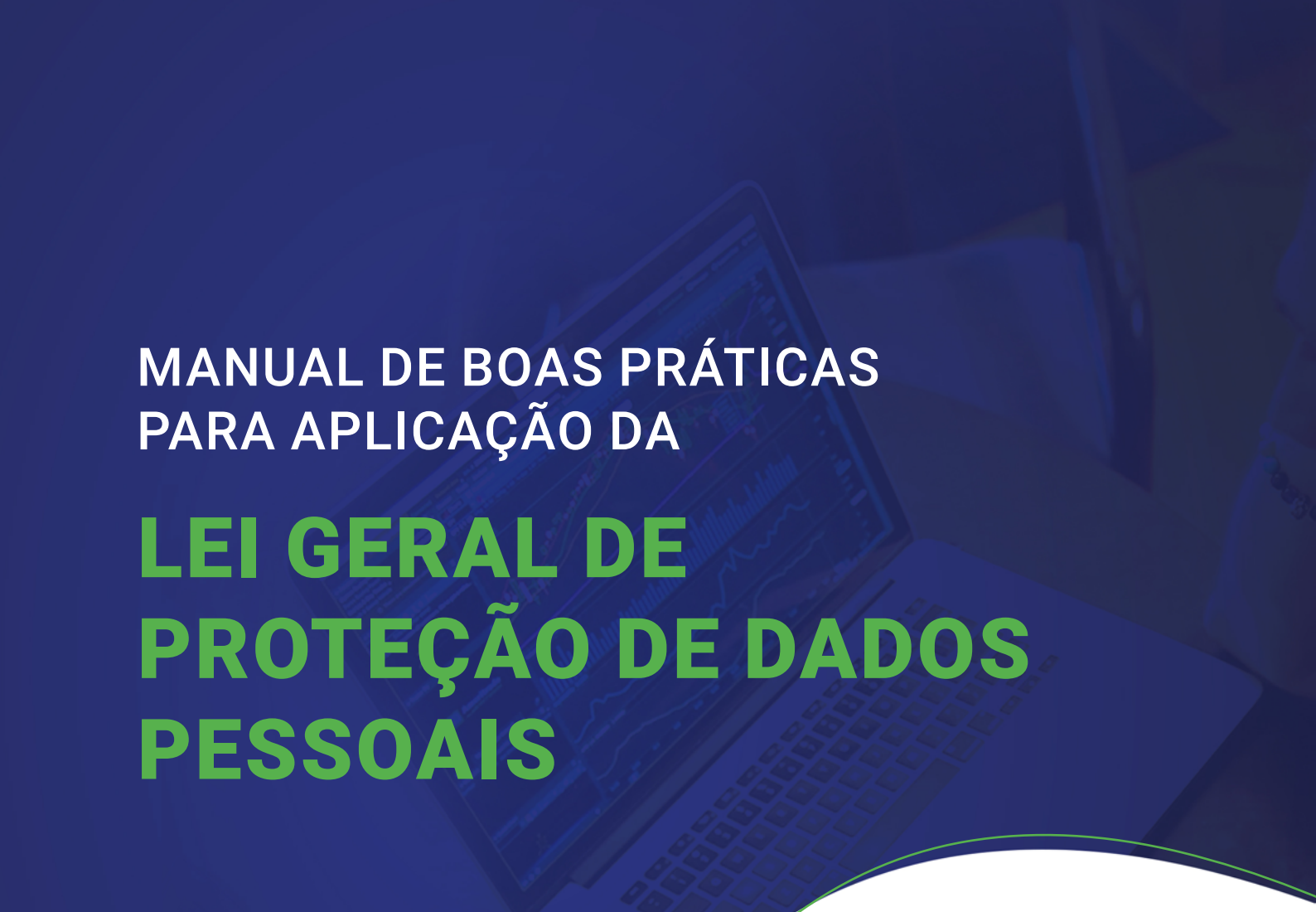


MANUAL DE BOAS PRÁTICAS
PARA APLICAÇÃO DA

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

acrefi
ASSOCIAÇÃO NACIONAL
DAS INSTITUIÇÕES DE CRÉDITO,
FINANCIAMENTO E INVESTIMENTO

FENAUTO

Elaborado em agosto de 2019 por *Pinheiro Neto Advogados*
Atualizado e Ampliado em agosto de 2022 por *Peck Advogados*

Presidente da ACREFI: Luis Eduardo da Costa Carvalho

Diretor Superintendente da ACREFI: Carlos Alberto Marcondes Machado

Presidente da FENAUTO: Enilson Espinola Sales de Sousa

Diretor Executivo da FENAUTO: Dilson Motta

Coordenação: Cintia M. Ramos Falcão - Consultora Jurídica

Direção de Arte: Renan K. Ciniello - Ciniello Design

ÍNDICE

Nos novos tempos, a união de forças tornou-se essencial, ainda mais quando falamos da disseminação do conhecimento e da boa informação. Nesta 2ª edição do Manual LGPD, a ACREFI une-se com a FENAUTO para compartilharem, juntas, as mais recentes atualizações que envolvem a Lei Geral de Proteção de Dados. São orientações importantes, que fazem parte do dia a dia do mercado financeiro e dos inúmeros revendedores de veículos automotores, localizados nos mais diversos pontos do País.

O Manual LGPD destaca atualizações significativas na Lei Geral de Proteção de Dados – aprovada pelo Congresso em 2018 e em vigor desde 14 de agosto de 2020 – bem como apresenta os aspectos gerais da legislação e das disposições relevantes, aplicáveis às sociedades de crédito, financiamento e investimento e aos revendedores de veículos automotores.

A LGPD representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataformas digitais. Além de alterar o padrão de como instituições privadas coletam, armazenam e compartilham informações de usuários. Por estar a LPGD tão intimamente ligada ao ambiente digital que, por sua vez, é sujeito aos constantes avanços da tecnologia, nada mais apropriado do que a edição atualizada deste manual.

Boa leitura!

Luis Eduardo da Costa Carvalho
Presidente da ACREFI

Enilson Sales
Presidente da FENAUTO

SOBRE ESTE MANUAL

Este manual foi desenvolvido para a Associação Nacional das Instituições de Crédito, Financiamento e Investimento (ACREFI) e para a Federação Nacional das Associações dos Revendedores de Veículos Automotores (FENAUTO), e busca apresentar pontos de atenção e aspectos da legislação aplicável relacionada à privacidade e à proteção de Dados Pessoais, principalmente a Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais ("LGPD"), atualizada pela Lei nº 13.853/2019 e Lei 14.010/2020, bem como as portarias e resoluções da Autoridade Nacional de Proteção de Dados (ANPD).

A análise, além de apresentar os aspectos gerais da legislação, trará as disposições relevantes aplicáveis às sociedades de crédito, financiamento e investimento, bem como aos revendedores de veículos automotores, tendo em vista as obrigações da (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"); (iii) Resolução CMN nº. 4.893, de 26 de fevereiro de 2021 ("Resolução CMN nº 4893/21"); (iv) Resolução CMN nº 4.935, de 29 de julho de 2021 ("Resolução CMN nº 4935/21"); e (v) Resolução Conjunta nº 1, de 04 de maio de 2020 ("Resolução Conjunta nº 1/20"). Em conjunto, as legislações acima serão chamadas, nesse manual, de "Regulamentação Setorial".

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

CAPÍTULO I
VISÃO GERAL DA LGPD E DA REGULAMENTAÇÃO SETORIAL

LGPD:

A LGPD é a primeira legislação específica, no Brasil, a tratar sobre o tema de proteção de Dados Pessoais. Inicialmente publicada em agosto de 2018, ela entrou em vigor apenas 2 anos depois, em agosto de 2020, devido ao reconhecimento da complexidade das ações que precisavam ser tomadas pelas empresas para a adequação de suas atividades.

Em agosto de 2021, um ano após sua entrada em vigor, passaram a valer as penalidades previstas na LGPD, que até então não poderiam ser aplicadas.

É importante ressaltar que a LGPD não foi criada para proibir o uso dos dados, mas sim para regulamentar e estabelecer as condições e requisitos 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.

A responsabilidade pela fiscalização do cumprimento da LGPD é da Autoridade Nacional de Proteção de Dados ("ANPD"), criada em 2018 por meio da Medida Provisória nº 869/2018, posteriormente convertida na Lei 13.853/2019.

A LGPD É UMA LEI DE PROTEÇÃO DE DADOS PESSOAIS E NÃO DE PROIBIÇÃO DE TRATAMENTO DE INFORMAÇÕES, POIS SÃO ESSENCIAIS NAS RELAÇÕES ENTRE INDIVÍDUOS E INSTITUIÇÕES!

REGULAMENTAÇÃO SETORIAL:

Lei de Sigilo Bancário

Instituições financeiras, incluindo-se as sociedades de crédito, financiamento e investimento, devem manter sigilo em suas operações ativas e passivas e serviços prestados.
Em regra, a Lei de Sigilo Bancário autoriza o compartilhamento de informações apenas quando o cliente autorizar, ressalvadas as possibilidades de compartilhamento sem a necessidade de autorização, como nos casos de troca de informações sobre emitentes de cheques sem fundo, devedores inadimplentes, sobre as informações da Lei de Cadastro Positivo, ou para as comunicações de práticas de ilícitos às autoridades competentes.

> A Lei de Sigilo Bancário também permite que o Banco Central do Brasil ("BACEN") ou a Comissão de Valores Mobiliários ("CVM") 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 BACEN estabeleceram que as instituições financeiras devem, entre outras obrigações, manter todos os cadastros atualizados de seus clientes, além de manter registros das transações realizadas em valores superiores a limites pré-definidos pelas autoridades competentes.

A criação e manutenção desses cadastros, nos termos a LGPD, podem ser fundamentadas na Base Legal de cumprimento de obrigação legal ou regulatória, conforme será melhor abordado no Capítulo VIII deste Manual.

Resoluções sobre Segurança Cibernética

A Resolução CMN nº 4893/21 substituiu a antiga Resolução CMN nº 4658/18, trazendo novas disposições sobre o gerenciamento de riscos cibernéticos e sobre o tratamento de dados em nuvem para as instituições financeiras.

Especificamente para as instituições de pagamento autorizadas a funcionar pelo BACEN, o gerenciamento de riscos cibernéticos e processamento de dados em nuvem é regulamentado pela Resolução BCB nº 85, de 8 de abril de 2021.

As resoluções acima mencionadas estabelecem os critérios para a implementação da "Política de Segurança Cibernética", trazendo os requisitos mínimos que devem estar presentes. Além disso, o BACEN estabelece a necessidade de divulgação da Política

de Segurança Cibernética, seja para o público interno (funcionários) ou para o público externo (prestadores de serviços), além de um resumo dos principais pontos para os clientes.

Resolução sobre Correspondentes no País

Em vigor desde fevereiro de 2022, a Resolução CMN nº 4935/21 trouxe novas disposições relacionadas à contratação de correspondentes no país, comumente chamados de Correspondentes Bancários, pelas instituições autorizadas a funcionar pelo BACEN. Esse tópico será abordado com mais detalhes no Capítulo VI – Correspondentes no país – do presente manual.

Resolução do *Open Finance*

Além das resoluções acima citadas, a Resolução Conjunta nº 1/2020, que dispõe sobre a implementação do Open Finance no Brasil também pode ser aplicada, desde que os associados da ACREFI se enquadrem na categoria de participantes obrigatórios definidos pela resolução ou decidam ingressar no ambiente como participantes voluntários.

O Open Finance tem como objetivo ser um ambiente de dados abertos, para incentivar a inovação, promover a concorrência e a cidadania financeira e aumentar a eficiência do Sistema Financeiro Nacional e do sistema de pagamentos brasileiro.

Para poder tratar os Dados Pessoais que eventualmente sejam compartilhados no Open Finance, a entidade regulada deverá solicitar o consentimento do Titular, que então poderá autorizar ou não o compartilhamento de seus Dados Pessoais. Contudo, é importante ressaltar que o consentimento autoriza apenas e tão somente o compartilhamento dos dados entre as instituições, sendo que qualquer Tratamento posterior deverá estar fundamentado em alguma das Bases Legais previstas na LGPD.

Além de observar os requisitos da LGPD e as demais regulamentações do BACEN e CVM, é imprescindível que os participantes do Open Finance também observem as disposições do manual de segurança do Open Finance, que traz os requisitos de segurança que devem ser adotados no âmbito do Open Finance.

CAPÍTULO II

POR QUE A LGPD INTERESSA ÀS ASSOCIADAS ACREFI, FENAUTO E DEMAIS INSTITUIÇÕES AUTORIZADAS PELO BACEN

A LGPD tem um extenso âmbito de aplicação, sendo exigível em qualquer operação de Tratamento de Dados Pessoais (i) realizada no Brasil ou relacionada a Dados Pessoais de pessoas naturais que se encontram no Brasil quando da coleta dos dados, ou (ii) 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: toda atividade que envolver o Tratamento de Dados Pessoais em meios físicos ou de forma presencial também deverão estar adequadas à legislação, como no caso de Dados Pessoais coletados durante o processo de abertura de contas em agências físicas.

No contexto financeiro, as atividades de crédito, financiamento e investimento frequentemente envolvem Tratamento e compartilhamento de Dados Pessoais, sendo que as atividades 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; (ii) o compartilhamento de Dados Pessoais no contexto de análise de risco de crédito é comum; (iii) para cadastrar os consumidores nas plataformas (digitais ou internas) 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 SE APLICA A TODO TIPO DE DADO PESSOAL, EM QUALQUER TIPO DE SUPORTE, SEJA FÍSICO OU DIGITAL.

Além dos impactos nas atividades principais, a LGPD também traz mudanças nas rotinas operacionais das empresas. Um exemplo é o direito que a LGPD garante aos Titulares de poder solicitar o acesso aos seus Dados Pessoais mantidos pelas empresas, o que faz necessária a implementação de ferramentas e mecanismos para atender a essas solicitações.

Será também necessário, por exemplo, estabelecer rotinas para receber as solicitações de correção, atualização ou complementação dos Dados Pessoais dos Titulares, para

A LGPD DEVE SER OBSERVADA POR TODAS AS EMPRESAS QUE TRATAM DADOS PESSOAIS NO BRASIL, SE MOSTRANDO MAIS DO QUE UMA SIMPLES VANTAGEM COMPETITIVA, MAS SIM COMO UMA EXIGÊNCIA DOS TITULARES.

a correção de Dados Pessoais que se mostrarem desatualizados, incorretos ou incompletos, ou mesmo para operacionalizar as solicitações de portabilidade dos Dados Pessoais para outro fornecedor de serviços.

É importante ressaltar que os impactos da LGPD vão além da relação com os clientes de cada empresa.

Os funcionários das empresas também são Titulares de Dados Pessoais e, da mesma forma que os clientes, têm seus direitos garantidos pela legislação. Contudo, os próprios funcionários também possuirão acesso aos Dados Pessoais de seus colegas e dos clientes da instituição, o que torna necessária a instituição de regras para o Tratamento dos Dados Pessoais pelos colaboradores, a adequação dos contratos de trabalho para inclusão de cláusulas de proteção de dados pessoais e de confidencialidade, e o fornecimento das informações sobre os Tratamentos realizados com os Dados Pessoais dos colaboradores, observando o princípio da transparência.

A adequação à LGPD é mais do que uma obrigação legal para reduzir os riscos de multas; é uma vantagem competitiva.

O próprio mercado, em efeito cascata, cobra a adequação à LGPD como um requisito mínimo para a escolha de parceiros de negócio e para o estabelecimento e a manutenção de relacionamento comercial entre instituições financeiras.

Além disso, os históricos e passivos decorrentes de descumprimento das obrigações estabelecidas pela LGPD também poderão ser fatores determinantes no âmbito da captação de investimentos e em operações de fusão e aquisição.

