto: O titular poderá: (i) receber os dados pessoais que forneceram a um controlador de modo estruturado, normalmente em formato interoperável ou de uso corriqueiro e que possa ser lido automaticamente por computadores *(machine-readable),* para que possam ser utilizados por outro fornecedor de serviço ou produto; e/ou (ii) exigir a transferência direta desses dados pessoais a outro fornecedor de serviço ou produto, igualmente em formato que possibilidade a utilização dos dados pessoais pelo novo fornecedor. Note-se que nem sempre essa segunda hipótese será tecnicamente possível, dada a potencial incompatibilidade de sistemas ou mesmo de estruturas de bancos de dados, situação em que os dados pessoais devem ser fornecidos diretamente ao titular.

Eliminação dos dados pessoais tratados com o consentimento do titular: O titular pode exigir, mediante requerimento expresso, a eliminação dos dados pessoais tratados com o seu consentimento, exceto nas hipóteses previstas no artigo 16 da LGPD (cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados).

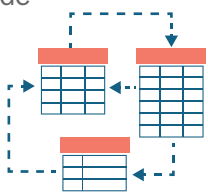
Uso compartilhado de dados: A LGPD assegura ao titular o direito de saber com quais entidades públicas e privadas o controlador realizou uso compartilhado de dados. O setor privado deve estar preparado para responder a essas requisições por meio da manutenção de registros de tratamento de dados pessoais *(record of processing activities),* tal como exigido pelo artigo 37 da LGPD. Um dos elementos mais complexos do uso compartilhado de dados está na obrigação imposta pelo § 6º do artigo 18, pelo qual *"o responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento".*

Possibilidade de não fornecer consentimento: A LGPD impõe aos controladores que utilizam o consentimento como base legal de tratamento de dados pessoais que informem aos titulares: (i) a possibilidade de não fornecer consentimento, quando factível, e (ii) as consequências da negativa, que em boa parte das vezes significará a impossibilidade de usufruir de determinado produto ou serviço.

Revogação do consentimento: Os controladores devem informar aos titulares que eles têm o direito de revogar seu consentimento a qualquer tempo e como podem exercer esse direito, preferencialmente por meio de um procedimento rápido e simplificado e sem serem prejudicados.

Direito de petição: A LGPD estabelece que *"o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional"* (art. 18, § 1º), de forma a deixar claro que o órgão responsável por receber eventuais queixas ou denúncias formuladas pelos titulares de dados pessoais é a Autoridade Nacional. É importante observar que o § 8º do mesmo artigo diz que *"o direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor"*. Daí não decorre, porém, que organismos de defesa do consumidor possam exercer o mesmo papel da Autoridade Nacional. Isso apenas significa que, em nome da facilitação de seus direitos, o titular pode peticionar a esses organismos, cuja função nesse contexto é limitada a receber a petição com a queixa ou a denúncia e encaminhá-la à Autoridade Nacional.

Direito de oposição: O § 2º do artigo 18 da LGPD estipula que "o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei". Em outras palavras, toda vez que a base legal de tratamento de dados não for o consentimento e houver descumprimento da LGPD, o titular pode se opor ao tratamento de seus dados pessoais, independentemente da adoção de medidas corretivas ou imposição de penalidades, exigindo a imediata interrupção de qualquer atividade de tratamento.



CAPÍTULO V

DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

A LGPD define os papéis dos agentes de tratamento, definidos pela lei como “Controlador” e como “Operador”.

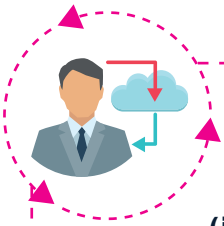
O controlador é quem exerce controle geral sobre (i) as finalidades para as quais e (ii) as maneiras pelas quais os dados pessoais são e serão tratados, seja por si só, em conjunto ou em comum com outros agentes. Em outras palavras, será o controlador que decidirá o “porquê” e o “como” da atividade de tratamento de dados, sendo o agente responsável por todo o ciclo de vida dos dados – da sua coleta à sua exclusão.

Como consequência da posição como principal tomador de decisões e do maior poder de controle sobre os procedimentos e as finalidades envolvendo o uso dos dados pessoais, o controlador também terá maiores responsabilidades sobre tais dados e, eventualmente, sobre quaisquer violações decorrentes do processo de tratamento dos mesmos.

O controlador não apenas representa a figura central na proteção dos direitos dos titulares – devendo observar a legislação e garantir que as atividades de processamento exercidas por todos os agentes envolvidos estejam em conformidade com a lei – mas também exerce funções relevantes para a cadeia de tratamento de dados. Dois dos principais deveres do controlador são, por exemplo, a elaboração de relatório de impacto à proteção de dados pessoais e a nomeação de um Encarregado pelo tratamento de dados pessoais para atuar como canal de comunicação entre o controlador e a Autoridade Nacional de Proteção de Dados, e o controlador e os titulares.

O operador é a pessoa natural ou jurídica, de direito público ou privado, 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.

Apesar de o operador atuar em nome do controlador e obedecendo as suas decisões, é comum que o controlador de dados conceda ao agente



O controlador ainda é responsável pelo seguinte:

(i) obtenção de consentimento específico do titular, quando necessário;

(ii) informação e prestação de contas e pela garantia de portabilidade dos dados;

(iii) garantia de transparência no tratamento de dados baseado em legítimo interesse;

(iv) manutenção de registro das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse;

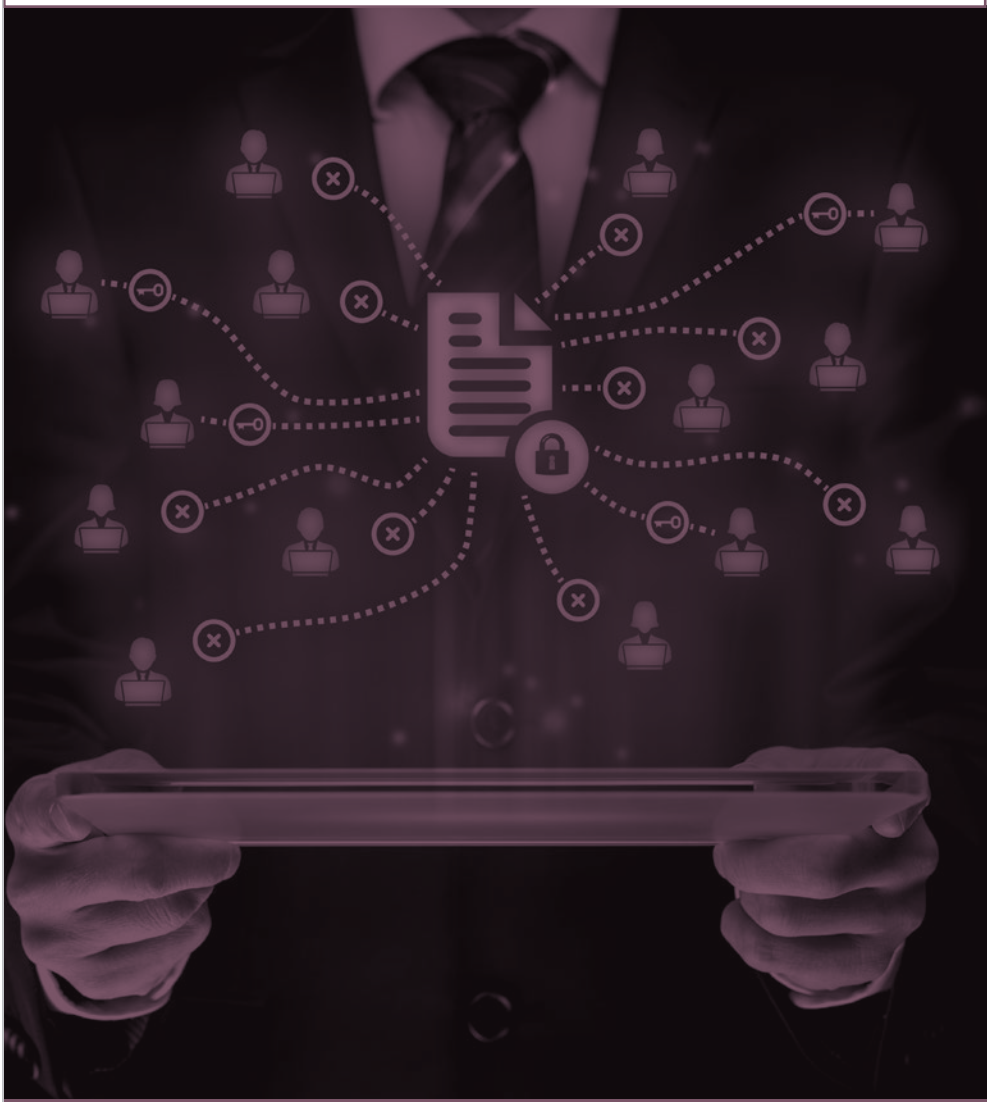
(v) reparação de danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais, e

vi) comunicação à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

operador um certo grau de discricionariedade e liberdade sobre o processo de tratamento dos dados, permitindo que exerça controle sobre o modo com que os dados serão tratados. Nesse sentido, o operador poderá exercer certo controle principalmente sobre os aspectos técnicos relativos a como um serviço específico será prestado.

Isso quer dizer que o operador tem a liberdade de utilizar a sua experiência na operação de tratamento de dados e seus conhecimentos técnicos para decidir como conduzir certas atividades em nome do controlador. No entanto, o operador não poderá tomar quaisquer decisões relevantes sobre os dados, como, por exemplo, quais dados serão usados para quais finalidades, qual o conteúdo dos dados, ou de que forma tais dados serão utilizados. Tais decisões podem ser tomadas tão somente pelo controlador, pois é esse quem possui poder decisório sobre os mesmos.

CAPÍTULO VI



DO 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 a Autoridade Nacional de Proteção de Dados (ANPD).

A ANDP poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Entre as principais funções do Encarregado, estão:

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

b) receber comunicações da autoridade nacional e adotar providências;

c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Por fim, deverá ser divulgada publicamente, de forma clara e objetiva, preferencialmente no website do controlador, a identidade e as informações de contato do Encarregado.

CAPÍTULO VII

POR QUE A LGPD INTERESSA ÀS FINANCEIRAS E DEMAIS INSITUIÇÕES AUTORIZADAS A OPERAR PELO BANCO CENTRAL DO BRASIL?

Atividades de crédito, financiamento e investimento frequentemente envolvem tratamento e compartilhamento de dados pessoais. As atividades bancárias e de financiamento estão entre as mais afetadas pela LGPD, especialmente no contexto da concessão de crédito digital, uma vez que (i) se baseiam fortemente nos hábitos e comportamentos dos consumidores, derivados do tratamento de dados pessoais; (ii) o compartilhamento de dados no contexto de análise de risco de crédito é comum; (iii) para cadastrar os consumidores nas plataformas são utilizados dados pessoais; e (iv) o tratamento de dados pessoais é muitas vezes necessário no combate à lavagem de dinheiro e prevenção a fraudes.

A LGPD tem um extenso âmbito de aplicação. A LGPD aplica-se a qualquer operação de tratamento de dados pessoais realizada em território brasileiro ou relacionada a dados pessoais de indivíduos localizados no Brasil no momento em que os dados foram coletados, ou ainda se o tratamento de dados pessoais tem por objetivo oferecer produtos ou serviços no Brasil. Além disso, é importante notar que a LGPD não está restrita ao ambiente digital. Por exemplo, dados pessoais coletados durante o processo de abertura de contas em agências físicas, entre outras situações, também estão sujeitos à LGPD.