Em abril de 2022, o Banco da Irlanda foi multado pela autoridade irlandesa de proteção de dados em €463 mil (aprox. R$ 2,5 milhões) após uma investigação da autoridade relacionadas a um incidente de segurança. A investigação mostrou que, devido a uma falha nos sistemas do banco, foram compartilhadas informações falsas dos Titulares com a Central de Registro de Crédito irlandesa, podendo causar impactos negativos no histórico de crédito dos Titular. Ainda de acordo com a autoridade irlandesa, o incidente ocorreu devido a adoção de medidas técnicas e organizacionais inadequadas para a garantir a segurança da informação por parte do banco*.

***Fonte:** https://www.independent.ie/business/technology/bank-of-ireland-fined-over-errors-reporting-details-of-47000-customers-loans-41522333.html#:~:text=Bank%20of%20Ireland%20has%20been,have%20affected%20their%20credit%20ratings

CAPÍTULO III
DEFINIÇÕES E CONCEITOS

Agentes de Tratamento: o Controlador e o Operador.

Algoritmo: sequência de instruções ou comandos realizados de maneira sistemática, por meio de dispositivos eletrônicos, com o objetivo de executar uma tarefa. Exemplo: o conjunto de regras utilizadas para definir, com base nos Dados Pessoais informados, o score de crédito de um Titular.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do Tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

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

Controlador conjunto: Controlador que, em conjunto com outro(s) Controlador(es), possui a competência para tomar decisões sobre o Tratamento de Dados Pessoais em determinada atividade de Tratamento da qual todos participam.

Controlador singular: Controlador que, apesar de possuir relação com outro(s) Controlador(es), possui a competência exclusiva para tomar as decisões relativas às suas próprias atividades de Tratamento de Dados Pessoais.

Dado Anonimizado: Dado Anonimizado é o dado que não pode ser associado a um Titular, perdendo completamente a possibilidade de identificá-lo. É importante notar que a anonimização do Dado Pessoal deve ser irreversível, isto é, não pode voltar a identificar o Titular após a utilização de meios técnicos razoáveis disponíveis na ocasião do Tratamento. Exemplo: informações meramente estatísticas extraídas de uma base de Dados Pessoais.

Dado Pessoal: é qualquer informação relacionada a uma pessoa natural identificada ou identificável. Qualquer dado que permita, sozinho ou em conjunto com outros dados, a identificação de um Titular será considerado como Dado Pessoal. Exemplo: nome, RG, CPF, endereço, histórico de compras etc.

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. Exemplo: cliente PCD, religião, impressão digital, biometria facial etc.

Decisão Automatizada: são as decisões tomadas, no Tratamento de Dados Pessoais, unicamente por meio de Algoritmos ou inteligência artificial, sem a participação humana no resultado do Tratamento. Exemplo: definição de score de crédito com base em Dados Pessoais imputados no sistema.

Incidente: uma violação na confidencialidade, integridade ou disponibilidade de dados ou informações, como o acesso ou divulgação não autorizados, a destruição, perda ou alteração. Exemplo: vazamento de Dados Pessoais.

Operador: é a pessoa natural ou jurídica, de direito público ou privado, que realiza o Tratamento de Dados Pessoais em nome do Controlador. Exemplo: serviço de armazenamento em nuvem contratado pela instituição financeira.

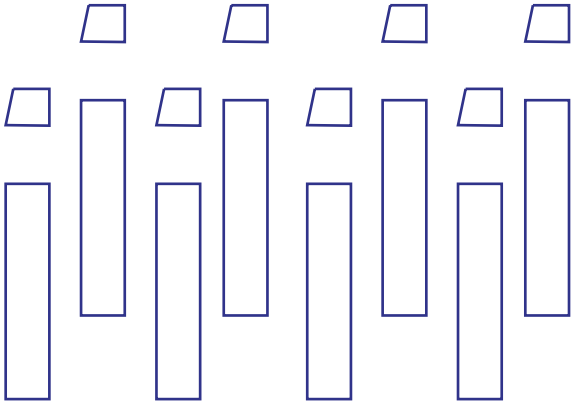
Relatório de Impacto à Proteção de Dados Pessoais ("RIPD"): documentação do Controlador que contém a descrição das atividades de Tratamento de Dados Pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos Titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Titular: é a pessoa natural a quem um Dado Pessoal se refere. Exemplo: clientes e colaboradores.

Tratamento: é qualquer operação realizada com Dados Pessoais, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Exemplo: envio de planilha com Dados Pessoais por e-mail.

CAPÍTULO IV
PRINCÍPIOS GERAIS DA LGPD

Um dos artigos mais importantes da LGPD é seu artigo 6º, que trata dos princípios de Tratamento de Dados Pessoais, equivalente ao artigo 5º do Regulamento Geral de Proteção de Dados da União Europeia (General Data Protection Regulation ou "GDPR"). Isso porque o artigo 6º determina que estará de boa-fé o agente que tratar os dados cumprindo com os princípios elencados pela lei.



OS PILARES PRINCIPAIS DA LGPD SÃO: TRANSPARÊNCIA, MINIMIZAÇÃO E SEGURANÇA!

A LGPD estabelece alguns princípios que se aplicam a todas as atividades de Tratamento de Dados Pessoais. São valores gerais que orientam a compreensão, interpretação e aplicação das regras estabelecidas pela LGPD e que devem sempre ser considerados, desde o início da atividade, quando esta envolver o Tratamento de Dados Pessoais.

Princípio	Definição da LGPD	Principal impacto	Exemplo
Finalidade	*"Realização do Tratamento para propósitos legítimos, específicos, explícitos e informados ao Titular, sem possibilidade de Tratamento posterior de forma incompatível com essas finalidades".*	Definir previamente, registrar e monitorar as finalidades de cada atividade de Tratamento realizada, além de informar ao Titular a finalidade (o porquê) do Tratamento.	Definir que uma das atividades de Tratamento terá como objetivo o envio de comunicação sobre produtos de investimento disponíveis aos clientes, por e-mail.

Adequação	*"Compatibilidade do Tratamento com as finalidades informadas ao Titular, de acordo com o contexto do Tratamento".*	Verificar se o Tratamento é adequado ao contexto em que os Dados Pessoais foram coletados, ou seja, se a atividade está em linha com as expectativas que o Titular possuía ao fornecer os seus Dados Pessoais.	Assegurar que o Tratamento ocorrerá mediante o envio de e-mail contendo informações sobre os produtos de investimento, eliminando as demais informações não relacionadas.
Necessidade	*"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".*	Avaliar se os Dados Pessoais tratados são realmente necessários para atingir aquela finalidade ou se é possível chegar no mesmo resultado utilizando menos Dados Pessoais.	Definir que serão tratados os seguintes Dados Pessoais: nome, e-mail, endereço (para encaminhamento à agência mais próxima) e perfil de investidor.
Livre Acesso	*"Garantia, aos Titulares, de consulta facilitada e gratuita sobre a forma e a duração do Tratamento, bem como sobre a integralidade de seus Dados Pessoais".*	Organizar os Dados Pessoais dos Titulares de forma que a busca para atender a um pedido de consulta de um Titular seja facilmente realizada, além de sempre possuir as informações atualizadas sobre os Tratamentos.	Fornecer o relatório completo, se solicitado pelo Titular, com a totalidade dos Dados Pessoais que o Controlador possui.
Qualidade dos dados	*"Garantia, aos Titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu Tratamento".*	Estabelecer um procedimento de atualização dos Dados Pessoais mediante solicitação dos Titulares, definindo as etapas para recepção do pedido e validação das alterações informadas.	O e-mail armazenado pelo Controlador está desatualizado (refere-se a uma conta antiga que o Titular não possui mais acesso), e o Titular solicita a alteração para o novo e-mail.

Transparência	*"Garantia, aos Titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do Tratamento e os respectivos Agentes de Tratamento, observados os segredos comercial e industrial".*	Elaborar documentos direcionados aos Titulares e disponibilizá-los no site e/ou em outros locais adequados, considerando a atividade de Tratamento, e assegurar que os Titulares sempre serão informados das alterações relevantes na finalidade e/ou forma do Tratamento.	Informar, em contratos e na Política de Privacidade, que a comunicação sobre possibilidades de investimento será realizada. *"Podemos utilizar seus Dados Pessoais para apresentarmos possibilidades de investimento que se adequarem ao seu perfil de investidor."*
Segurança	*"Utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".*	Adotar medidas de segurança compatíveis com o Tratamento, e revisar as medidas de segurança eventualmente existentes para validação. Adotar medidas de mitigação de riscos e danos em casos de Incidentes.	Proteger a lista de e-mails em servidor seguro, e adotar medidas técnicas e organizacionais de segurança no envio de e-mails (como utilizar um servidor seguro para o envio).
Prevenção	*"Adoção de medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais".*		Elaborar um estudo para entender se existe risco de causar danos aos Titulares com o Tratamento.
Não Discriminação	*"Impossibilidade de realização do Tratamento para fins discriminatórios ilícitos ou abusivos".*	Revisar as finalidades, objetivos e consequências práticas do Tratamento para assegurar a inexistência de discriminação ilícita ou abusiva.	Enviar o mesmo e-mail com as possibilidades para todos os Titulares com o mesmo perfil de investidor.

Responsa-bilização e Prestação de Contas	*"Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas"*.	Criar evidências relacionadas à adoção de medidas para cumprimento da LGPD, registrando, por exemplo, políticas adotadas, decisões tomadas pela diretoria, indicadores de atendimento aos Titulares, índices de Incidentes evitados e similares.	Armazenar todos os documentos relacionados com a atividade de Tratamento e apresentá-los à ANPD se solicitado.

CAPÍTULO V
AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Controlador e Operador

As instituições financeiras possuem responsabilidades no Tratamento dos Dados Pessoais de seus clientes e colaboradores. Na maioria dos fluxos, são enquadradas como controladoras e devem se atentar às obrigações trazidas na LGPD. A LGPD traz a figura de dois Agentes de Tratamento: o Controlador e o Operador.

O Controlador é a pessoa natural ou jurídica, de direito público ou privado, que exerce controle geral sobre as finalidades para as quais e as maneiras pelas quais os Dados Pessoais serão tratados.

O CONTROLADOR "MANDA", TOMANDO AS DECISÕES E ASSUMINDO A RESPONSABILIDADE SOBRE O TRATAMENTO.

Em outras palavras, a competência para decidir o **"porquê"** e o **"como"** da atividade de Tratamento é do Controlador, sendo ele o Agente de Tratamento responsável por todo o ciclo de vida dos Dados Pessoais– da sua coleta à sua exclusão. Na maioria dos fluxos, as instituições financeiras e de pagamento serão Controladoras dos Dados Pessoais.

Como consequência da posição como 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.

O OPERADOR "OBEDECE", E ATUA EM NOME DE UM CONTROLADOR E SEGUINDO SUAS INSTRUÇÕES.

Já 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 de Dados Pessoais compartilhados pelo Controlador, devendo tratar tais dados apenas 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 conceda ao Operador um certo grau de discricionariedade e liberdade sobre o processo de Tratamento, permitindo que tome determinadas decisões sobre o modo com que os Dados Pessoais serão tratados. Nesse sentido, o Operador poderá definir, por exemplo, os aspectos técnicos relativos a como um serviço específico será prestado, como a escolha do software e equipamentos que serão utilizados e o detalhamento das medidas de segurança que serão aplicadas.

Contudo, o Controlador poderá exigir do Operador um nível mínimo de medidas de segurança a serem implementadas, já que o Controlador continuará sendo responsável pela proteção dos Dados Pessoais tratados e pela conformidade da operação com a LGPD. Em qualquer cenário, o Operador deverá agir apenas dentro dos limites permitidos e das finalidades determinadas pelo Controlador.

Para auxiliar o entendimento quanto ao posicionamento das partes enquanto Agentes de Tratamento, considere os seguintes exemplos abaixo:

Uma instituição financeira contrata um sistema de CRM (*Customer Relationship Management*) de um fornecedor. O fornecedor está em uma posição de Operador da instituição financeira, pois prestará o serviço em nome e para a instituição, não tendo controle ou titularidade sobre os dados que ali trafegam, apenas sobre o sistema em si.

Uma loja de venda de automóveis contrata um prestador de serviço para realizar o armazenamento de documentos, dados e informações em servidores externos, a chamada "nuvem". Nessa situação, o prestador de serviços apenas disponibiliza o servidor e o espaço de armazenamento, não possuindo controle sobre os documentos lá guardados, não podendo decidir sobre a exclusão de nenhum deles. Assim, o prestador de serviços atua como Operador da loja, que é a Controladora neste caso.

A LGPD define diferentes responsabilidades para os Agentes de Tratamento, atribuindo a maioria das obrigações ao Controlador, que deverá ser responsável pela conformidade das atividades de Tratamento de Dados Pessoais sob seu controle.

Em resumo, a LGPD estipula as seguintes obrigações aos Agentes de Tratamento:

Controlador	Operador
• *Definir meios, formas, duração etc. sobre o Tratamento;* • *Atribuir as bases legais às atividades de Tratamento de Dados Pessoais;* • *Demonstrar que o consentimento foi obtido em conformidade com a LGPD;* • *Disponibilizar as informações sobre o Tratamento dos Dados Pessoais e informar os Titulares em casos de alteração;* • *Assegurar que o consentimento para Tratamento de Dados de Crianças foi fornecido pelos pais ou responsável legal;* • *Recepcionar e tratar as solicitações de Direitos dos Titulares;* • *Fornecer informações sobre critérios e procedimentos da decisão automatizada;* • *Oferecer garantias nos casos de transferências internacionais;* • *Criar, manter e atualizar o Registro das Operações de Tratamento;* • *Elaborar RIPDs;* • *Fornecer as instruções de Tratamento ao Operador;* • *Indicar o Encarregado;* • *Adotar medidas de segurança, técnicas e administrativas;* • *Garantir a Segurança da Informação;* • *Comunicar incidentes à ANPD e aos Titulares;* • *Adotar regras de boas práticas e de governança;* • *Demonstrar a efetividade do Programa de Governança em Privacidade;* • *Reparação de danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de Dados Pessoais.*	• *Realizar o Tratamento em nome do Controlador;* • *Criar, manter e atualizar o Registro das Operações de Tratamento de Dados Pessoais;* • *Obedecer às instruções lícitas do Controlador;* • *Adotar medidas de segurança, técnicas e administrativas;* • *Garantir a Segurança da Informação.*

A POSIÇÃO DOS AGENTES DE TRATAMENTO NÃO É ESTÁTICA! TODA RELAÇÃO ENTRE DOIS AGENTES DE TRATAMENTO PRECISA SER ANALISADA PARA IDENTIFICAR AS POSIÇÕES ASSUMIDAS.

Independentemente das obrigações acima listadas, é importante ressaltar que a adoção de um Programa de Governança em Privacidade e das regras de boas práticas é interessante a todas as empresas, uma vez que as figuras de Controlador e Operador não são estáticas, isto é, variam de acordo com a atividade concreta de Tratamento analisada. Por exemplo: uma empresa que presta serviço de armazenamento em nuvem para outras empresas poderá atuar como Operadora nesta prestação de serviços, mas ainda será considerada a Controladora dos Dados Pessoais de seus próprios funcionários.

Pluralidade de Controladores

Apesar de a LGPD prever apenas as figuras do Controlador e do Operador, nem toda relação entre duas empresas terá cada uma em um papel enquanto Agente de Tratamento. É possível a existência de uma relação entre dois ou mais Controladores, na qual uma parte não se submete às instruções da outra no Tratamento de Dados Pessoais.

Essa relação entre dois ou mais Controladores, não prevista na LGPD, foi trazida para o cenário da LGPD por meio do Guia Orientativo sobre Agentes de Tratamento e Encarregado, elaborado pela ANPD. No guia, a ANPD prevê duas formas de existência de uma relação entre uma pluralidade de Controladores: (i) a controladoria conjunta e (ii) a controladoria singular.

CONTROLADORES CONJUNTOS POSSUEM RESPONSABILIDADE SOLIDÁRIA SOBRE O TRATAMENTO! AMBOS RESPONDEM PELOS DANOS CAUSADOS AOS TITULARES E A TERCEIROS.

De acordo com a definição da ANPD, a controladoria conjunta é *"a determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD"*.