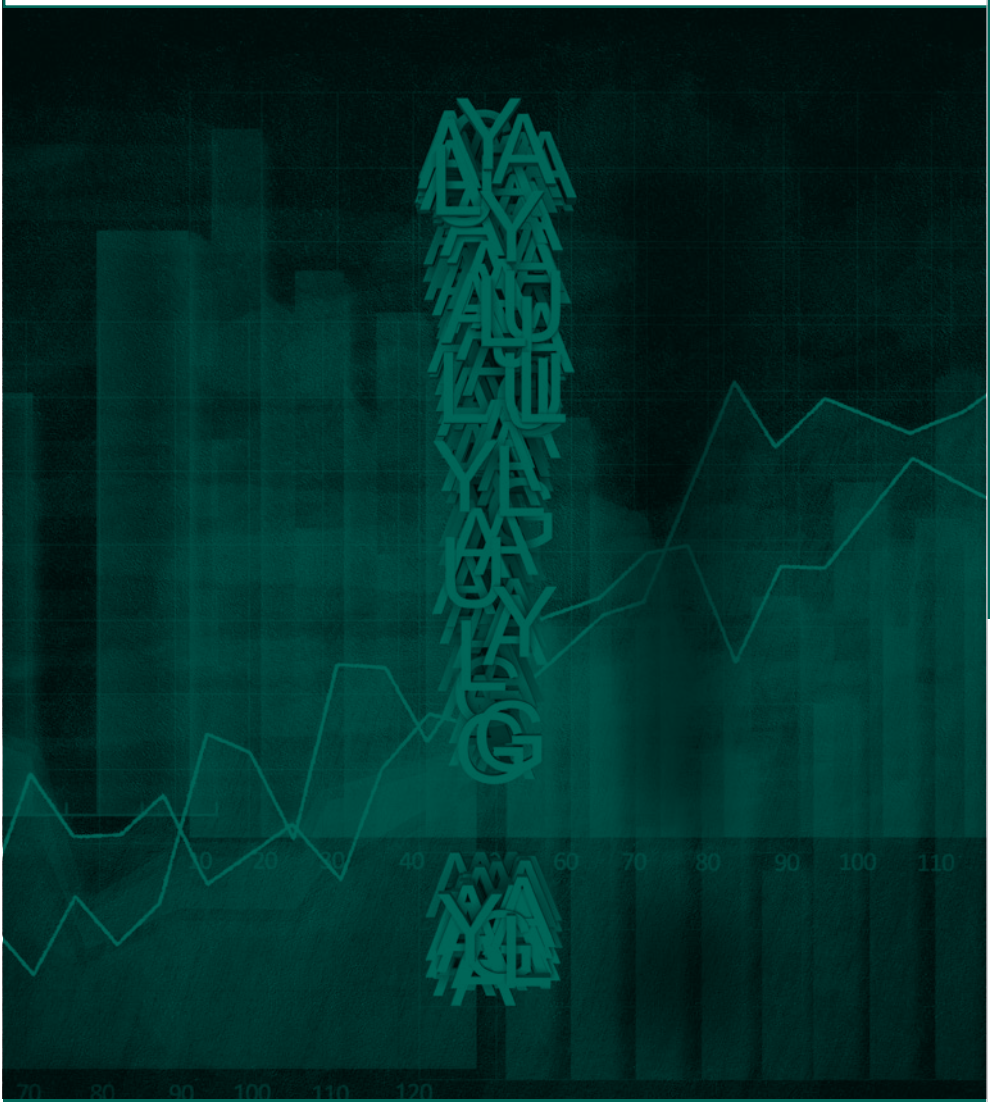
“ALÉM DISSO, É IMPORTANTE NOTAR QUE A LGPD NÃO ESTÁ RESTRITA AO AMBIENTE DIGITAL. POR EXEMPLO, DADOS PESSOAIS COLETADOS DURANTE O PROCESSO DE ABERTURA DE CONTAS EM AGÊNCIAS FÍSICAS, ENTRE OUTRAS SITUAÇÕES, TAMBÉM ESTÃO SUJEITOS À LGPD”

Impactos nas rotinas operacionais. Os direitos e as obrigações estabelecidos pela LGPD requerem a revisão e a adequação de diversas rotinas operacionais das instituições financeiras. Por exemplo, a LGPD estabelece que os titulares de dados podem solicitar o acesso aos dados pessoais mantidos pelas empresas, bem como a revisão dos seus respectivos perfis pessoais ou de consumo que tenham sido formados com base em tratamento automatizado de dados (p.ex. por meio de algoritmos para construção de um índice de adimplência). Será necessário criar mecanismos para atender a essas solicitações. Será também necessário estabelecer rotinas para a exclusão de dados mediante revogação do consentimento do titular ou de dados que não servem mais à finalidade para a qual foram originalmente coletados. Ainda, a LGPD determina que o titular de dados pode solicitar a portabilidade de seus dados para outro fornecedor de serviço ou produto, o que também requer o estabelecimento de processos operacionais específicos.

O descumprimento da LGPD tem um custo alto. Além das sanções administrativas e judiciais aplicáveis em caso de descumprimento – a multa pode chegar a 2% do faturamento da empresa no Brasil, até o limite de R$ 50 milhões, por infração – estar em desconformidade com a LGPD pode acarretar danos reputacionais significativos, prejudicando a imagem e as marcas da empresa perante seus consumidores e clientes.

Além disso, a adequação à LGPD será cobrada pelo próprio mercado, tornando-se uma vantagem competitiva importante para a escolha de parceiros de negócio e para o estabelecimento e a manutenção de relacionamento comercial entre instituições financeiras. Além disso, os passivos decorrentes de descumprimento das obrigações estabelecidas pela LGPD também serão fatores determinantes no âmbito da captação de investimentos e em operações de fusão e aquisição.

CAPÍTULO VIII



CUIDADOS COM O CONSENTIMENTO

O tratamento de dados pessoais só pode ser realizado em dez hipóteses estabelecidas pela LGPD. Essas hipóteses são conhecidas como *bases legais de tratamento.*

Uma das bases legais de tratamento é o *consentimento do titular,* ou seja, a concordância com o tratamento de seus dados pessoais para uma finalidade determinada.

O consentimento, no entanto, precisa respeitar alguns requisitos para que seja considerado válido:

Livre: o consentimento deve refletir uma manifestação livre da vontade do titular. Ou seja, o titular dos dados não pode ser compelido a consentir com o tratamento.

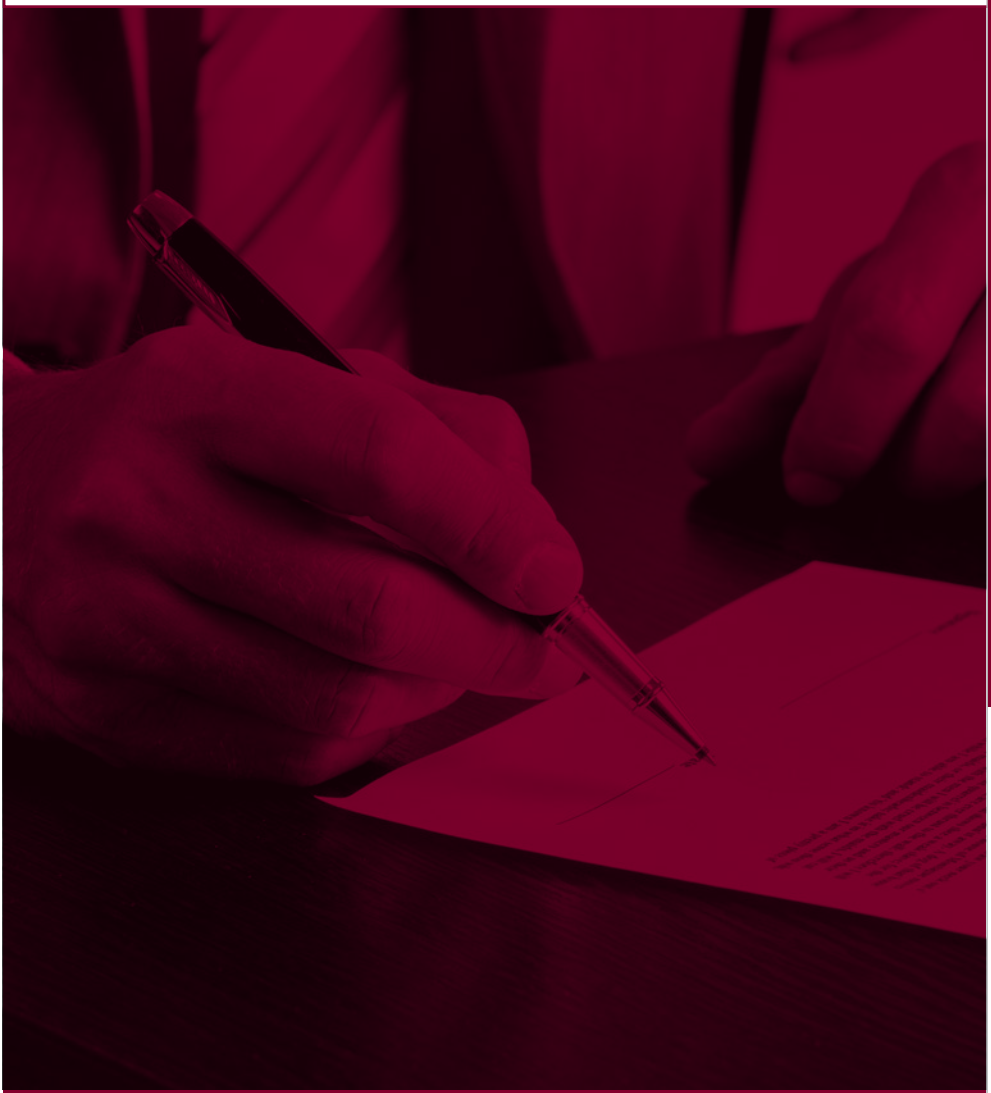
Informado: o titular deve ter recebido informações claras, objetivas e suficientes para decidir de maneira consciente se concorda com o tratamento de seus dados pessoais para as finalidades mencionadas.

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 (por exemplo, gravação de uma ligação telefônica). Consentimentos implícitos, que não tenham sido registrados, ou que deixem por algum motivo dúvidas sobre a vontade do titular, poderão ser desconsiderados.

Relacionado a uma finalidade determinada: o titular de dados deverá autorizar o tratamento de dados para uma finalidade específica. Autorizações genéricas ou vagas podem ser consideradas nulas.

Além de se atentar aos pontos acima, é muito importante que as financeiras se atentem ao fato de que o consentimento é revogável a qualquer tempo pelo titular de dados pessoais.

CAPÍTULO IX



POSSO TRATAR DADOS SEM O CONSENTIMENTO DO TITULAR?

A LGPD traz nove hipóteses em que é possível tratar dados pessoais sem obter o consentimento do titular. Entre elas, as que possuem maior relevância às sociedades de crédito, financiamento e investimento são:

Cumprimento de obrigação legal ou regulatória: se uma lei ou uma regulamentação setorial exige determinada atividade de tratamento de dados, não é preciso solicitar a autorização do titular de dados. É o caso, por exemplo, de registros de acesso a aplicações online para cumprir com as obrigações de retenção previstas no Marco Civil da Internet, legislação que exige que os últimos seis meses de atividade do usuário sejam registrados pelas empresas que oferecem funcionalidades online. Também é o caso para as hipóteses de quebra de sigilo previstas na Lei 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. O tratamento desses dados pessoais é feito justamente para cumprir o contrato celebrado.

Para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Ou seja, o armazenamento ou outra forma de tratamento de dados pessoais para utilização em eventual processo judicial é possível, independente de autorização do titular. Por exemplo, pode ser necessário guardar o histórico de compras e dados de contato de consumidores em casos de litígios pós-venda.

Para atender aos interesses legítimos da empresa responsável pelo tratamento ou aos interesses legítimos de terceiros, desde que o tratamento de dados não ofereça um risco importante aos direitos e liberdades fundamentais dos titulares de dados. Esses pontos são detalhados na seção seguinte, que trata especificamente do legítimo interesse, mas é importante compreender que a LGPD exige a análise do impacto à privacidade do titular de dados e a documentação dessa análise quando se utiliza o legítimo interesse.

Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. A lei brasileira inovou ao definir a proteção do crédito como uma base legal autônoma que autoriza o tratamento de dados pessoais. Ainda que a lei não tenha definido o conceito de "proteção do crédito", entendemos que a expressão deve ser interpretada extensivamente, autorizando o tratamento de dados pessoais tanto para atividades inerentes à concessão de crédito quanto para atividades de apoio, incluindo, portanto, o oferecimento de produtos e serviços de crédito e o gerenciamento de riscos dessas operações.

As outras hipóteses previstas na LGPD envolvem tratamentos de dados para a proteção da vida ou da incolumidade física do titular dos dados ou de terceiro, para a tutela da saúde, ou situações específicas de tratamento de dados pela administração pública ou por órgão de pesquisa.