Para avaliar a existência de controladoria conjunta, é necessário que ocorram os três requisitos indicados na figura abaixo:

- **Dois ou mais Controladores com poder de decisão sobre o tratamento;**
- **Interesse mútuo dos Controladores envolvidos sobre o mesmo tratamento;**
- **Caráter comum ou convergente das decisões conjuntas relacionadas ao tratamento.**

A controladoria singular existirá nas situações em que um ou mais dos requisitos da controladoria conjunta não for identificado.

Como exemplo de controladoria conjunta, pode-se citar o seguinte cenário: Banco e Concessionária instituem uma parceira especial para ofertar o financiamento de veículos a seus clientes. Tanto o Banco quanto a Concessionária querem atingir o maior número possível de Titulares e, para isso, decidem compartilhar entre si os respectivos bancos de dados de clientes e leads. Para operacionalizar a divulgação do produto, as empresas contratam a Agência de Publicidade, que fará o disparo das comunicações e recebeu instruções de ambas sobre qual o perfil do público-alvo desejado e outras características do Tratamento.

Nesse cenário, Banco e Concessionária são classificados como Controladores conjuntos, uma vez que:

(i) ambos são Controladores (ou seja, ambos possuem poder de decisão na operação);

(ii) ambos possuem interesse mútuo na operação de Tratamento (divulgar o novo financiamento especial para seus clientes), mas cada uma possui uma finalidade própria (o Banco quer fidelizar novamente seus clientes que possuem um financiamento de veículo e angariar novos financiamentos, enquanto a Concessionária quer alavancar suas vendas); e

(iii) as decisões tomadas pelo Banco e Concessionária são convergentes (isso é, as decisões se complementam de forma única para a realização da atividade de Tratamento).

Ainda, a Agência de Publicidade atuará como Operadora do Banco e da Concessionária, já que poderá tratar os Dados Pessoais apenas dentro das finalidades e limites definidos pelos Controladores (Banco e Concessionária).

Quando uma relação não for caracterizada como controladoria conjunta, ou seja, quando um dos requisitos acima não estiverem presentes, estaremos diante de uma controladoria singular, que é classificada como uma situação residual da controladoria conjunta. Como exemplo de controladoria singular, pode-se citar os exemplos abaixo:

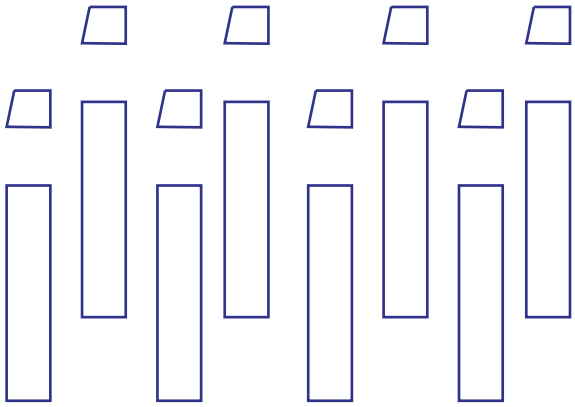
Uma instituição financeira está com dificuldade de entrar em contato com seus clientes inadimplentes, e decide utilizar o serviço de enriquecimento de dados de um bureau de crédito. Nesse caso, ambas as partes possuem a competência para decidir sobre o Tratamento dos Dados pessoais, cada um no âmbito de sua própria atividade. Assim, ambos são considerados como Controladores, mas em uma relação de controladoria singular, já que não há interesse comum ou decisões convergentes entre as partes na atividade de Tratamento;

A relação entre a concessionária de veículos e a montadora será uma relação de controladoria singular, uma vez que ambas as partes possuem competência para tomar decisões sobre o Tratamento, mas realizam os Tratamentos para finalidades próprias, de acordo com seus próprios interesses.

Agentes de Tratamento de Pequeno Porte

Para finalizar o capítulo, é necessário abordar sobre os Agentes de Tratamento de Pequeno Porte, um novo enquadramento dos Agentes de Tratamento em relação a seu porte, conforme regulado pela Resolução CD/ANPD nº 02, de 27 de janeiro de 2022 (“Resolução CD/ANPD nº 02/22”).

MESMO SE FOR ENQUADRADA COMO UM AGENTE DE TRATAMENTO DE PEQUENO PORTE, A INSTITUIÇÃO DEVE CUMPRIR A LGPD!



É importante ressaltar que **esse enquadramento diz respeito apenas quanto ao porte do Agente de Tratamento, não existindo a criação de uma nova figura além do Controlador e do Operador.** Ou seja, um Controlador poderá ser classificado como um Controlador de Pequeno Porte; o Agente de Tratamento continuará sendo classificado como Controlador ou como Operador, apenas possuindo um porte empresarial distinto das grandes empresas e conglomerados.

Os Agentes de Tratamento de Pequeno Porte podem ser microempresas, empresas de

pequeno porte e startups, inclusive quando não possuírem fins lucrativos. A resolução traz, ainda, a definição de microempresa, empresa de pequeno porte e startups, de forma delimitar o seu escopo de aplicação.

Há situações que afastarão a flexibilização das regras, mesmo se diante de MEI, microempresas, empresas de pequeno porte, startups, dentre outros. São elas: (i) a realização de Tratamento de Dados Pessoais considerado de alto risco; (ii) o auferimento de receita bruta superior aos limites legais estabelecidos para cada categoria de empresa; ou (iii) o pertencimento do Agente de Tratamento de Pequeno Porte a grupo econômico cuja receita global ultrapasse os limites estabelecidos por lei para microempresas, empresas de pequeno porte ou startups.

Os dois últimos requisitos são critérios objetivos vinculados à receita, seja do Agente de Tratamento de Pequeno Porte, seja do grupo econômico ao qual está vinculado. Contudo, o primeiro critério de exclusão foi trazido especificamente pela Resolução CD/ANPD nº 02/22, criando o conceito de Tratamento de alto risco, o qual deverá ser avaliado no caso concreto.

A resolução trouxe duas categorias de critérios, os critérios gerais e os critérios específicos, representados na tabela abaixo:

Critérios Gerais	Critérios Específicos
Tratamento de Dados Pessoais em larga escala	Uso de tecnologias emergentes ou inovadoras
	Vigilância ou controle de zonas acessíveis ao público
Tratamento de Dados Pessoais que possa afetar significativamente interesses e direitos fundamentais dos Titulares	Decisões tomadas unicamente com base em Tratamento automatizado de Dados Pessoais
	Utilização de Dados Pessoais Sensíveis ou de Dados Pessoais de crianças, adolescentes ou idosos.

Para a verificação da existência de um Tratamento de alto risco, é necessária a presença de, pelo menos, um dos critérios gerais e um dos critérios específicos acima. **Por exemplo, um Controlador que possa ser classificado como um Agente de Tratamento de Pequeno Porte (uma fintech, por exemplo) mas que trate Dados Pessoais de idosos em larga escala não pode se beneficiar do regime jurídico diferenciado trazido pela Resolução CD/ANPD nº 02/22.**

As definições dos critérios gerais foram trazidas pelos dois primeiros parágrafos do artigo 4º da resolução:

Tratamento de Dados Pessoais em larga escala: existirá "quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado"; e

Tratamento de Dados Pessoais que possa afetar significativamente interesses e direitos fundamentais de Titulares: existirá quando "a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade".

Ou seja, será necessária uma avaliação da situação específica do Tratamento para verificar a existência desse Tratamento de alto risco, sendo que a ANPD ainda poderá disponibilizar guias e orientações para auxiliar o Agente de Tratamento de Pequeno Porte nessa avaliação.

As flexibilizações e mudanças trazidas pela Resolução CD/ANPD nº 02/22 serão tratadas em cada capítulo específico relacionado ao tema da obrigação (por exemplo, as disposições sobre direitos dos Titulares serão tratadas no Capítulo XIII), já que todas as demais obrigações da LGPD permanecem aplicáveis aos Agentes de Tratamento que se enquadrarem como sendo de pequeno porte.

CAPÍTULO VI
CORRESPONDENTES NO PAÍS

Em 1º de fevereiro de 2022 entrou em vigor a nova resolução do BACEN sobre correspondentes no país (também chamados de Correspondentes Bancários), a Resolução CMN nº 4935, de 29 de julho de 2021 ("Resolução CMN nº 4935/21"), em substituição à antiga Resolução BACEN nº 3954/11.

A resolução foi elaborada tendo os aspectos da proteção de Dados Pessoais em vista, uma vez que traz, em diversas passagens, obrigações ao Correspondente Bancário de fornecer informações claras, exatas e adequadas aos Titulares, referenciando os princípios da transparência e do livre acesso previstos na LGPD.

A primeira obrigação expressa trazida pela Resolução CMN nº 4935/21 é a de que a contratação de Correspondentes Bancários deverá ser dar somente com correspondentes no Brasil, mas a prestação de serviços poderá ocorrer de forma pessoal ou por plataforma eletrônica, seja por meio de site na internet, aplicativo ou outras plataformas de comunicação em rede.

Um dos principais aspectos da resolução é a de que o correspondente atua por conta e sob as diretrizes da instituição contratante, quem assume a inteira responsabilidade pelo atendimento prestado aos clientes e usuários por meio do contratado.

Além disso, a Resolução CMN nº 4935/21 estabelece que a instituição financeira será a responsável por garantir a segurança da informação dos Dados Pessoais e das transações realizadas por meio do correspondente, bem como assegurar o cumprimento da legislação e regulamentação aplicável.

A INSTITUIÇÃO FINANCEIRA PODE EXIGIR, ALÉM DAS CLÁUSULAS PREVISTAS NA RESOLUÇÃO, OUTRAS CONDIÇÕES CONTRATUAIS, COMO O CUMPRIMENTO DO DISPOSTO NA RESOLUÇÃO DE SEGURANÇA CIBERNÉTICA (RES. 4893/21).

A resolução obriga que a relação entre a instituição contratante e o Correspondente Bancário seja formalizada por meio de contrato, que disponha especificamente sobre o objeto da contratação, nos termos das possibilidades do artigo 12 da Resolução CMN nº 4935/21, além de quatorze condições gerais do contrato de correspondente.

Além disso, os Correspondentes Bancários que prestarem serviços envolvendo operações de crédito e arrendamento mercantil devem, obrigatoriamente, atestar a qualidade técnica do atendimento por meio de certificação emitida por entidade de reconhecida capacidade técnica. Essa certificação deve abordar, em adição aos aspectos técnicos da operação, as disposições da LGPD, do Código de Defesa do Consumidor, da regulamentação aplicável, além de ética e ouvidoria.

CAPÍTULO VII

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

O Encarregado pelo Tratamento de Dados Pessoais ("Encarregado") é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os Titulares dos Dados Pessoais e ANPD.

A ANDP poderá estabelecer normas complementares sobre a definição e as atribuições do Encarregado, além de indicar as 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 Pessoais.

O OPERADOR TAMBÉM PODERÁ INDICAR UM ENCARREGADO, JÁ QUE ELE PODERÁ, EM DETERMINADA ATIVIDADE DE TRATAMENTO, SER CLASSIFICADO COMO CONTROLADOR.

Os Agentes de Tratamento classificados como sendo de pequeno porte não são obrigados a indicar um Encarregado, sendo que a indicação nesses casos é considerada uma política de boa prática e de governança.

Isso não afasta o dever do Agente de Tratamento de Pequeno Porte possuir um canal de comunicação com o Titular de Dados Pessoais, para o recebimento de solicitações.

O Encarregado deve, como medida de boa prática, possuir liberdade e autonomia para realizar suas atribuições, isto é, idealmente, deverá estar inserido dentro de uma **estrutura própria** dentro da empresa, r**eportando diretamente aos Diretores/Conselho.**

Entre as principais funções do Encarregado, estão:

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

b) receber comunicações da ANPD 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 site do Controlador, a identidade e as informações de contato do Encarregado.

A DIVULGAÇÃO DO CONTATO DO ENCARREGADO PODE OCORRER POR MEIO DA POLÍTICA DE PRIVACIDADE DISPONIBILIZADAS NOS SITES DAS EMPRESAS, COMO ATUALMENTE É FEITO PELA MAIORIA DOS AGENTES DE TRATAMENTO.

CAPÍTULO VIII

BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Uma das principais condições trazidas pela LGPD para a regularidade do Tratamento de Dados Pessoais é a necessidade de fundamentação da atividade de Tratamento em uma das hipóteses estabelecidas pela referida legislação. Essas hipóteses são conhecidas como Bases Legais de Tratamento.

As Bases Legais existentes são apresentadas em dois artigos da lei: no artigo 7º estão as Bases Legais para o Tratamento de Dados Pessoais, enquanto o artigo 11 da LGPD dispõe as Bases Legais que autorizam o Tratamento dos Dados Pessoais Sensíveis.

Essa diferenciação é importante, uma vez que os Dados Pessoais Sensíveis **apenas** poderão ser tratados se estiverem fundamentados por uma das hipóteses trazidas no artigo 11. Dessa forma, por exemplo, **não é possível tratar Dados Pessoais Sensíveis com justificativa no legítimo interesse.**

Existem 11 Bases Legais previstas na LGPD, sendo que 10 são aplicáveis ao Tratamento de Dados Pessoais e 8 são aplicáveis ao Tratamento de Dados Pessoais Sensíveis – nesse ponto, é importante ressaltar que algumas das Bases Legais são comuns aos Tratamentos de Dados Pessoais e Dados Pessoais Sensíveis.

A tabela abaixo indica as Bases Legais existentes para o Tratamento de cada tipo de Dado Pessoal:

Bases Legais para o Tratamento de Dados Pessoais	Bases Legais para o Tratamento de Dados Pessoais Sensíveis
Consentimento	Consentimento
Cumprimento de obrigação legal ou regulatória	Cumprimento de obrigação legal ou regulatória
Execução de políticas públicas pela administração pública	Execução de políticas públicas pela administração pública
Realização de estudo por órgãos de pesquisa	Realização de estudo por órgãos de pesquisa
Execução de contrato ou procedimentos preliminares	
Exercício regular de direitos	Exercício regular de direitos, inclusive em contrato

Proteção da vida ou incolumidade física do Titular ou terceiros	Proteção da vida ou incolumidade física do Titular ou terceiros
Tutela da saúde	Tutela da saúde
Atender a interesses legítimos	
Proteção do crédito	
	Prevenção à fraude e garantia de segurança do Titular

É importante frisar que não existe uma ordem hierárquica das Bases Legais, isso é, uma não é superior ou inferior à outra; o que existe é o cenário concreto de cada Tratamento, que será melhor enquadrado, com base nas suas características, em determinada Base Legal.

Também não será necessário buscar mais de uma legitimadora para cada Tratamento de Dados Pessoais desejado. Por exemplo, ao fundamentar e enquadrar o Tratamento de Dados Pessoais baseado no legítimo interesse, em relação a uma finalidade específica pretendida, não será necessária a obtenção do consentimento do Titular.

Na sequência, serão abordadas, com maiores detalhes, as Bases Legais que mais se enquadram no contexto das atividades conduzidas pelo público-alvo deste manual. São elas: (i) consentimento; (ii) cumprimento de obrigação legal ou regulatória; (iii) execução de contrato ou procedimentos preliminares; (iv) exercício regular de direitos; (v) legítimo interesse; (vi) proteção do crédito; e (vii) prevenção à fraude e garantia de segurança ao Titular.

O CONSENTIMENTO NÃO É A REGRA! A LGPD É UMA LEI DE EXCEÇÕES AO CONSENTIMENTO, NÃO EXISTINDO ORDEM HIERÁRQUICA ENTRE AS BASES LEGAIS PREVISTAS NA LEI.

Consentimento

O consentimento é uma das Bases Legais trazidas pela LGPD. Ele é definido pelo artigo 5º, inciso XII da LGPD como sendo a *"manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"*.

A utilização do consentimento, contudo, não é a regra para o Tratamento de Dados Pessoais pela LGPD. Na realidade, quando há a análise de um fluxo de Dados Pessoais, com a identificação das finalidades do Tratamento, o que se busca é avaliar as exceções ao consentimento, utilizando outra Base Legal para fundamentar o Tratamento. Idealmente, o consentimento deve ser utilizado apenas nas hipóteses nas quais não for possível fundamentar o Tratamento em outra Base Legal disponível.