No caso de dados pessoais *sensíveis*, nem todas essas bases legais estão disponíveis – por exemplo, o legítimo interesse, a execução de contrato e a proteção do crédito não autorizam o tratamento de dados pessoais sensíveis. Nessas hipóteses, é recomendável avaliar se o tratamento de dados sensíveis realmente compensa a necessidade de cumprir com as exigências adicionais previstas na LGPD para esses casos.

"A LEI BRASILEIRA INOVOU AO DEFINIR A PROTEÇÃO DO CRÉDITO COMO UMA BASE LEGAL AUTÔNOMA QUE AUTORIZA O TRATAMENTO DE DADOS PESSOAIS"

CAPÍTULO X

LEGÍTIMO INTERESSE

O tratamento de dados pessoais com base no legítimo interesse é, certamente, a hipótese mais abrangente e flexível prevista na LGPD. A lei não estabelece em quais situações existe ou não um *legítimo interesse* para tratar dados pessoais, e indica que essa análise deverá ser realizada a partir de situações concretas.

Essas situações concretas incluem, mas não se limitam, a apoio e promoção de atividades do controlador; e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

É mais provável que exista um legítimo interesse em situações em que o tratamento a ser realizado esteja dentro das expectativas razoáveis dos titulares de dados e tenham um pequeno impacto à sua privacidade, ou se houver uma justificativa relevante para o tratamento.

Existem três elementos que devem ser considerados:
(i) identificar para quais finalidades o tratamento será realizado, e se essas finalidades são legítimas e consideradas a partir de situações concretas;
(ii) verificar se é realmente necessário realizar o tratamento de dados para atingir aquela finalidade, e
(iii) balancear o interesse legítimo identificado com os direitos e as liberdades fundamentais dos titulares de dados que sejam impactados por esse tratamento.

A LGPD não apresenta uma lista pré-determinada do que constitui ou não legítimo interesse, justamente porque isso é determinado caso a caso. A LGPD cita como exemplos o apoio e a promoção de atividades do responsável pelo tratamento dos dados pessoais.

Isso significa que, em tese, o tratamento de dados pessoais para finalidades atreladas a atividades de concessão de crédito e financiamentos, por exemplo, poderia ser realizado com fundamento no legítimo interesse, desde que observados os requisitos e os elementos indicados acima. Na prática, sempre será necessária uma análise detalhada de cada operação e das maneiras e finalidades do tratamento para confirmar se é possível ou não utilizar o legítimo interesse como base legal.

Uma vez verificada a possibilidade de tratar dados pessoais com base no legítimo interesse, é necessário elaborar um *relatório de impacto à proteção de dados pessoais* (conhecido em inglês como *Data Protection Impact Assessment – DPIA*). Esse relatório deve descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades e aos direitos dos titulares de dados, bem como medidas, salvaguardas e mecanismos de mitigação de risco adotados. A Autoridade Nacional de Proteção de Dados poderá solicitar a apresentação desse relatório.

“NA PRÁTICA, SEMPRE SERÁ NECESSÁRIA UMA ANÁLISE DETALHADA DE CADA OPERAÇÃO E DAS MANEIRAS E FINALIDADES DO TRATAMENTO PARA CONFIRMAR SE É POSSÍVEL OU NÃO UTILIZAR O LEGÍTIMO INTERESSE COMO BASE LEGAL”

CAPÍTULO XI

TÉRMINO DO TRATAMENTO DE DADOS PESSOAIS

A LGPD estipula a obrigatoriedade de eliminação dos dados pessoais ao término do tratamento. Isso ocorre nas seguintes hipóteses:
a) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
b) fim do período de tratamento;
c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou
d) determinação da autoridade nacional, quando houver violação da lei.

Contudo, a LGPD estipula que a conservação dos dados pessoais será autorizada em alguns casos:
a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
c) transferência à terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na lei; ou
d) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Note-se que certas atividades de tratamento (tais como operações de análise de crédito e prevenção a fraude) justificam o tratamento contínuo dos dados pessoais envolvidos, não existindo nessas hipóteses um dever geral de eliminação dos dados pessoais. Por exemplo, a própria existência de modelos para análise de crédito e prevenção a fraude pressupõe a possibilidade de comparações de dados pessoais oriundos de múltiplas amostras, relacionadas a pessoas naturais diferentes, e a eliminação desses dados inviabilizaria a própria atividade.

CAPÍTULO XII

GOVERNANÇA

No contexto de adequação à LGPD e para garantir o efetivo cumprimento das suas disposições, é altamente recomendável que as instituições adotem programas de governança em privacidade, especialmente tendo em vista as obrigações de controles internos, prevenção à lavagem de dinheiro e política de segurança cibernética previstas na Regulamentação Setorial.

Esses programas devem estabelecer, por exemplo, condições, regimes 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 de tratamento, ações educativas, mecanismos internos de supervisão e mitigação de riscos, procedimentos de resposta a incidentes de segurança, entre outros.

É também muito importante que todos os processos, decisões, esforços e ações relacionados à governança de dados pessoais na empresa sejam documentados e mantidos em arquivo para apresentação à ANPD, se necessário.

“A ADOÇÃO DE POLÍTICAS DE BOAS PRÁTICAS E GOVERNANÇA NÃO APENAS AUXILIA A INSTITUIÇÃO A CUMPRIR COM AS OBRIGAÇÕES ESTABELECIDAS PELA LGPD, COMO EVIDENCIA OS ESFORÇOS NESSE SENTIDO E SERÁ CONSIDERADA (COMO UM ATENUANTE) NA APLICAÇÃO DE PENALIDADES EM CASO DE DESCUMPRIMENTO DA LGPD”

A adoção de políticas de boas práticas e governança não apenas auxilia a instituição a cumprir com as obrigações estabelecidas pela LGPD, como evidencia os esforços nesse sentido e será considerada (como um atenuante) na aplicação de penalidades em caso de descumprimento da LGPD.

Do ponto de vista prático, um programa de governança em privacidade deve:

a) demonstrar o comprometimento da instituição em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) ser aplicável a todo o conjunto de dados pessoais que estejam sob o controle da empresa, independentemente do modo como se realizou sua coleta;

c) ser adaptado à estrutura, à escala e ao volume das operações da instituição, bem como à sensibilidade dos dados tratados;

d) estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) estar integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) contar com planos de resposta a incidentes e remediação; e

h) ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

CAPÍTULO XIII

ASPECTOS INTERNACIONAIS DA LGPD E DA REGULAMENTAÇÃO SETORIAL

LGPD:

A LGPD foi fortemente inspirada no Regulamento Geral de Proteção de Dados europeu (*General Data Protection Regulation* – GDPR) que entrou em vigor na Europa em maio de 2018. Assim como o GDPR, a LGPD estabelece limitações à transferência internacional de dados pessoais para países que não ofereçam um grau de proteção de dados pessoais adequados aos previstos na LGPD. Essas limitações se aplicam inclusive às transferências internacionais decorrentes de serviços de cloud e armazenamento em datacenters localizados em outros países.

Esse sistema é conhecido como "adequação", e sua intenção é evitar que dados pessoais protegidos pela LGPD sejam enviados para países que ofereçam risco à privacidade dos seus titulares, sem que a Autoridade Nacional de Proteção de Dados possa intervir.

Justamente por isso, a Autoridade Nacional de Proteção de Dados deverá indicar quais são os países que ela considera que oferecem grau adequado de proteção aos dados pessoais.

A LGPD estabelece hipóteses em que é possível transferir dados pessoais para outros países mesmo que não tenham sido reconhecidos como adequados pela Autoridade Nacional de Proteção de Dados.

Por exemplo, empresas que efetuam regularmente transferências internacionais deverão oferecer garantias por meio de contratos (que podem ser tanto cláusulas-padrão criadas pela Autoridade Nacional de Proteção de Dados, quanto normas corporativas globais criadas pela empresa e aprovadas pela ANPD).

Em outros casos, as empresas podem se valer do cumprimento de obrigação legal ou regulatória, da execução de contrato ou do exercício regular de direitos para efetuar a transferência internacional, ou podem contar com o consentimento específico e destacado do titular de dados pessoais para a transferência.

Do ponto de vista prático, antes de realizar qualquer transferência internacional de dados pessoais – mesmo que decorrentes da utilização de serviços de cloud –é importante analisar cuidadosamente se a transferência é permitida e qual o mecanismo legal será utilizado para justificá-la.

Além disso, como a LGPD se aplica a qualquer empresa, nacional ou estrangeira, que queira tratar dados pessoais de pessoas localizadas no território brasileiro, inclusive no contexto do oferecimento de produtos ou serviços, é importante que as instituições financeiras se atentem que eventuais parceiros comerciais estrangeiros também estarão sujeitos à LGPD se efetuarem o tratamento de dados pessoais de titulares nessas condições.

Resolução 4658/18

A contratação de serviços de processamento, armazenamento de dados e de computação em nuvem prestados no exterior por sociedades de crédito, financiamento e investimento, deve observar os seguintes requisitos, além dos já mencionados acima:

(i) existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados. No caso de inexistência de convênio, a instituição contratante deverá solicitar autorização do Banco Central do Brasil para a contratação;

(ii) a instituição contratante deve assegurar que a prestação dos serviços referidos não cause prejuízos ao seu regular funcionamento, nem atrapalhe a atuação do Banco Central do Brasil;

(iii) a instituição contratante deve definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e

(iv) a instituição contratante deve prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção dos serviços.

CAPÍTULO XIV

VIOLAÇÕES E SANÇÕES

LGPD:

Violações à LGPD estão sujeitas a sanções administrativas, a serem aplicadas pela Autoridade Nacional de Proteção de Dados, após processo administrativo, sem prejuízo de outras sanções ou penalidades civis ou criminais.

As duas principais sanções são:
i) multa de até 2% do faturamento do grupo econômico no Brasil no último exercício, até o limite de R$ 50.000.000,00 por infração, e
ii) publicização da infração, ou seja, determinação da Autoridade Nacional de Proteção de Dados para que a violação da LGPD seja amplamente divulgada em meios de comunicação, para conhecimento do público.

Em outras palavras, além de eventual prejuízo financeiro, violar a LGPD pode acarretar danos reputacionais significativos, prejudicando a imagem e as marcas da empresa perante seus consumidores e clientes.

Além disso, a Autoridade Nacional de Proteção de Dados poderá aplicar advertência, com prazo para a adoção de medidas corretivas e, em casos mais graves, determinar o bloqueio temporário ou a eliminação definitiva dos dados pessoais a que se refere a infração.

Lei de Sigilo Bancário

A quebra de sigilo, fora das hipóteses autorizadas, constitui crime e sujeita os responsáveis à pena de reclusão, de um a quatro anos, e multa. Cabe mencionar ainda que incorre nas mesmas penas quem omitir, retardar injustificadamente ou prestar falsamente as informações requeridas.

Lei de Combate à Lavagem de Dinheiro

As instituições (e seus controladores e administradores) que descumprirem as obrigações adoção de controles internos preventivos e de comunicação de operações ao COAF estarão sujeitas às seguintes sanções administrativas, cumulativamente ou não:

(i) advertência;

(ii) multa pecuniária variável não superior: a) ao dobro do valor da operação; b) ao dobro do lucro real obtido ou que presumivelmente seria obtido pela realização da operação; ou c) ao valor de R$ 20.000.000,00;

(iii) inabilitação temporária, pelo prazo de até dez anos, para o exercício do cargo de administrador de instituições financeiras e demais entidades autorizadas a operar pelo Banco Central do Brasil e Superintendência de Seguros Privados; e

(iv) cassação ou suspensão da autorização para o exercício de atividade, operação ou funcionamento.

“ALÉM DISSO, A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PODERÁ APLICAR ADVERTÊNCIA, COM PRAZO PARA A ADOÇÃO DE MEDIDAS CORRETIVAS E, EM CASOS MAIS GRAVES, DETERMINAR O BLOQUEIO TEMPORÁRIO OU A ELIMINAÇÃO DEFINITIVA DOS DADOS PESSOAIS A QUE SE REFERE A INFRAÇÃO”

CAPÍTULO XV

PONTOS DE ATENÇÃO E PERGUNTAS FREQUENTES

Quando a LGPD não se aplica?