De acordo com a definição, portanto, são quatro as características básicas do consentimento:

- **Livre:** o consentimento deve refletir uma manifestação livre da vontade do Titular. Ou seja, o Titular dos Dados Pessoais não pode ser obrigado a consentir com o Tratamento, assim como o consentimento não pode ser obrigatório para a contratação de um serviço ou compra de um produto;

- **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 capaz de demonstrar verdadeira vontade do Titular em autorizar o Tratamento. Isso pode ser feito por escrito ou por outros meios, desde que não deixem dúvidas (por exemplo, por meio de gravação de uma ligação telefônica ou pelo preenchimento de um formulário online no qual a checkbox de consentimento não esteja pré-selecionada). Consentimentos implícitos, que não tenham sido registrados, ou que deixem por algum motivo dúvidas sobre a vontade do Titular, serão considerados nulos; e

- **Relacionado a uma finalidade determinada:** o Titular deverá autorizar o Tratamento de dados para uma finalidade específica. Autorizações genéricas ou vagas podem ser consideradas nulas.

Além disso, é importante se atentar ao fato de que o consentimento é **revogável a qualquer momento**, isto é, o Titular pode solicitar, por meio de manifestação expressa, a revogação do consentimento, momento a partir do qual não será mais lícita a continuidade daquele Tratamento de Dados Pessoais.

O consentimento, justamente por seus requisitos e características, mostra-se como **uma das Bases Legais com maior ônus ao Controlador**, que deve ser capaz de provar que sua coleta ocorreu em conformidade com a LGPD. Além disso, a recomendação é que a utilização do consentimento ocorra apenas nas situações nas quais nenhuma outra Base Legal seja aplicável.

De forma prática, a utilização do consentimento traz a necessidade de atuação do Controlador em três etapas distintas: (i) avaliação do uso de consentimento; (ii) coleta do consentimento; e (iii) gestão do consentimento. Essas etapas podem ser operacionalizadas, de forma indicativa, a partir das seguintes atividades:

Avaliação do uso de consentimento

o Definir a finalidade específica do Tratamento;

o Avaliar se o Tratamento não pode ser enquadrado em nenhuma outra Base Legal;

o Elaborar a solicitação de consentimento observando:

• A apresentação em cláusula destacada das demais, caso o consentimento seja coletado de forma escrita;

• A utilização de linguagem clara e simples, de fácil compreensão, nas informações sobre o objetivo do Tratamento e Dados Pessoais que serão coletados;

• A existência de consentimentos separados para cada finalidade distinta ("granulares"), permitindo aos Titulares selecionar apenas aqueles Tratamentos com os quais concordarem;

• A identificação do Controlador responsável pelo Tratamento;

• A necessidade de coleta de consentimento específico em caso de compartilhamento dos Dados Pessoais com outros Controladores; e

• O fornecimento da informação de que o Titular pode recusar fornecer o consentimento e as consequências dessa recusa, bem como da possibilidade de revogação do consentimento a qualquer momento;

Coleta do consentimento

o Armazenar informações suficientes que permitam a identificação de como e quando o consentimento foi coletado (por exemplo, registro do endereço IP de origem, data e hora da conexão);

o Armazenar uma cópia de quais informações foram apresentadas ao Titular no momento da coleta de consentimento, de forma a provar que o Titular possuía informações suficientes sobre o Tratamento;

Gestão do consentimento

o Oferecer meios práticos, simples e gratuitos para que o Titular possa revogar o consentimento, como um formulário online ou uma plataforma de gestão de consentimento no site ou aplicativo do Controlador;

o Revisar periodicamente o fluxo da atividade de Tratamento e as informações do consentimento obtido, de modo a verificar se não houve alteração da atividade e se o consentimento permanece válido;

o Adotar procedimentos para notificar o Titular em caso de alteração da finalidade, forma e duração do Tratamento, identificação do Controlador e/ou uso compartilhado dos Dados Pessoais, com destaque específico quanto ao teor das alterações, possibilitando ao Titular a revogação do consentimento em caso de discordância das alterações;

- Implementar procedimentos para assegurar que as ações relacionadas à revogação do consentimento sejam tomadas o quanto antes;
- Assegurar que os Titulares não serão penalizados pela negativa ou revogação do consentimento.

Além da LGPD, outras leis relacionadas ao setor financeiro trazem a figura do consentimento, como a regulamentação vinculada ao *Open Finance*.

O consentimento no âmbito do *Open Finance* fundamentará apenas o compartilhamento de Dados Pessoais entre as instituições participantes, sendo que o Tratamento posterior dos dados demandará o enquadramento em outra Base Legal, como o legítimo interesse.

Cumprimento de Obrigação Legal ou Regulatória

Esta Base Legal será aplicável sempre que o Tratamento de Dados Pessoais for imposto por uma lei ou regulamentação setorial, não existindo a possibilidade para que o Controlador opte por não realizar o Tratamento.

Em outras palavras, o Tratamento deve ser **necessário para atender a uma exigência da lei**, não sendo possível utilizar essa Base Legal quando existir a possibilidade de que o Controlador atenda a obrigação sem tratar Dados Pessoais.

EXEMPLO: MANTER OS CADASTROS ATUALIZADOS DOS CLIENTES BANCÁRIOS É UM CUMPRIMENTO DE OBRIGAÇÃO IMPOSTA PELA LEI DE COMBATE À LAVAGEM DE DINHEIRO.

Por exemplo, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, exige que as empresas que oferecem funcionalidades online armazenem os registros de acesso a aplicações de internet pelo prazo de seis meses contados da atividade do usuário, para possibilitar sua identificação posterior caso necessário. Neste caso, a coleta e armazenamento desses Dados Pessoais serão realizados com fundamentação na Base Legal do cumprimento de obrigação legal ou regulatória. Contudo, os dados de conexão não poderão ser

acessados e compartilhados sem que haja uma ordem judicial para tanto.

De forma a resguardar os interesses do Controlador, à título exemplificativo, recomenda-se que o Controlador:

- documente a decisão de fundamentar o Tratamento nesta Base Legal para o cumprimento de uma lei ou regulamentação; e
- identifique a origem da obrigação a ser cumprida (ou seja, o número da lei/regulamentação e o artigo específico).

Execução de Contrato ou procedimentos preliminares

Essa Base Legal poderá justificar os Tratamentos necessários ao cumprimento de obrigação contratual assumida, ou então para executar procedimentos preliminares relacionados a um contrato (como a utilização de Dados Pessoais para elaborar a minuta de um contrato).

A LGPD, contudo, traz duas exigências para a utilização desta Base Legal: (i) o contrato deve ser celebrado com o Titular de Dados Pessoais (ou seja, não é possível utilizar essa Base Legal caso o contrato seja celebrado entre Controlador e Operador, por exemplo), e (ii) para o Tratamento em procedimentos preliminares ao contrato, a solicitação de contratação deve ter partido do próprio Titular.

EXEMPLO: O TRATAMENTO RELACIONADO AO FORNECIMENTO DE PRODUTOS OU SERVIÇOS AO TITULAR PODERÁ SER FUNDAMENTADO COM BASE EM EXECUÇÃO DO CONTRATO.

Por exemplo, esta Base Legal poderá fundamentar o Tratamento de Dados Pessoais para entregar um produto ou um serviço adquirido, onde naturalmente é preciso conhecer o nome completo, o endereço e outras informações de contato do Titular. Além disso, dependendo do âmbito do serviço a ser prestado, também poderão ser tratados dados financeiros, profissão do Titular, renda mensal e outros, de forma a avaliar, por exemplo, propostas de financiamento. Da mesma forma, o Tratamento de Dados Pessoais para procedimentos preliminares pode ser exemplificado com o cenário de uma solicitação do Titular para orçamento ou proposta para a avaliação da contratação de algum serviço.

De forma a assegurar que essa Base Legal será aplicável a um Tratamento, o Controlador, idealmente, deve:

- possuir um contrato assinado ou uma solicitação de contrato enviada pelo Titular;
- assegurar que o Titular que terá seus Dados Pessoais tratados é parte no contrato;

- avaliar se o Tratamento realizado é de fato necessário para a execução do contrato; e
- documentar e manter armazenado o contrato que fundamentou o Tratamento.

Exercício Regular de Direitos

A Base Legal de Exercício Regular de Direitos em Processos permite a realização de Tratamentos de Dados Pessoais com a finalidade de exercer direitos em processos, sejam eles judiciais, administrativos ou arbitrais.

SEMPRE QUE O CONTROLADOR PRECISAR ATUAR EM ALGUM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL, A BASE LEGAL SERÁ O EXERCÍCIO REGULAR DE DIREITOS.

Ou seja, com fundamento nessa Base Legal, será possível o Tratamento de Dados Pessoais sempre que a finalidade estiver vinculada à atuação do Controlador em processo judicial, administrativo ou arbitral.

Como exemplo clássico, tem-se a utilização de Dados Pessoais armazenados para a elaboração da contestação em um processo judicial ajuizado pelo Titular após o encerramento de sua relação com o Controlador, ou então para o próprio Controlador ajuizar uma ação de reparação de danos eventualmente causados pelo Titular contra seu patrimônio.

Pode-se dizer, portanto, que essa Base Legal decorre tanto do direito de acesso à Justiça, quanto dos princípios do contraditório e da ampla defesa, justificando os Tratamentos de Dados Pessoais pelo tempo em que perdurar o processo judicial, administrativo ou arbitral.

A Base Legal do exercício regular de direitos também pode fundamentar o Tratamento de Dados Pessoais Sensíveis, conforme previsão da LGPD. Nesse sentido, além de possibilitar o armazenamento e uso para processos judiciais, administrativos ou arbitrais, a LGPD prevê que o Controlador também poderá fundamentar o Tratamento para exercer seus direitos em um contexto contratual, mesmo quando envolverem Dados Pessoais Sensíveis.

Para a utilização dessa Base Legal de forma a mitigar os riscos atrelados, o Controlador poderá tomar as seguintes ações:

- armazenamento dos Dados Pessoais em base segregada da base de dados principal do Controlador;
- adoção de controles de acesso e implementação de restrições para leitura e modificação dos Dados Pessoais armazenados ("need-to-know basis"); e
- assegurar que o armazenamento dos Dados Pessoais se dará durante todo o curso do processo judicial, administrativo ou arbitral.

Legítimo Interesse

A Base Legal do legítimo interesse é a mais flexível e abrangente entre as Bases Legais existentes, podendo ser utilizada para atender os interesses legítimos do Controlador ou de terceiros. Por ter essa flexibilidade, acaba sendo uma das Bases Legais mais utilizadas pelos Controladores para fundamentar o Tratamento de Dados Pessoais.

ATENÇÃO: USE O LEGÍTIMO INTERESSE COM CUIDADO!
OS DIREITOS DOS TITULARES NÃO PODEM SER DESRESPEITADOS POR CAUSA DO INTERESSE DO CONTROLADOR.

A lei não estabelece em quais situações existe ou poderá existir o legítimo interesse para tratar Dados Pessoais, e indica que essa análise deverá ser realizada pelo Controlador, a partir de situações concretas.

Essas situações concretas incluem, mas não se limitam, a apoio e promoção de atividades do Controlador, como por exemplo, o envio de comunicações de marketing de produtos e serviços do próprio Controlador ou de seus parceiros.

Ao utilizar o legítimo interesse, o Controlador assumirá obrigações adicionais, no sentido de ser necessário balancear o legítimo interesse para o Tratamento com os direitos e as liberdades fundamentais do Titular, de forma a não oferecer riscos relevantes aos Titulares.

É mais provável que exista um legítimo interesse nas situações em que o Tratamento a ser realizado esteja dentro das expectativas razoáveis dos Titulares e tenham um pequeno impacto à sua privacidade. Para isso, existem três elementos que devem ser analisados antes de se decidir por fundamentar um Tratamento no legítimo interesse:

Teste da Finalidade

Identificação das finalidades e avaliação da legitimidade, que verificará se o interesse pretendido é legítimo e lícito.

Teste da Necessidade

Identificação da possibilidade de se atingir a Finalidade por outro meio e/ou utilizando menos Dados Pessoais.

Teste do Balanceamento

Análise se o uso dos Dados Pessoais está dentro das legítimas expectativas do Titular e se os direitos e garantias fundamentais do Titular estão sendo resguardados.

Uma vez verificada a possibilidade de tratar Dados Pessoais com base no legítimo interesse, é necessária a aplicação de um conjunto adicional de medidas de salvaguarda, justamente para manter o Tratamento balanceado com as expectativas do Titular.

Nesse sentido, a ANPD poderá solicitar ao Controlador o Relatório de Impacto à Proteção de Dados Pessoais ("RIPD"), sendo recomendável que o Controlador possua um procedimento para a elaboração deste documento, de modo a preparar a documentação que comprove a regularidade do Tratamento baseado no legítimo interesse.

Esse relatório deve descrever os processos de Tratamento de Dados Pessoais que podem gerar riscos às liberdades e aos direitos dos Titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Em resumo, para assegurar que o legítimo interesse, enquanto Base Legal, é aplicável e será utilizado em conformidade com a legislação, recomenda-se, à título exemplificativo, as seguintes ações:

- Analisar o Tratamento pretendido para identificar a presença dos três elementos (finalidade, necessidade e balanceamento), armazenando as evidências e resultados da análise;
- Assegurar que o Tratamento não será intrusivo ou poderá gerar riscos relevantes aos Titulares;
- Elaborar o RIPD e armazenar o documento para apresentação à ANPD, caso solicitado;
- Adotar um procedimento de revisão periódica do Tratamento baseado no legítimo interesse, e elaborar um novo RIPD em caso de modificações no Tratamento;
- Garantir a transparência ao Titular sobre os Tratamentos realizados com base no legítimo interesse; e

- Se possível, oferecer aos Titulares a possibilidade de se opor ao Tratamento, e interromper o Tratamento de Dados Pessoais dos Titulares que manifestaram oposição.

O legítimo interesse, enquanto Base Legal, pode ser utilizado para fundamentar diversas atividades de Tratamento de Dados Pessoais como, por exemplo a captura de imagens das instalações do Controlador por câmeras de segurança.

O legítimo interesse não pode ser utilizado para fundamentar as atividades de Tratamento que envolvam Dados Pessoais Sensíveis!

Proteção do Crédito

Apesar de trazer como uma Base Legal própria, a LGPD não forneceu maiores informações sobre o conceito de proteção do crédito, nem detalhamento sobre as situações ou hipóteses nas quais é cabível a utilização de tal Base Legal.

Ainda assim, é possível compreender essa utilização de maneira ampla, isto é, possível de ser utilizada na totalidade das atividades ligadas à concessão de crédito. Isso significa que a análise do histórico do Titular, consulta das informações de dívidas em órgãos de proteção ao crédito, bem como consulta das informações previstas na Lei do Cadastro Positivo (Lei nº 12.414/2011) poderá ser fundamentado com base na proteção ao crédito.

A UTILIZAÇÃO DA BASE LEGAL DA PROTEÇÃO DO CRÉDITO EXIGE QUE O CONTROLADOR SE ATENTE ÀS LEGISLAÇÕES RELACIONADAS, COMO A LEI DE CADASTRO POSITIVO E A LEI DE SIGILO BANCÁRIO.

É importante destacar, contudo, que as demais disposições aplicáveis ao processo de análise do crédito, incluídas as obrigações trazidas pelo Código de Defesa do Consumidor, pela Lei do Cadastro Positivo, pela Lei do Sigilo Bancário e pelas resoluções e regulamentações específicas do BACEN também deverão ser observadas nestes Tratamentos, uma vez que a LGPD trouxe expressamente a necessidade de observância da legislação aplicável sobre o tema.

Assim, para operacionalizar a Base Legal da proteção ao crédito, é recomendado que o Controlador:

- identifique os Tratamentos atrelados a atividades, por exemplo, de concessão de crédito, oferecimento de produtos e gestão de risco;

- observe que obrigações da legislação aplicável serão aplicáveis, inclusive quanto as resoluções e regulamentações do BACEN;

- defina quais informações relacionadas às análises de crédito são consideradas como segredos de negócio (por exemplo, a fórmula e algoritmo utilizado para criar o score de crédito); e

- arquive os resultados das análises e os Dados Pessoais utilizados.