A LGPD não é aplicável ao tratamento de dados de pessoas jurídicas e nem de dados anonimizados, já que nenhum desses dados é considerado *dado pessoal.*

A LGPD também não se aplica ao tratamento de dados pessoais realizado:

- por pessoa natural para fins exclusivamente particulares e não econômicos;
- para fins exclusivamente jornalísticos, artísticos ou acadêmicos;
- para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Não obstante, a Lei de Sigilo Bancário permanece aplicável com relação a todas as operações ativas, passivas e serviços prestados por instituição financeira, conforme definição em referida lei. Desta forma, independente se a contraparte da operação ou tomador do serviço é pessoa jurídica ou ainda se os dados serão utilizados para os fins elencados acima, aplicando-se apenas as excludentes previstas na Lei de Sigilo Bancário apresentadas no início deste manual.

Existem dados pessoais que exigem mais proteção do que outros?

Sim, o tratamento de algumas categorias de dados pessoais oferece maiores riscos de danos aos respectivos titulares e por isso são tratados pela LGPD como "dados sensíveis".

São considerados dados sensíveis pela LGPD: 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. É importante observar que a fotografia do rosto de uma pessoa pode ser considerada dado biométrico.

Em boa parte dos casos, as sociedades de crédito, financiamento e investimento deverão obter o consentimento dos titulares de maneira específica para poder tratar dados sensíveis.

Posso reaproveitar bases de dados existentes para desenvolver novos produtos/serviços?

Cuidado. Se os dados foram coletados com base no consentimento para um uso específico e esse consentimento não previa o desenvolvimento desses novos produtos ou serviços, provavelmente será necessário obter um novo consentimento dos titulares de dados pessoais.

Alternativamente, é necessário verificar se o tratamento de dados pessoais realizado para o desenvolvimento desses novos produtos ou serviços poderia ser enquadrado em uma das outras nove hipóteses em que é permitido tratar dados pessoais sem consentimento, e se atende aos princípios estabelecidos na LGPD, principalmente aos princípios da transparência, finalidade, adequação e necessidade.

Posso usar dados públicos à vontade?

Dados pessoais publicamente disponíveis – seja porque foram tornados públicos pelo titular, seja porque encontram-se em bases de acesso público – não deixam de ser dados pessoais. Nesses casos, a LGPD permite que dados pessoais sejam utilizados sem necessidade de obtenção de consentimento do titular, mas continua sendo necessário enquadrar esse tratamento em uma das outras bases legais disponíveis e observar todos os direitos dos titulares de dados e os princípios estabelecidos pela LGPD.

Ou seja, é necessário dar transparência ao tratamento desses dados publicamente disponíveis e às finalidades do tratamento, enquadrar o tratamento em uma base legal, franquear ao titular acesso a informações sobre quais dados pessoais estão sendo tratados, como e porque, entre outras obrigações aplicáveis.

E dados anônimos?

Dados anônimos não são considerados dados pessoais e, a princípio, não estão sujeitos à LGPD. É importante, no entanto, confirmar se os dados podem realmente ser considerados anônimos. Em muitas ocasiões, dados aparentemente anônimos podem ser facilmente re-identificados.

Por exemplo: há situações em que os dados pessoais passam por procedimentos que removem identificadores pessoais (como nome e CPF), os quais são substituídos por números, códigos ou *hashes*, criando-se uma nova base de dados. Porém, se o detentor dessa base de dados também tiver acesso à base original identificada (como, por exemplo, quando uma mesma empresa cria diferentes bases de dados com informações pessoais removidas para que diferentes áreas de negócio trabalhem com elas), ou possa cruzar informações de outras bases de dados às quais têm acesso para identificar os titulares, essa base de dados supostamente anonimizada será, em verdade, considerada apenas pseudonimizada, aplicando-se normalmente a LGPD.

“É IMPORTANTE, NO ENTANTO, CONFIRMAR SE OS DADOS PODEM REALMENTE SER CONSIDERADOS ANÔNIMOS. EM MUITAS OCASIÕES, DADOS APARENTEMENTE ANÔNIMOS PODEM SER FACILMENTE RE-IDENTIFICADOS”

O que fazer em caso de um incidente de segurança?

Incidentes de segurança que possam acarretar risco ou dano aos titulares de dados devem ser comunicados à Autoridade Nacional de Proteção de Dados e aos respectivos titulares de dados. A LGPD estabelece o conteúdo mínimo que deve constar da notificação.

Além disso, a Autoridade Nacional ao verificar a gravidade do incidente, poderá determinar providências adicionais, tais como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

Toda empresa deve criar e manter um plano de resposta a incidentes, definindo como agir interna e externamente nessas situações.

Em complemento ao disposto na LGPD, as instituições financeiras estão sujeitas ao disposto na Resolução 4658/18, a qual estabelece que tais instituições deverão contar com uma política de segurança cibernética e controles e procedimentos relacionados ao gerenciamento de risco cibernético. Neste contexto, em caso de incidente, a instituição deverá também observar e seguir os procedimentos estabelecidos em sua política e em conformidade com a regulamentação em vigor.

Quais os cuidados envolvendo criação de perfis *(profiling)*?

Em primeiro lugar, o titular dos dados pessoais tem o direito de solicitar a revisão de seus perfis (de comportamento, consumo, etc.) formados de maneira automatizada (por exemplo, por algoritmos).

Outro ponto de atenção envolvendo a formação de perfis é a dificuldade em torná-los anônimos. Perfis compostos por um grande volume de informações, ainda que que não estejam atribuídas a um identificador pessoal como nome, CPF ou RG, por vezes possibilitam a identificação da pessoa a quem se referem por meio de inferências. Isso porque, quanto maior o volume e mais específicas as informações acerca de uma pessoa (ainda que não identificada), menor o universo de indivíduos a quem aqueles dados podem ser atribuídos.

Por exemplo, em uma primeira análise, alguém poderia considerar que informações sobre os hábitos de deslocamento de pessoas não identificadas seriam consideradas informações anônimas. No entanto, se esses hábitos forem detalhados ao ponto de se identificar trajetos, rotinas e endereços específicos, a pessoa pode se tornar facilmente identificável e esse perfil não poderá ser considerado anônimo.

A Instituição pode ser responsabilizada por atos de terceiros?

Sim. Todos os profissionais ou empresas que tomarem decisões e estiverem diretamente envolvidos nas atividades de tratamento de dados pessoais realizadas em violação à lei serão solidariamente responsáveis pelo ressarcimento dos danos causados aos titulares, salvo se puderem provar que (i) não realizaram o tratamento de dados pessoais que lhes é atribuído, ou (ii) embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados, ou (iii) o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

Por esses motivos, é bastante importante trabalhar com parceiros comerciais que estejam buscando se adequar à LGPD, já que eventual desconformidade alheia pode, conforme as circunstâncias do caso, acarretar responsabilidade solidária.

No que se refere especificamente à contratação de serviços de processamento em nuvem e gerenciamento de risco cibernético nos termos da Resolução 4658/18, bem como ao armazenamento de documentos digitalizados nos termos da Resolução 4474/16, as instituições financeiras que contratarem terceiros para a prestação de tais serviços deverão observar os critérios estabelecidos na regulamentação para a realização de tais contratações e responderão pelos serviços e prestadores contratados no que se refere à observância dos requisitos regulatórios.

A LGPD passa a valer em 2020. E como ficam as regras do Marco Civil da Internet?

O Marco Civil da Internet (Lei 12.965/2014), em vigor desde junho de 2014, estabelece que o usuário da Internet tem direito ao seguinte:

(i) não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

(ii) informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

(iii) consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais, e

(iv) exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros.

A LGPD, porém, regula todas as atividades de tratamento de dados pessoais, inclusive nos meios digitais.

Isso significa que, até a entrada em vigor da LGPD, continuam válidas as regras do Marco Civil da Internet para as atividades realizadas online. Posteriormente, espera-se que a LGPD substitua as regras do Marco Civil da Internet, de forma a evitar conflitos entre as duas leis.

> **A LGPD, PORÉM, REGULA TODAS AS ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS, INCLUSIVE NOS MEIOS DIGITAIS**

CAPÍTULO XVI

SIGILO BANCÁRIO E COMPARTILHAMENTO DE DADOS COM TERCEIROS

Ponto importante de atenção é o compartilhamento de dados pessoais com terceiros (cobrança, advogados, correspondentes no País).

A Lei de Sigilo Bancário contem disposições bastante amplas e estabelece que as instituições financeiras devem manter sigilo em todas as suas operações ativas, passivas e serviços prestados. Para que informações possam ser fornecidas nos termos da lei, o compartilhamento deve ocorrer segundo alguma das exceções legais que autorizam as instituições financeiras a fornecer as informações ou mediante autorização expressa do titular das informações.

Assim, de maneira geral, o compartilhamento de informações com terceiros deve ser precedido de consentimento do interessado. Entretanto, na prática, nem sempre existe autorização expressa em todas as situações em que as instituições financeiras prestam serviços a seus clientes que demandam a participação de terceiros (como transações realizadas por meio de correspondentes no País). Também existem situações em que instituições financeiras precisam compartilhar as informações para proteger seus próprios interesses legítimos (como situações em que instituições financeiras precisam compartilhar informações com advogados ou empresas de cobrança).

Via de regra, pode-se dizer que estes compartilhamentos seriam razoáveis caso seja necessário que o terceiro receba a informação e caso apenas receba as informações necessárias para realizar a atividade. É importante, no entanto, ressaltar que as diversas situações precisam ser analisadas na prática em vista dos termos da Lei de Sigilo Bancário de forma a avaliar sua legalidade. Também é recomendável que os terceiros que recebem estas informações concordem em manter o sigilo das informações e sigam as políticas de privacidade da instituição financeira.

Por fim, vale mencionar que a Resolução 3.954/2011, a qual trata dos correspondentes no País, determina no artigo 8º, parágrafo único, que o contrato de correspondente pode prever a prestação de serviços complementares de coleta de informações cadastrais e de documentação, bem como controle e processamento de dados. Desta forma, percebe-se que a própria regulamentação bancária reconhece que correspondentes podem coletar informações para a prestação de seus serviços.

“ENTRETANTO, NA PRÁTICA, NEM SEMPRE EXISTE AUTORIZAÇÃO EXPRESSA EM TODAS AS SITUAÇÕES EM QUE AS INSTITUIÇÕES FINANCEIRAS PRESTAM SERVIÇOS A SEUS CLIENTES QUE DEMANDAM A PARTICIPAÇÃO DE TERCEIROS (COMO TRANSAÇÕES REALIZADAS POR MEIO DE CORRESPONDENTES NO PAÍS)”

CAPÍTULO XVII

CHECKLIST

Até agosto de 2020, as sociedades de crédito, financiamento e investimento precisam adaptar seus processos à LGPD. As seguintes medidas são os primeiros passos para esse projeto de adequação:

- [ ] Fazer um mapeamento geral de todas as atividades que envolvem tratamentos de dados pessoais, incluindo processos de coleta, armazenamento e compartilhamento, verificando, também, se há tratamento de dados pessoais sensíveis.

- [ ] Definir as bases legais mais apropriadas para o tratamento de dados, conforme a finalidade específica (consentimento, legítimo interesse, execução de contrato, cumprimento de obrigação legal ou regulatória, proteção ao crédito, etc).

- [ ] Analisar se há discrepâncias entre as obrigações legais e as atividades da empresa e definir quais estratégias adotar para adequação.

- [ ] Alocar responsabilidades internas para execução das ações necessárias.

- [ ] Implementar ferramentas que permitam aos titulares de dados pessoais exercerem seus direitos garantidos pela LGPD

- [ ] Elaborar, revisar, adaptar e aditar contratos que envolvam tratamento e/ou compartilhamento de dados pessoais, tanto nas relações com usuários e consumidores, quanto nas relações com fornecedores e parceiros comerciais.

- [ ] Elaborar relatórios de impacto à proteção de dados pessoais nos casos de tratamento baseado em legítimo interesse e em outras situações em que isso seja recomendável.

- [ ] Elaborar e revisar políticas internas, planos de resposta a incidentes e outros documentos sobre privacidade e proteção de dados pessoais.

- [ ] Revisar e implementar técnicas e procedimentos de segurança da informação e programas de privacidade desde a concepção e como padrão *(privacy by design/by default).*

- [ ] Estabelecer um programa de governança em proteção de dados pessoais.

ANOTAÇÕES

ACREFI

A CASA DO CRÉDITO DESDE 1958

ACREFI

COMPARTILHANDO CONHECIMENTO

Rua Líbero Badaró, 425 – 28º andar – São Paulo – SP
Tel.: (11) 3107-7177 Fax: (11) 3106-6082
www.acrefi.org.br