A proteção do crédito não pode ser utilizada para fundamentar as atividades de Tratamento que envolvam Dados Pessoais Sensíveis!

Prevenção à fraude e garantia de segurança do Titular

No que se refere à Base Legal da prevenção à fraude e garantia de segurança do Titular, é necessário reforçar que tal Base Legal se refere especificamente ao Tratamento de Dados Pessoais Sensíveis, por exemplo, a eventuais dados biométricos utilizados para validação de identidade dos Titulares em determinadas operações, como a autenticação do Titular para realizar transações bancarias por meio do aplicativo de internet banking, ou então por meio da utilização de biometria para auferir prova de vida em fluxos de contratação eletrônica.

A LGDP traz justamente a definição das situações nas quais a prevenção à fraude poderá justificar o Tratamento de Dados Pessoais Sensíveis: em processos de identificação e autenticação de cadastros em sistemas eletrônicos. Além disso, há a previsão expressa da necessidade de se manter resguardados os direitos do Titular mencionados no artigo 9º da lei.

APESAR DE O ACESSO MEDIANTE A BIOMETRIA FACIAL PODER SER FUNDAMENTADO COMO PREVENÇÃO À FRAUDE, O TRATAMENTO DO DADO PESSOAL SENSÍVEL TRAZ MAIORES RISCOS AO CONTROLADOR.

Isso significa que, quando houver o Tratamento de Dados Pessoais Sensíveis para autenticação ou identificação do Titular em sistemas eletrônicos, justificado na prevenção à fraude ou garantia de sua segurança, não poderá ser afastado o direito do Titular em receber as informações relativas ao Tratamento destes Dados Pessoais, sendo ressaltado o dever de transparência do Controlador para com o Titular.

A prevenção à fraude SOMENTE pode ser utilizada para fundamentar as atividades de Tratamento que envolvam Dados Pessoais Sensíveis!

Como resumo, o quadro abaixo indica as principais bases legais aplicáveis e um exemplo de sua utilização como fundamentar uma atividade de Tratamento:

Bases Legais | Dados Pessoais

Cumprimento de Obrigação Legal ou Regulatória	Execução de Contrato	Exercício regular de direitos em processos	Legítimo Interesse	Proteção do Crédito	Consentimento
o Dados Pessoais necessários para procedimento de KYC	o Dados Pessoais para realizar a entrega de um produto ou executar um serviço contratado	o Dados Pessoais relacionados a ação indenizatória de consumo	o Enriquecimento de Dados Pessoais para cobrança de Titulares inadimplentes	o Dados Pessoais realcionados à saúde financeira do Titular	o Dados Pessoais para participação em campanha promocional específica

Bases Legais | Dados Pessoais Sensíveis

Cumprimento de Obrigação Legal ou Regulatória	Exercício regular de direitos, inclusive em contratos	Prevenção à Fraude e Segurança do Titular	Consentimento
o Dados Pessoais para exame admissional	o Dados pessoais relacionados à saúde, em processo trabalhista	o Identificação biométrica para confirmação de identidade no aplicativo do internet banking	o Dados Pessoais para identificação de humor a partir do reconhecimento facial

CAPÍTULO IX

COMPARTILHAMENTO DE DADOS PESSOAIS COM TERCEIROS

O compartilhamento de Dados Pessoais com terceiros (como escritórios de cobrança, escritórios de advocacia, correspondentes no País, entre outros) é um importante ponto de atenção para qualquer Controlador de Dados Pessoais.

Adotar o compartilhamento de Dados Pessoais pressupõe a necessidade de adoção de alguns cuidados por quem estiver enviando as informações a terceiros, uma vez que saber quem é a parte que receberá os Dados Pessoais e o nível de conformidade dela com os requisitos de segurança e da LGPD é essencial para mitigar riscos, sejam eles reputacionais ou financeiros.

A LGPD não proíbe o compartilhamento de Dados Pessoais entre Controladores, ou entre Controladores e Operadores, ou entre Operador e Suboperador, mas apresenta algumas obrigações que devem ser observadas quando o compartilhamento ocorrer.

O COMPARTILHAMENTO DE DADOS PESSOAIS NÃO É PROIBIDO PELA LGPD, MAS DEVE SER AVALIADO COM CUIDADO, JÁ QUE O CONTROLADOR CONTINUA RESPONSÁVEL PELO COMPARTILHAMENTO QUE REALIZAR.

Por exemplo, o Controlador tem o dever de informar o Titular, mediante questionamento deste, sobre o compartilhamento dos Dados Pessoais, apresentando tanto as informações sobre o compartilhamento e a sua finalidade, quanto as informações sobre os outros Agentes de Tratamento que receberam os Dados Pessoais.

Além disso, no Tratamento de Dados Pessoais Sensíveis, a ANPD poderá vedar ou regulamentar o compartilhamento desses dados que tiver como objetivo a obtenção de vantagem econômica para os Controladores.

Do ponto de vista prático, **a primeira ação que uma empresa deve adotar para efetuar o compartilhamento é entender quem é a parte que receberá os Dados Pessoais** e, sempre que possível, realizar um procedimento para verificar qual é o nível de maturidade que esse terceiro possui para receber os dados que serão compartilhados. Como sugestão, este Manual contém um checklist de avaliação de terceiros no Capítulo XX.

Outro passo importante é a definição de quais cláusulas serão incorporadas no contrato a ser assinado entre as empresas, de forma a assegurar que a LGPD e as eventuais

leis relacionadas sejam cumpridas, bem como para prever a responsabilidade de cada parte na relação. Ainda que não haja um contrato formalmente assinado, recomenda-se que, sempre que existir o compartilhamento de Dados Pessoais, haja a assinatura de um documento (por exemplo, um termo de Tratamento de Dados Pessoais) que contenha as cláusulas sobre proteção de Dados Pessoais.

Essas cláusulas poderão variar de acordo com a posição que cada parte assumir como Agente de Tratamento. Em uma relação entre dois Controladores singulares, é possível a adoção de cláusulas que imponham menos obrigações individuais a cada parte, já que cada Controlador será responsável apenas por suas próprias atividades de Tratamento.

Já em uma relação entre Controladores conjuntos, as cláusulas que definem a responsabilidade de cada parte são cruciais para delimitar o escopo de atuação e a responsabilidade de cada Controlador na atividade de Tratamento. Nesse sentido, o contrato poderá definir, por exemplo, de quem será a responsabilidade pelo atendimento dos direitos dos Titulares, ou mesmo quem deverá ser a responsável pela comunicação de incidentes à ANPD.

Por outro lado, uma relação entre Controlador e Operador exige a adoção de cláusulas mais restritivas ao Operador, de forma a limitar a sua possibilidade de atuação no Tratamento dos Dados Pessoais às instruções e diretrizes definidas pelo Controlador.
Além disso, é preciso levar em consideração, também, a Lei de Sigilo Bancário, que contém disposições bastante amplas e estabelece que as instituições financeiras devem manter sigilo em todas as suas operações ativas, passivas e serviços prestados.

Considerado os cenários que envolvem a prestação de serviços de uma instituição financeira, é possível que se tenha a necessidade de compartilhamento de Dados Pessoais sem a coleta do consentimento previsto na Lei de Sigilo Bancário, como ocorre quando a prestação de serviços exige a participação de terceiros (como transações realizadas por meio de correspondentes no País), ou nas situações em que o Controlador necessitar compartilhar informações com advogados para proteger seus interesses.

No entanto, é necessário ressaltar que as diversas situações precisam ser analisadas caso a caso, de modo a avaliar se o compartilhamento está em conformidade com a Lei de Sigilo Bancário.

ATENÇÃO: UTILIZAR AS CLÁUSULAS CONTRATUAIS ERRADAS EM RELAÇÃO À POSIÇÃO DAS PARTES COMO AGENTES DE TRATAMENTOSPODE REPRESENTAR UM GRANDE RISCO!

CAPÍTULO X
SEGURANÇA CIBERNÉTICA E REGULAMENTAÇÃO SETORIAL

A LGPD determina a necessidade quanto à adoção de medidas de segurança, técnicas e administrativas, para proteger os Dados Pessoais de incidentes.

Apesar de não dispor expressamente quais são os requisitos de segurança mínimos que devem ser aplicados pelos Agentes de Tratamento, a LGPD estipula que a ANPD poderá regulamentar sobre a matéria.

Contudo, é possível que o Controlador se utilize de parâmetros já adotados e reconhecidos pelo mercado, como aqueles dispostos nas normas ISO da família 27000, como **as normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002.**

Neste sentido, é importante esclarecer que essa recomendação visa garantir a adoção de medidas técnicas e operacionais de segurança da informação, de modo a proteger as informações contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação ou difusão ou o acesso não autorizado.

AS NORMAS DA FAMÍLIA ISO 27000 SÃO BONS PARÂMETROS DE SEGURANÇA, APESAR DE NÃO TEREM SIDO IMPOSTAS PELA LGPD.

Contudo, por estarem dispostas em uma norma técnica, **as recomendações não possuem caráter vinculante, isto é, não são obrigações legais ou regulatórias impostas pelo legislador.**

Por outro lado, as instituições financeiras possuem o dever de atender a Res. CMN nº 4983/21 (e as instituições de pagamento, a Res. BCB nº 85/21), que traz as disposições sobre a política de segurança cibernética que deve ser adotada pelas instituições autorizadas a funcionar pelo BACEN.

É extremamente importante ressaltar que a política prevista nessa resolução não englobará apenas os Dados Pessoais tratados pelas instituições, mas deverá abranger toda e qualquer informação que a instituição possua.

Além dos elementos que devem ser levados em conta para elaborar a política de segurança cibernética, a Res. CMN nº 4983/21 também obriga as instituições a adotarem

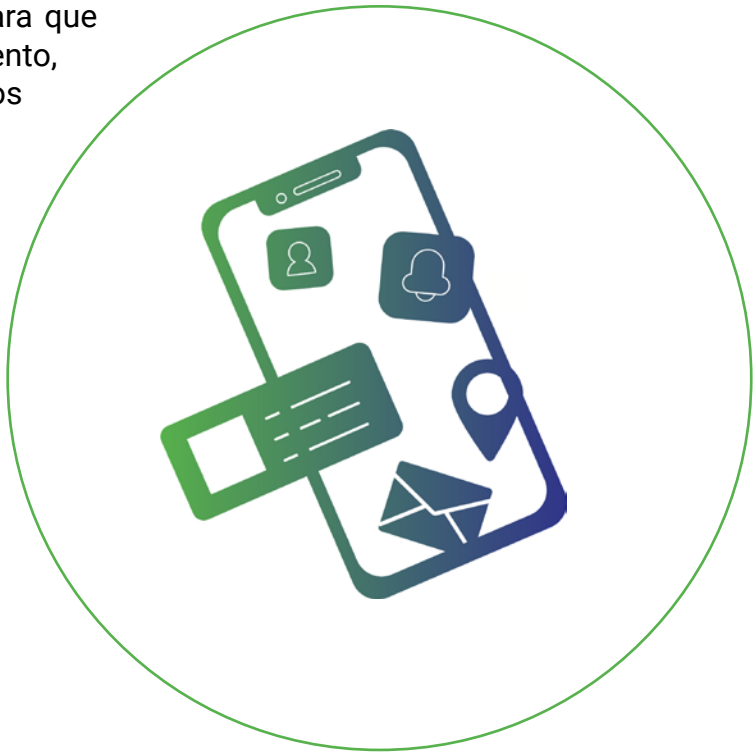
um plano de ação e de resposta a incidentes, prevendo, no mínimo: (i) as ações a serem desenvolvidas para adequar a estrutura da instituição à política de segurança cibernética; (ii) rotinas, procedimentos, controles e tecnologias a serem utilizados na prevenção e resposta a incidentes; e (iii) a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

Como já dito, a política de segurança cibernética abrange muitas outras situações que não necessariamente envolvem Dados Pessoais, mas sua adoção pode facilitar o atendimento das disposições da LGDP no que estiver relacionado com a implementação de medidas de segurança, de prevenção e de resposta a incidentes envolvendo Dados Pessoais.

Além disso, a Resolução CMN nº 4893/21 também trouxe alterações nas regras para o uso de serviços de nuvem. Com a nova resolução, as instituições não mais precisam comunicar previamente ao BACEN sobre utilização de serviços relevantes de processamento e armazenamento em nuvem, sendo que podem contratar os serviços e comunicar posteriormente ao BACEN em até 10 (dez) dias da contratação.

Por outro lado, foi mantida a obrigação de existência de convênio para troca de informações entre o BACEN e as autoridades supervisoras dos países onde os serviços serão prestados. Caso não exista o convênio necessário, a instituição (financeira ou de pagamento) deverá solicitar autorização prévia do BACEN para a operação, com no mínimo 60 (sessenta) dias de antecedência.

Além disso, foi mantida a exigência para que as instituições financeiras e de pagamento, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, adotem procedimentos que contemplem a adoção de medidas de governança, de forma a garantir a conformidade do prestador de serviços com as legislações aplicáveis, bem como a adoção de medidas e controles mínimos de segurança das informações.



CAPÍTULO XI
INCIDENTES E COMUNICAÇÃO DE INCIDENTES

Uma das obrigações que a LGPD traz expressamente em seu texto é a de que o Controlador deve comunicar à ANPD e aos Titulares a ocorrência de um incidente de segurança com os Dados Pessoais que possa acarretar risco ou dano relevante aos Titulares.

Em primeiro lugar, é preciso entender o que a LGPD quis dizer ao citar "incidente de segurança". Apesar de não trazer a informação nas suas definições, a definição de incidente de segurança pode ser encontrada no site da ANPD[1], sendo interpretada como *"qualquer evento adverso confirmado, relacionado à violação na segurança de Dados Pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de Tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do Titular dos Dados Pessoais".*

Ou seja, um incidente é qualquer evento que implique na quebra da confidencialidade, disponibilidade ou integridade dos Dados Pessoais, como vazamento, perda ou roubo de equipamentos com Dados Pessoais armazenados, incêndios ou alagamentos que danifiquem documentos ou equipamentos com Dados Pessoais, entre outros.

NA DÚVIDA, A RECOMENDAÇÃO DA ANPD É REPORTAR O INCIDENTE COM DADOS PESSOAIS. É PREFERÍVEL REPORTAR UM INCIDENTE COM BAIXOS RISCOS DO QUE NÃO REPORTAR UM INCIDENTE ERRONEAMENTE AVALIADO.

Em segundo lugar, é preciso definir quais incidentes deverão ser comunicados à ANPD e aos Titulares, conforme definido pela LGPD. No artigo 48 da LGPD, a obrigação de comunicação existe sempre que o incidente puder gerar **risco** ou **dano** relevante aos Titulares, mas a definição do que pode ser considerado um risco ou dano relevante não está presente pela lei.

Dessa forma, é necessário que o Controlador faça uma análise individual de cada incidente que ocorra, para determinar se há a possibilidade de criar o risco ou dano relevante que torne obrigatória a comunicação aos Titulares e à ANPD.

Como recomendação, a ANPD sugere que os incidentes sejam notificados mesmo na existência de dúvida sobre o risco ou dano relevante ao Titular, uma vez que a subavaliação

1-Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

da situação pode ser considerada como um descumprimento à legislação de proteção de Dados Pessoais.

A Resolução CD/ANPD nº 02/22 prevê que a ANPD poderá definir um procedimento simplificado ou uma flexibilização nas obrigações relacionadas à comunicação de incidentes envolvendo Dados Pessoais para aqueles Agentes de Tratamento que se enquadrarem como Agentes de Tratamento de Pequeno Porte.

A resolução ainda prevê expressamente que os Agentes de Tratamento de Pequeno Porte terão prazo em dobro para a comunicação de incidentes à ANPD e aos Titulares, exceto quando houver potencial comprometimento à integridade física ou moral dos Titulares ou à segurança nacional.

Como sugestão de um fluxo de avaliação de incidentes e notificação à ANPD e aos Titulares, recomenda-se os seguintes passos:

1. Identificação do incidente
2. Acionamento do plano ação e de resposta a incidentes, conforme diretrizes internas
3. Avaliação interna do incidente (envolve Dados Pessoais?)
4. Comunicação do incidente ao Encarregado, se envolver Dados Pessoais
5. Avaliação interna do incidente (natureza, categoria e quantidade de Titulares afetados; categoria e quantidade de Dados Pessoais afetados; consequências concretas e prováveis)
6. Avaliação de existência de risco ou dano relevante aos Titulares
7. Em caso positivo, levantamento das informações necessárias para a notificação do incidente à ANPD
8. Comunicação do incidente aos Titulares afetados

CAPÍTULO XII

ARMAZENAMENTO DOS DADOS PESSOAIS E TÉRMINO DO TRATAMENTO

A LGPD estipula a obrigatoriedade de eliminação dos Dados Pessoais ao término do Tratamento. Isso significa que, em regra, ao ser verificada alguma das hipóteses a seguir, o Controlador deverá eliminar os Dados Pessoais que possui, sob pena de incorrer em desconformidade com a LGPD.

As hipóteses de término do Tratamento são:

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 ANPD, quando houver violação da lei.

Contudo, nem sempre o término de um Tratamento exigirá a eliminação dos Dados Pessoais. Existem algumas hipóteses nas quais o Controlador poderá armazenar Dados Pessoais, conforme estipulado pela LGPD:

a) para cumprimento de obrigação legal ou regulatória pelo Controlador;
b) por estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos Dados Pessoais;
c) para transferência à terceiro, desde que respeitados os requisitos de Tratamento de dados dispostos na lei; ou
d) para uso exclusivo do Controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Além disso, o Controlador pode necessitar armazenar os Dados Pessoais para outras finalidades além daquelas para as quais os dados foram inicialmente coletados. Por exemplo, o Controlador pode armazenar os Dados Pessoais de um Titular após o encerramento da relação contratual entre as partes, para elaboração de defesa em eventual processo judicial.

A ADOÇÃO DE PRAZOS MÍNIMOS DE ARMAZENAMENTO E PROCEDIMENTOS DE DESCARTE SEGURO DE DADOS PESSOAIS PODE DIMINUIR O RISCO DE TRATAMENTO INADEQUADO DE DADOS PESSOAIS.

A LGPD não impede a guarda desses Dados Pessoais, mas exige que o

Controlador seja capaz de demonstrar que o armazenamento é necessário e possui a fundamentação em alguma Base Legal prevista na lei.

Para isso, recomenda-se a definição de prazos mínimos de armazenamento dos Dados Pessoais, considerando a necessidade e a finalidade para a qual o armazenamento será realizado após o encerramento da atividade de Tratamento.

Resgatando o exemplo dado acima, de armazenamento para defesa em eventual processo judicial, geralmente o prazo mínimo de armazenamento está vinculado com o prazo previsto em lei para o ajuizamento de ações.

Contudo, é preciso também se atentar para a existência de prazos previstos em setores regulados, como acontece no setor financeiro, por meio das regulamentações específicas do BACEN, como a obrigatoriedade de manutenção dos dados dos clientes bancários pelo prazo de 10 anos contados a partir do ano seguinte do término do relacionamento com o Titular (conforme exigência do artigo 67 da Circular BACEN nº 3978/2020).

Dessa forma, considerando as diferentes disposições legais aplicáveis a diferentes empresas, cada Controlador deverá estabelecer e detalhar seus próprios prazos de armazenamento de Dados Pessoais, geralmente organizados em uma tabela de temporalidade, que contenha o tipo de dado coletado, a finalidade do armazenamento, o tempo de guarda e o embasamento legal, quando aplicável.

Além disso, boas práticas de armazenamento seguro de Dados Pessoais podem mitigar riscos de incidentes ou de Tratamentos inadequados de Dados Pessoais. Por exemplo, afasta-se o risco de Tratamento em desconformidade com a LGPD caso os Dados Pessoais para eventual utilização na defesa em processo judicial estejam armazenados em ambiente segregado da base de dados principal e com aplicação de controles de acesso, de forma a evitar que os todos os colaboradores do Controlador possuam acesso a esses Dados Pessoais.

CAPÍTULO XIII

DIREITOS DOS TITULARES DE DADOS PESSOAIS

A LGPD garantiu diversos direitos aos Titulares, os quais podem ser exercidos a qualquer momento e mediante requerimento expresso direcionado ao Controlador, que deve atender as solicitações sem custos para o Titular, nos prazos previstos na lei ou em regulamentação pela ANPD.

OS DADOS PESSOAIS SÃO DO TITULAR A QUEM SE REFEREM, E NÃO SÃO PROPRIEDADE DAS EMPRESAS!

Direito	Principal Impacto
Confirmação da existência do Tratamento	O Controlador deve saber informar se os Dados Pessoais de um Titular são ou não objeto de seu Tratamento. Para isso, o Controlador deve possuir um registro atualizado e completo das atividades de Tratamento.
Acesso aos dados	Caso solicitado, o Controlador deve fornecer ao Titular uma cópia de todos os Dados Pessoais dele que são tratados. Além do registro atualizado, a organização dos Dados Pessoais em um ambiente sistematicamente estruturado facilita o atendimento a esse direito. O Controlador deve responder imediatamente ao Titular, em formato simplificado, ou em 15 dias, no formato completo. Os Agentes de Tratamento de Pequeno Porte possuem prazo de 15 dias para entregar o relatório simplificado, ou 30 dias para o relatório completo.

Correção de dados incompletos, inexatos ou desatualizados	O Controlador deverá corrigir, complementar ou atualizar os Dados Pessoais quando estiverem incorretos, incompletos ou desatualizados. O Controlador poderá adotar procedimentos de verificação das informações atualizadas, inclusive mediante solicitação de comprovação da alteração
Anonimização, bloqueio ou eliminação de dados	Os Dados Pessoais que forem desnecessários, excessivos ou tratados em desconformidade com a LGPD podem ser objeto de solicitação de anonimização, bloqueio ou eliminação. O Controlador deve possuir o registro das atividades de Tratamento de forma que possa averiguar se a alegada desnecessidade, excessividade ou desconformidade no Tratamento existe.
Portabilidade dos dados a outro fornecedor de serviço ou produto	O Titular poderá exigir a transferência direta de seus Dados Pessoais a outro fornecedor de serviço ou produto. Para isso, apesar de ainda estar pendente a regulamentação da ANPD, os Dados Pessoais devem ser encaminhados ao novo Controlador de modo estruturado e em formato interoperável, que possa ser lido de forma automática por computadores (*machine readable*).
Eliminação dos Dados Pessoais tratados com o consentimento do Titular	O Controlador deve possuir o registro de todas as atividades de Tratamento, para permitir a exclusão dos Dados Pessoais nelas tratados quando solicitado pelo Titular, ressalvadas as hipóteses previstas no artigo 16 da LGPD ou as hipóteses de armazenamento com finalidade e Base Legal específica.
Informações acerca do uso compartilhado de dados	O Controlador deve estar preparado para responder a essas requisições por meio da manutenção de registros de Tratamento de Dados Pessoais, tal como exigido pelo artigo 37 da LGPD, incluindo as informações sobre com quais entidades públicas e privadas o Controlador realizou uso compartilhado de Dados Pessoais.

Informações sobre a possibilidade de não fornecer consentimento e as consequências	Os Controladores devem adequar os procedimentos de coleta de consentimento para informem aos Titulares: (i) a possibilidade de não fornecer consentimento, quando esta for a Base Legal adequada, e (ii) as consequências da negativa, que em grande parte das vezes significará a impossibilidade de usufruir de determinada funcionalidade do produto ou serviço.
Revogação do consentimento	Os Controladores devem informar aos Titulares que eles têm o direito de revogar seu consentimento a qualquer tempo. Além disso, os Controladores devem possuir uma forma para essa revogação, preferencialmente por meio de um procedimento rápido e simplificado.
Direito de petição	O Titular poderá peticionar contra o Controlador perante a ANPD, definindo de maneira expressa que ela é o órgão responsável por receber eventuais queixas ou denúncias formuladas pelos Titulares de Dados Pessoais. O Controlador deverá estar preparado para responder aos questionamentos da ANPD, inclusive mediante a apresentação de documentos e provas sobre a regularidade do Tratamento.
Direito de oposição	O Controlador deve possuir o registro de todas as atividades de Tratamento, já que quando a Base Legal 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.
Revisão de decisões automatizadas	O Controlador que se utilizar de decisões automatizadas no Tratamento de Dados Pessoais deverá possibilitar que o Titular solicite a revisão de decisões tomadas unicamente com base em tratamento automatizado de Dados Pessoais que afetem seus interesses, como aquelas destinadas a criação de perfis (*profiling*).

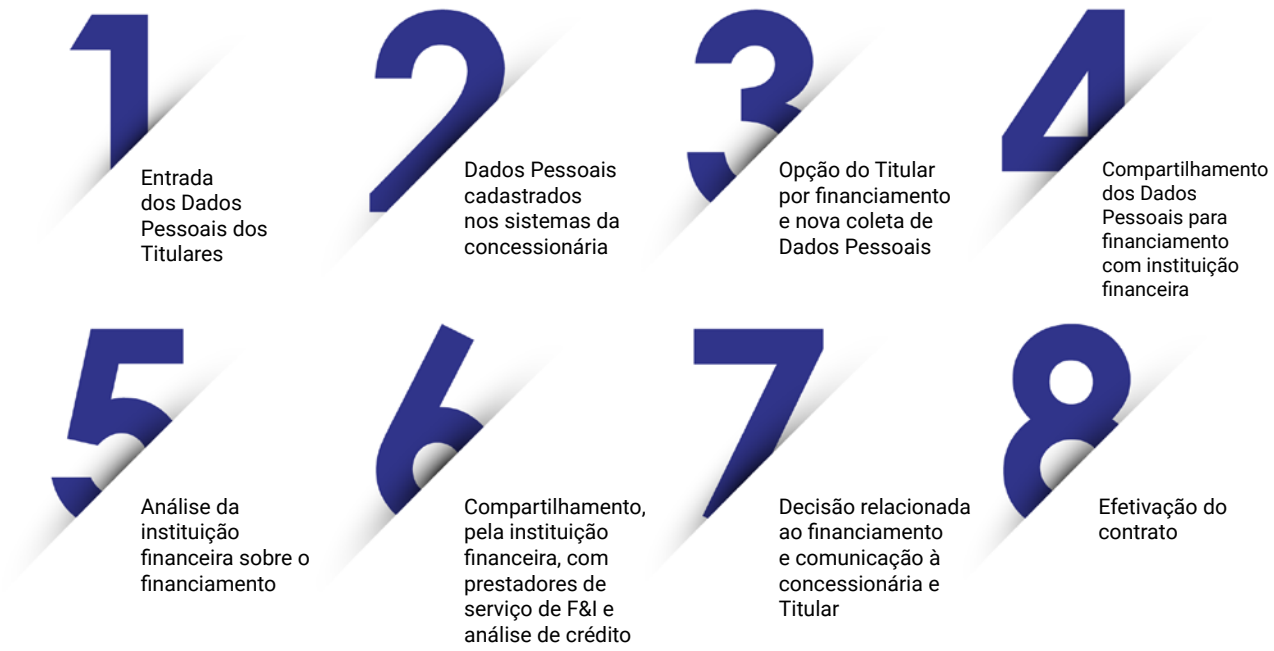
CAPÍTULO XIV

PRINCIPAIS FLUXOS DE DADOS PESSOAIS E PONTOS DE ATENÇÃO

Abaixo são apresentados os fluxos mais comuns de Dados Pessoais que existem em concessionárias e instituições financeiras.

Aquisição e financiamento de um veículo

O primeiro está relacionado com o processo de aquisição e financiamento de um veículo, no qual participam concessionária e instituição financeira, além de seus parceiros e prestadores de serviços.



A entrada dos Dados Pessoais, ou seja, o ponto de coleta dos dados pelo Agente de Tratamento, pode estar configurada de diversas formas, tanto físicas (como nas lojas, *showrooms* e eventos), quanto digitais (como por meio de portais e sites, formulários de "fale conosco" e contatos telefônicos ou por mensagens de texto).

Nessa etapa, o principal ponto de atenção a ser observado pelo Agente de Tratamento responsável pela coleta é o dever de transparência com o Titular, fornecendo as informações relativas aos Tratamentos que serão realizados com os Dados Pessoais. Geralmente, essa transparência é assegurada por meio da Política de Privacidade

disponível no site ou em outro formato com resultado similar (como impresso ou acessível por *QR Code*).

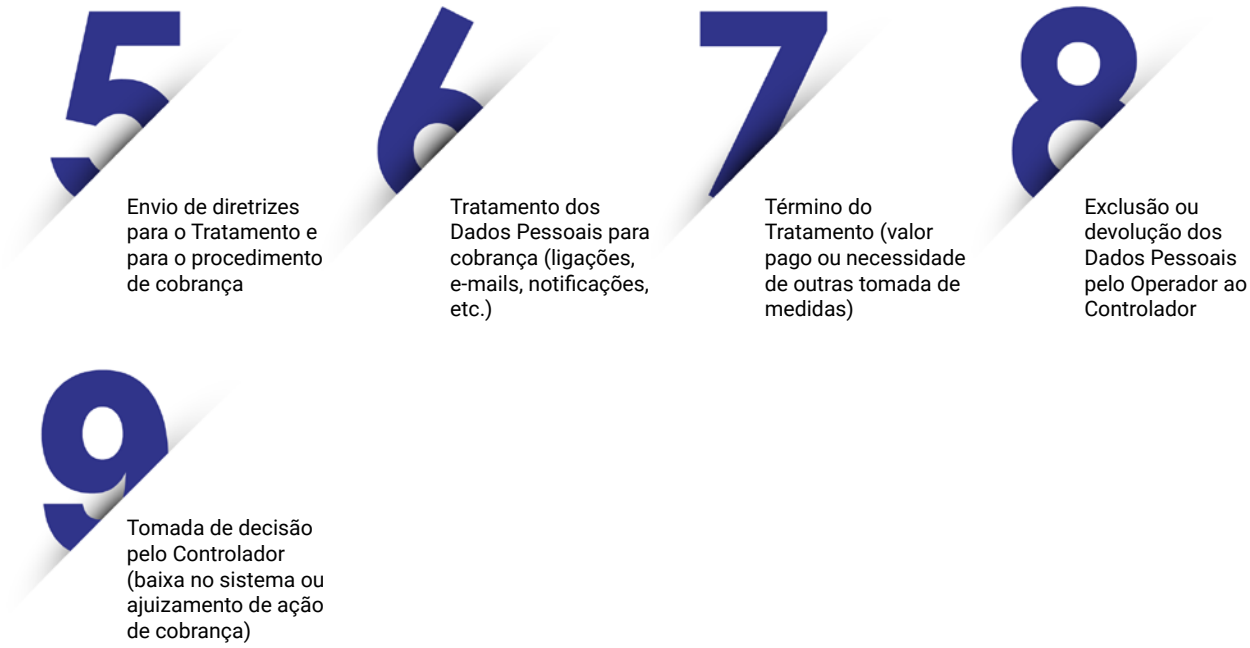
O armazenamento dos Dados Pessoais no sistema exige que o sistema esteja pronto para receber os dados e mantê-los de forma estruturada, permitindo o acesso fácil e a consulta rápida aos Dados Pessoais, especialmente com o intuito de facilitar o atendimento aos direitos dos Titulares. Além disso, todo o sistema do Agente de Tratamento deverá possuir controles, mecanismos e medidas de segurança aptas a proteger os Dados Pessoais de incidentes, mitigando o risco de vazamentos, perdas de informação ou Tratamento inadequado.

Por sua vez, o compartilhamento de Dados Pessoais requer, como principal ponto de atenção, a elaboração de um contrato entre a parte que irá compartilhar os dados e que irá recebê-los, com as disposições relativas à proteção de Dados Pessoais conforme indicado no Capítulo IX. Além disso, é recomendado que sejam adotados protocolos e medidas para a comunicação segura dos Dados Pessoais, à exemplo da criptografia.

Cobrança de Dívidas por terceiros contratados

Outro fluxo importante de ser analisado é o fluxo existente entre o Controlador e o escritório de cobrança de dívidas. Nesse cenário, usualmente, o prestador de serviços é caracterizado como um Operador, uma vez que o processo de cobrança é realizado de acordo com as diretrizes passadas pelo Controlador.

1. Entrada dos Dados Pessoais (compras, empréstimos, financiamentos, cartões de crédito etc.)
2. Identificação de montantes não pagos (existência de divida)
3. Tentativas de cobranças internas
4. Compartilhamento de Dados Pessoais com escritório de cobrança



Não obstante, dadas as especificidades de cada caso, é possível a existência de uma relação entre dois Controladores neste fluxo (por exemplo, quando o escritório de cobrança realizar o enriquecimento de Dados Pessoais por conta própria). Nesse caso, o escritório que realiza a cobrança possui tanta responsabilidade perante os Titulares quanto o Controlador que originalmente compartilhou os dados, podendo responder exclusivamente em casos de danos causados aos Titulares.

Em ambos os casos, as duas principais questões a serem analisadas são: (i) a classificação das partes enquanto Agentes de Tratamento, e (ii) as cláusulas contratuais a serem utilizadas.

Para o primeiro ponto de atenção, é necessário entender quais serão as atividades que a contratada poderá realizar e os limites, isto é, qual será o nível de autonomia e discricionariedade que ela terá para tratar os Dados Pessoais. Com essa definição, será possível definir quais as cláusulas contratuais que serão utilizadas.

Em relação às cláusulas, é importante definir quais serão as finalidades do Tratamento, as responsabilidades de cada parte no monitoramento da respectiva conformidade com a legislação aplicável e, principalmente, as responsabilidades em caso de incidente. Além disso, nos casos em que a contratada for Operadora, é imprescindível que o contrato estipule a obrigatoriedade da devolução ou eliminação dos Dados Pessoais após o término do Tratamento, bem como a vedação de utilização posterior dos dados para outras finalidades.

Envio de comunicações de marketing

O próximo fluxo que será analisado está relacionado com o envio de mensagens de comunicações gerais relacionada aos serviços contratados e o envio de mensagens de

marketing para os Titulares, por meio dos canais por eles identificados no momento do cadastro. Esses dois fluxos são extremamente semelhantes, mas com uma pequena diferenciação em seus finais, relacionado à possibilidade de o Titular requerer o encerramento dos envios.

O primeiro fluxo, relacionado ao envio de comunicações e mensagens relacionadas aos produtos e serviços já contratados, demanda atenção quanto: (i) ao **conteúdo da mensagem**, que deve estar relacionada à contratação realizada pelo Titular; (ii) ao **prazo de comunicação**, que deverá ocorrer apenas enquanto vigente o contrato; e (iii) ao **canal de comunicação**, que deverá ser apenas aquele(s) indicado(s) pelo Titular no momento do cadastro. Via de regra, esse fluxo terá como Base Legal a execução de contrato.

O segundo fluxo, que se refere ao envio de mensagens de marketing, geralmente se baseia no legítimo interesse do Controlador para as comunicações. Por esse motivo, é importante balancear, como dito no Capítulo VIII, as expectativas do Titular com o interesse do Controlador e, idealmente, oferecer ao Titular a possibilidade de se descadastrar ou de solicitar o cancelamento do envio das comunicações a qualquer momento.

De forma geral, os seguintes pontos de atenção devem ser observados durante o ciclo de vida dos dados:

- **Coleta**
  - Observar os princípios da finalidade, necessidade e adequação na definição dos Dados Pessoais que serão coletados;
  - Fornecer as informações necessárias sobre o Tratamento, para atender ao princípio da transparência;
  - Elaborar, quando necessário, o RIPD e a avaliação de legítimo interesse (LIA);
  - Quando o consentimento for a Base Legal aplicável, informar sobre a possibilidade de negativa do consentimento, suas consequências e a possibilidade de revogação posterior a qualquer momento;
  - Utilizar medidas e ferramentas de segurança para garantir a transmissão segura dos Dados Pessoais entre o ponto de coleta e o servidor destino;

- **Utilização**
  - Assegurar que as finalidades informadas ao Titular são as únicas para as quais os Dados Pessoais são tratados;
  - Garantir que o acesso aos Dados Pessoais se dá apenas às pessoas com necessidade de utilizá-los (*need-to-know basis*);
  - Possuir políticas internas que definem responsabilidades pelos Tratamentos dos Dados Pessoais;
  - Implementar medidas e ferramentas técnicas para garantir que os sistemas nos quais os Dados Pessoais serão tratados são seguros e protegidos contra acessos não-autorizados;

- **Compartilhamento**

  • Utilizar medidas e ferramentas de segurança para garantir a transmissão segura dos Dados Pessoais, à exemplo de criptografia;

  • Avaliar o terceiro que receberá os Dados Pessoais para identificar o risco envolvido com o compartilhamento;

  • Possuir instrumentos contratuais assinados com as partes que receberão os Dados Pessoais, garantindo a confidencialidade e proteção dos dados;

  • Quando a transferência for para outro país, adotar alguns dos mecanismos específicos que serão regulamentados pela ANPD para permitir a transferência internacional;

- **Armazenamento**

  • Implementação de medidas e ferramentas de segurança para proteger os Dados Pessoais armazenados, como criptografia (para dados em suporte eletrônicos), ou armários com chave (para dados em suporte físico);

  • Definição do tempo mínimo de armazenamento dos Dados Pessoais;

  • Manutenção da gestão de acesso aos Dados Pessoais armazenados, com tipos específicos de credenciais autorizadas para acessar os Dados Pessoais;

  • Quando necessário, armazenar os Dados Pessoais em bancos de dados segregados, para evitar o acesso e utilização indevida (como nos casos de Dados Pessoais armazenados para uso em eventual processo judicial);

- **Eliminação**

  • Adotar o procedimento de descarte seguro, determinando regras para a eliminação de documentos físicos com Dados Pessoais e para a limpeza completa de dispositivos eletrônicos para descarte;

  • Assegurar que o prazo de armazenamento mínimo dos Dados Pessoais, conforme a Tabela de Temporalidade, já foi superado;

  • Enviar a instrução de eliminação dos Dados Pessoais para os Operadores que eventualmente também tratem os Dados Pessoais objetos da eliminação.

CAPÍTULO XV
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.

A ADOÇÃO DE POLÍTICAS DE BOAS PRÁTICAS E GOVERNANÇA REVELA OS ESFORÇOS EM CUMPRIR A LGPD E PODERÁ SER CONSIDERADA COMO UM ATENUANTE NA APLICAÇÃO DE PENALIDADES EM CASO DE VIOLAÇÃO À LGPD.

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.

Do ponto de vista prático, à título exemplificativo, recomenda-se a avaliação da adoção das seguintes políticas e normas:

- Política de Governança em Privacidade, instituindo as diretrizes gerais de privacidade a serem observadas pelo Agente de Tratamento;

- Política de Segurança da Informação, instituindo as diretrizes gerais de segurança da informação a serem observadas pelo Agente de Tratamento, inclusive quanto a Dados Pessoais;
- Norma de Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), para determinar as situações na qual o RIPD deverá ser elaborado, e de que forma;
- Norma de Privacy by Design, para assegurar a implementação da privacidade desde a concepção de novos produtos e serviços desenvolvidos;
- Procedimento de Descarte Seguro, estipulando os requisitos para eliminar ou descartar um documento (físico ou eletrônico) que contenha Dados Pessoais e/ou dados empresariais; e
- Procedimento de Resposta a Incidentes, estipulando os responsáveis e as ações que deverão ser tomadas em caso de incidente.

Os Agentes de Tratamento de Pequeno Porte poderão adotar uma política simplificada de segurança da informação, desde que contemple requisitos essenciais e necessários para o Tratamento de Dados Pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Além disso, a adoção, pelos Agentes de Tratamento de Pequeno Porte, das recomendações e das boas práticas de prevenção e segurança divulgadas pela ANPD, inclusive por meio de guias orientativos, poderá ser classificada como uma das atenuantes prevista na LGPD em caso de incidente envolvendo Dados Pessoais.

CAPÍTULO XVI

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A Autoridade Nacional de Proteção de Dados, comumente chamada de ANPD, foi criada pela LGPD para atuar no papel de implementação e fiscalização do cumprimento da lei no território nacional.

A ANPD é composta de diversos órgãos, sendo os dois principais: (i) o Conselho Diretor, que é o órgão máximo de direção, composto de cinco diretores; e (ii) o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, órgão consultivo da ANPD, composto de 23 membros.

A ANPD TERÁ UMA ATUAÇÃO BASEADA EM:

EDUCAÇÃO
FISCALIZAÇÃO
SANÇÃO

De forma geral, as principais competências da ANPD são:

- fiscalizar e aplicar sanções em caso de Tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo;
- apreciar petições de Titular contra Controlador após comprovada pelo Titular a apresentação de reclamação ao Controlador não solucionada no prazo estabelecido em regulamentação;
- promover na população o conhecimento das normas e das políticas públicas sobre proteção de Dados Pessoais e das medidas de segurança; e
- realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o Tratamento de Dados Pessoais efetuado pelos Agentes de Tratamento;

Por fim, vale ressaltar que a ANPD também possui competência para regulamentar alguns pontos da LGPD que expressamente foram vinculados à necessidade de regulamentação posterior, possuindo um papel ativo na construção do regramento de proteção de Dados Pessoais no Brasil.

CAPÍTULO XVII
PROCEDIMENTO FISCALIZATÓRIO

Como exposto no capítulo anterior, uma das funções da ANPD será a de fiscalizar o cumprimento da LGPD, sendo a responsável pela instauração de processos administrativos para investigar e, se necessário, punir os Agentes de Tratamento por conta de violações às obrigações previstas em lei.

A ANPD fará esse controle por meio do processo de fiscalização e do processo administrativo sancionador, ambos a serem instaurados no âmbito da própria ANPD, e regulamentados pela Resolução CD/ANPD nº 01, de 28 de outubro de 2021 ("Res. CD/ANPD nº 01/21").

De acordo com as disposições da resolução, a atividade de fiscalização tem como objetivo, em primeiro lugar, orientar os Agentes de Tratamento, seguido pela prevenção e repressão das infrações à LGPD.

Nesse sentido, a fiscalização pela ANPD será desenvolvida, principalmente, por meio das atividades de monitoramento, orientação e atuação preventiva, sem prejuízo, quando necessário, da atuação repressiva.

A resolução define as atividades da ANPD da seguinte forma:

(i) **Monitoramento:** levantamento de informações e dados relevantes para subsidiar a tomada de decisões pela ANPD para assegurar o regular funcionamento do ambiente regulado;

(ii) **Orientação:** atuação baseada na economicidade e na utilização de métodos e ferramentas para promover a orientação, conscientização e a educação dos Agentes de Tratamento e Titulares de Dados Pessoais;

(iii) **Atuação Preventiva**: construção, preferencialmente conjunta e dialogada, de soluções e medidas que visam auxiliar o Agente de Tratamento a retornar à situação de conformidade ou evitar e remediar situações que possam acarretar risco ou dano aos Titulares e a outros Agentes de Tratamento;

(iv) **Atuação Repressiva:** atuação coercitiva da ANPD, voltada à interrupção de situações de dano ou risco, com o retorno à conformidade e respectiva punição dos responsáveis por meio do processo administrativo sancionador.

Em adição às obrigações trazidas pela LGPD, a Res. CD/ANPD nº 1/21 trouxe as seguintes obrigações aos Agentes de Tratamento submetidos à fiscalização da ANPD:

- Fornecer cópias de documentos, dados e informações relevantes para a avaliação das atividades de Tratamento de Dados Pessoais, nas formas e prazos estabelecidos pela ANPD;
- Permitir o acesso às instalações, equipamentos, sistemas, aplicativos e outros recursos tecnológicos, documentos, dados e informações de natureza técnica, operacional e outras relevantes para a avaliação das atividades de Tratamento de Dados Pessoais, ainda que os documentos, sistemas, informações e similares estejam em posse de terceiro;
- Possibilitar o conhecimento, pela ANPD, dos sistemas de informação utilizados para o Tratamento de dados e informações;
- Submeter-se às auditorias realizadas ou determinadas pela ANPD;
- Manter os documentos (físicos ou digitais) armazenados pelos prazos estabelecidos na legislação e regulamentações específicas, bem como durante todo o prazo do processo administrativo nos quais sejam necessários; e
- Disponibilizar, sempre que solicitado, representante apto a oferecer suporte à atuação da ANPD, com conhecimento e autonomia para prestar dados, informações e outros aspectos relacionados.

É importante ressaltar que **não é possível alegar sigilo ou segredo de negócio perante a ANPD como forma de evitar o compartilhamento de dados ou informações.**

Nesse sentido, qualquer não cumprimento dos deveres estabelecidos na resolução poderá caracterizar obstrução à atividade de fiscalização, e sujeitar o Agente de Tratamento a medidas repressivas, além de outras medidas necessárias para concluir a ação de fiscalização.

A atividade repressiva da ANPD poderá ser instaurada, mediante processo administrativo sancionador, caso o Agente de Tratamento deixe de observar as medidas preventivas determinadas pela ANPD, ou de forma direta, mediante decisão da própria autoridade.

A ANPD PREVÊ QUE O AGENTE DE TRATAMENTO PODERÁ SOLICITAR O SIGILO DAS INFORMAÇÕES RELATIVAS À ATIVIDADE EMPRESARIAL QUE POSSAM RESULTAR EM VIOLAÇÃO DE SEGREDO COMERCIAL OU INDUSTRIAL EM CASO DE DIVULGAÇÃO, MAS NÃO PREVÊ A ESCUSA NA APRESENTAÇÃO DESSAS INFORMAÇÕES.

Nem todo processo administrativo sancionador resultará em uma punição ao Agente de Tratamento. Além da possibilidade de não ser identificada uma violação à LGPD, o Agente de Tratamento poderá apresentar uma proposta para celebração de termo de ajuste de conduta, cuja adoção será deliberada pelo Conselho Diretor da ANPD.

Contudo, não sendo apresentada, ou sendo rejeitada, a proposta de termo de ajuste de conduta, o processo administrativo sancionador seguirá normalmente, sendo possibilitado o direito à defesa do Agente de Tratamento. Ao final, caso a ANPD entenda que ocorreu uma violação à LGPD, poderá ser aplicada uma das sanções previstas na LGPD, assegurado, ainda, o direito de que o Agente de Tratamento recorra da decisão ao Conselho Diretor da ANPD.

CAPÍTULO XVIII
VIOLAÇÕES E SANÇÕES

É IMPORTANTE QUE A EMPRESA SE ATENTE À NECESSIDADE DA CONFORMIDADE LEGAL, PARA QUE OS RISCOS EXISTENTES SEJAM MITIGADOS E, PRINCIPALMENTE, PARA QUE OS DANOS REPUTACIONAIS QUE ACABAM POR PREJUDICAR A CONFIANÇA PERANTE O MERCADO SEJAM CONTROLADOS

SANÇÕES DA LGPD

Ao final do processo administrativo sancionador, conforme tratado no Capítulo XVII, o Agente de Tratamento que cometeu uma violação à LGPD poderá ser responsabilizado com alguma das sanções previstas no artigo 52 da LGPD. São elas:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa de até 2% do faturamento do grupo econômico do infrator no Brasil no último exercício, limitado ao valor de R$ 50 milhões por infração;
- Multa diária, observado o limite de R$ 50 milhões;
- Publicização da infração;
- Bloqueio dos Dados Pessoais a que se refere a infração até a sua regularização;
- Eliminação dos Dados Pessoais a que se refere a infração;
- Suspensão parcial do funcionamento do banco de dados a que se refere a infração, por no máximo 6 meses, prorrogáveis por mais 6 meses, até a regularização da atividade de Tratamento pelo Controlador;
- Suspensão do exercício da atividade de Tratamento de Dados Pessoais, por 6 meses, prorrogáveis por mais 6 meses; ou
- Proibição parcial ou total do exercício de atividades relacionadas a Tratamentos de Dados Pessoais.

Em outras palavras, a LGPD prevê nove possibilidades de punição, que variam desde uma simples advertência, com indicação de prazo para que o Agente de Tratamento realize as correções, passando por punições que geram prejuízo financeiro ou reputacional, até mesmo com a proibição de que a empresa realize qualquer atividade de Tratamento de Dados Pessoais, praticamente inviabilizando a continuidade do negócio.

Além disso, alguns critérios poderão ser considerados pela ANPD para a aplicação de penalidade, como a boa-fé e a cooperação do Agente de Tratamento infrator, além da adoção de políticas de boas práticas e governança e a pronta adoção de medidas corretivas.

Como referência, vale citar algumas sanções que foram aplicadas na União Europeia com base no GDPR, mas que podem servir como alerta de como a ANPD poderá atuar no Brasil.

	ETid-1157	ESPANHA	28-04-2022	40.000	Working Capital Management España, SL	Arte. 6 (1) GDPR	Base legal insuficiente para o processamento de dados	link
Autoridade	Autoridade Espanhola de Proteção de Dados (aepd)							
Setor	Finanças, Seguros e Consultoria							
Resumo	A DPA espanhola (AEPD) impôs uma multa de 40.000 euros à agência de informação de crédito Working Capital Management España, SL. Um titular de dados apresentou uma reclamação à AEPD contra a empresa. Terceiros fraudulentos fizeram um empréstimo com a NBQ Technology, SAU em nome do titular dos dados sem que o titular dos dados realmente celebrasse um contrato. Depois que o titular dos dados posteriormente não fez pagamentos, a NBQ divulgou as informações do titular dos dados à Gestão do Capital de Giro. A AEPD determinou que a Working Capital Management, procedeu ao tratamento ilegal dos dados do titular dos dados desde que os dados pessoais foram inseridos nos sistemas de informação da empresa sem verificar se o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.							
URL direto	https://www.enforcementtracker.com/ETid-1157 (Copiar:) | URL curto: https://etid.link/ETid-1157							

Fonte: https://www.enforcementtracker.com/. Acesso em 23/05/2022.

	ETid-1170	ROMÊNIA	18-05-2022	5.000	Kredyt Inkaso Investments RO SA	Arte. 5 GDPR, art. 6 GDPR, art. 9 GDPR, art. 33 GDPR	Base legal insuficiente para o processamento de dados	link
Autoridade	Autoridade Nacional de Supervisão da Romênia para Processamento de Dados Pessoais (ANSPDCP)							
Setor	Finanças, Seguros e Consultoria							
Resumo	A DPA romena multou a Kredyt Inkaso Investments RO SA em 5.000 euros. Um titular de dados apresentou uma reclamação à DPA contra o controlador por ter divulgado seus dados pessoais e os de seu filho menor a instituições médicas sem autorização e sem que o titular dos dados tenha qualquer relação com as instituições. Durante sua investigação, a DPA descobriu que o controlador havia divulgado dados como endereço residencial, status profissional, bem como dados do contrato de trabalho. Além disso, o DPA descobriu que o controlador não havia notificado o DPA da violação de dados em tempo hábil exigido pelo art. 33 RGPD.							
URL direto	https://www.enforcementtracker.com/ETid-1170 (Cópia:) | URL curto: https://etid.link/ETid-1170							

Fonte: https://www.enforcementtracker.com/. Acesso em 23/05/2022.

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 de 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.

CAPÍTULO XIX
CONCLUSÃO

A Lei Geral de Proteção de Dados Pessoais, conforme explicado no Capítulo I, é a primeira legislação brasileira específica a tratar sobre a proteção de Dados Pessoais. Após sua publicação, diversos órgãos reguladores passaram a adequar suas resoluções, reeditando normas e atualizando regulamentações para incluir a necessidade de cumprir a LGPD, além de estabelecerem regras específicas para os Tratamentos de Dados Pessoais nos respectivos setores.

Assim, apesar de ser a legislação específica sobre o tema, a LGPD não é a única lei que deve ser cumprida quando a questão envolver proteção de Dados Pessoais. Principalmente em setores regulados, como no caso do setor bancário, diversas normas do BACEN e da CVM (como a Res. CMN 4893/21, de Segurança Cibernética) trazem obrigações relacionadas à proteção de Dados Pessoais, que devem ser atendidas em complementação às disposições da LGPD.

É importante reforçar que as disposições da LGPD não foram criadas para impedir o Tratamento de Dados Pessoais, mas sim para dispor “a regra do jogo”, definindo as responsabilidades das empresas nos Tratamentos de Dados Pessoais.

Para assegurar que os Tratamentos realizados pela empresa estarão de acordo com as disposições de proteção de Dados Pessoais, sugere-se a adoção de um Programa de Governança em Privacidade, composto de políticas, normas e procedimentos adotados internamente, de forma a organizar as atividades da empresa com as exigências da legislação aplicável.

Por fim, é interessante destacar que a conformidade com a LGPD não é uma meta fixa, isso é, um objetivo que, uma vez atingido, estará validado para sempre. Estar em conformidade com a LGPD demanda um esforço contínuo, por meio de acompanhamento, atualização e revisão periódica do Programa de Governança em Privacidade.

Nesse sentido, o presente Manual pode ser utilizado como apoio informativo e educacional para a conscientização e identificação de pontos de atenção relativos ao Programa de Governança em Privacidade, mas não substitui e nem deve ser entendido como aconselhamento jurídico.

CAPÍTULO XX
PERGUNTAS FREQUENTES

1) Quando a LGPD não se aplica?

De acordo com seu artigo 4º, a LGPD não é aplicável 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.

Além disso, é importante destacar que a LGPD é aplicável apenas ao Tratamento de Dados Pessoais, vinculados a um Titular. Ou seja, qualquer dado que permita identificar, direta ou indiretamente um Titular, estará sob o escopo da lei. Contudo, se os dados estiverem relacionados a uma pessoa jurídica, não serão considerados Dados Pessoais e, por consequência, não incidirá a LGPD, **exceto se a documentação tiver alguma informação sobre a pessoa responsável pela empresa (como sócio, diretor, acionista etc.).**

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.

2) Quais são as principais categorias de Titulares envolvidos no Tratamento?

Cada atividade de Tratamento terá uma categoria de Titular diferente, a depender do contexto de cada atividade. Contudo, é possível indicar as principais categorias de Titulares de Dados Pessoais que geralmente estão presentes nas atividades de Tratamento comuns de um Controlador:

- Clientes;
- Prospects/leads;
- Colaboradores do Controlador;

- Dependentes dos colaboradores;
- Candidatos de processos seletivos;
- Colaboradores de prestadores de serviço e parceiros; e
- Representantes legais de outros Agentes de Tratamento;

3) Existem dados pessoais que exigem mais proteção do que outros?

Sim, o Tratamento de algumas categorias de Dados Pessoais pode oferecer maiores riscos de danos aos respectivos Titulares e por isso são considerados pela LGPD como "Dados Pessoais Sensíveis".

Os Dados Pessoais Sensíveis são aqueles previstos expressamente na LGPD como sendo 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.

É importante observar, contudo a diferença entre um Dado Pessoal Sensível puro e um Dado Pessoal que pode revelar outro Dado Pessoal Sensível. É o caso da fotografia, que, por si só, não é um Dado Pessoal Sensível. Contudo, é possível o Tratamento da mesma fotografia para a extração do perfil biométrico da face daquele Titular, gerando um Dado Pessoal Sensível. Nesses casos, apesar de ser um Dado Pessoal simples, caberá ao Controlador a análise da necessidade de proteção adicional ao Tratamento da fotografia.

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

É possível realizar o reaproveitamento das bases existentes para desenvolver e/ou ofertar novos produtos ou serviços. Contudo, é necessário bastante cuidado nesse Tratamento.

De forma geral, sempre que os Dados Pessoais tiverem sido coletados com base no legítimo interesse ou para a execução de contrato, será necessário avaliar se há uma **legítima expectativa** do Titular de que aquele Tratamento posterior ocorra, além de verificar o atendimento aos princípios da LGPD – principalmente os da transparência, finalidade, adequação e necessidade.

Contudo, se os dados foram coletados com base no consentimento para um uso específico e esse consentimento não previa o desenvolvimento de novos produtos ou serviços, a obtenção de um novo consentimento do Titular poderá se revelar necessária para garantir a conformidade do Tratamento.

5) Posso usar dados públicos à vontade?

Dados Pessoais publicamente disponíveis – seja porque foram tornados manifestamente públicos pelo Titular, seja porque encontram-se em bases de acesso público – não deixam de ser Dados Pessoais. Nesses casos, a LGPD permite o Tratamento destes Dados Pessoais, desde que o Tratamento possa ser enquadrado em alguma das Bases Legais previstas pela LGPD, além de ser necessário observar todos os direitos dos Titulares e os princípios estabelecidos pela lei.

Além disso, e principalmente, o Tratamento de Dados Pessoais publicamente disponíveis deve considerar a boa-fé, a finalidade e o interesse público que justificaram sua disponibilização. Ou seja, **o Tratamento de um número celular de contato, por exemplo, publicamente disponível em site de órgão de classe (como OAB) não deve ser utilizado para fins de marketing, já que a finalidade e o interesse público na disponibilização** desse Dado Pessoal é incompatível com seu uso para envio de mensagens de marketing.

6) E quanto aos dados anônimos, posso usar à vontade?

Dados anônimos não são considerados Dados Pessoais, por não possuírem a capacidade de identificar um Titular, e, a princípio, não estão sujeitos à LGPD. Contudo, é importante verificar se os Dados Pessoais podem realmente ser considerados anônimos, já que, em muitas ocasiões, aparentes anonimizações de Dados pessoais podem ser facilmente revertidas.

Por exemplo, há situações nas quais os Dados Pessoais passam por procedimentos que removem identificadores pessoais (como nome e CPF), que são substituídos por números, códigos ou *hashes*, criando-se uma outra base de dados.

Porém, se alguma pessoa tiver acesso à base "anonimizada" e à base original identificada, ou então se ela puder cruzar informações de outras bases de dados às quais têm acesso para identificar os Titulares, essa base de dados supostamente anonimizada estará sob o escopo da LGPD, pois é possível a identificação dos Titulares.

De acordo com a LGPD, os Dados Pessoais somente serão considerados como anonimizados se o procedimento for irreversível, mesmo mediante a aplicação de meios próprios (mesmo procedimento de anonimização) ou por meio de esforços razoáveis (como tempo e custo necessários para reverter o procedimento de anonimização, considerando as tecnologias disponíveis).

7) Quando devo comunicar um incidente de segurança?

De acordo com a LGPD, a obrigação de comunicar um incidente de segurança existe

sempre que o incidente possa acarretar risco ou dano relevante aos Titulares de Dados Pessoais. Essa comunicação deve ocorrer tanto à ANPD quanto aos respectivos Titulares afetados.

A ANPD, contudo, ainda não regulamentou quais são os critérios específicos que caracterizam "riscos" ou "danos relevantes" aos Titulares. Assim, a definição dependerá da análise do próprio Controlador, que deverá decidir se o incidente deve ser comunicado ou não.

Enquanto não há a regulamentação do tema, a ANPD recomenda que os casos nos quais existem dúvidas sobre os riscos ou danos sejam notificados, já que a subavaliação do risco e/ou do dano ao Titular poderá gerar uma nova desconformidade com a LGPD (além daquela causada pelo incidente).

8) Preciso adequar os contratos já vigentes com cláusulas de proteção de Dados Pessoais?

Apesar de não existir uma obrigação expressa na LGPD exigindo que os contratos sejam adequados, tal atitude é vista como uma boa-prática no mercado, uma vez que demonstra que o Controlador está atento à necessidade de observar a legislação de proteção de Dados Pessoais em todas as relações que possui com terceiros.

O primeiro passo para essa adequação é a revisão do contrato, para identificar os seguintes pontos, que auxiliarão na definição das cláusulas que serão utilizadas:

- Há Tratamento de Dados Pessoais no objeto do contrato?
- Quem são as partes envolvidas na operação?
- Qual é a posição de cada parte enquanto Agente de Tratamento?
- Quais são as categorias de Dados Pessoais tratados? Há Tratamento de Dados Pessoais Sensíveis?
- Qual é a finalidade do compartilhamento dos Dados Pessoais com o terceiro?
- O quanto essa operação impactaria na atividade da empresa se fosse encerrada?
- Qual é o risco da operação? E o risco do terceiro?

Com essas respostas, a definição da posição dos Agentes de Tratamento e, consequentemente, das responsabilidades e das cláusulas que serão utilizadas torna-se mais simples, permitindo uma avalição precisa do contrato e da relação entre as partes.

9) 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 que foram criados de maneira automatizada, seja por inteligência algorítmica ou inteligência artificial.

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 do Titular por meio de inferências. Isso porque, quanto maior o volume e mais específicas as informações acerca de uma pessoa, 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.

10) A Instituição pode ser responsabilizada por atos de terceiros?

Sim. Todos os Agentes de Tratamento que estiverem diretamente envolvidos nas atividades de Tratamento de Dados Pessoais realizadas em violação à lei serão 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; (ii) embora tenham realizado o Tratamento de Dados Pessoais, 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, na escolha dos Operadores, é bastante importante trabalhar com parceiros comerciais que possuam programas de governança e mecanismos de conformidade com a LGPD, já que o Controlador responde diretamente perante os Titulares e à ANPD por quaisquer eventuais desconformidades do Operador com a LGPD.

No que se refere especificamente à contratação de serviços de processamento em nuvem e gerenciamento de risco cibernético nos termos da Res. CMN nº 4893/21, 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.

11) Eu sou enquadrado como Agente de Tratamento de Pequeno Porte. Quais regras devo seguir?

De modo geral, todos os Agentes de Tratamento, sejam eles enquadrados como sendo de pequeno porte ou não, devem seguir todas as disposições da LGPD.

Contudo, a Resolução CD/ANPD nº 02/22 trouxe um regime diferenciado para os Agentes de Tratamento de Pequeno Porte, que podem adotar com as seguintes flexibilizações:

- Fornecimento de informações quanto ao Tratamento de Dados Pessoais aos Titulares e atendimento das requisições envolvendo os direitos em formato:
  - Eletrônico;
  - Impresso; ou
  - Qualquer outro que assegure os direitos previstos na LGPD e o acesso facilitado às informações pelos Titulares;
- Associação, por meio de entidades de representação empresarial, por pessoas jurídicas ou pessoas naturais, para fins de negociação, mediação e conciliação de reclamações apresentadas pelos Titulares;
- Procedimento flexibilizado ou simplificado de comunicação de incidentes, nos termos da regulamentação específica da ANPD;
- Não obrigatoriedade da indicação de Encarregado pelo Tratamento de Dados Pessoais, observado o requisito de disponibilizar um canal de comunicação com o Titular para atender a legislação;
- Adoção de medidas administrativas e técnicas de segurança de acordo com requisitos mínimos a serem divulgados pela ANPD, inclusive por meio de guias orientativos, bem como possibilidade de adoção de política simplificada de segurança da informação;
- Prazos em dobro para:
  - Atender as solicitações de exercício de direito dos Titulares;
  - Efetuar a comunicação de incidentes à ANPD e aos Titulares, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional;
  - Fornecer a declaração completa dos Dados Pessoais tratados pelo Controlador; e
  - Apresentar informações, documentos, relatórios e registros solicitados pela ANPD;
- Possibilidade de apresentação em até 15 dias da declaração simplificada na resposta à solicitação de acesso aos Dados Pessoais pelo Titular.

CAPÍTULO XXI
CHECKLISTS

A avaliação de terceiros é um ponto crucial na hora de decidir quem será a outra parte na contratação de um fornecedor, prestador de serviço ou mesmo na hora de firmar convênios e parcerias empresariais.

O resultado da avaliação desses terceiros deve ser revisado, idealmente, pelo Encarregado da empresa que realiza a contratação, de modo que possa ser averiguada a conformidade do terceiro com os controles próprios da empresa contratante, permitindo a melhor definição relacionada com a assunção de riscos.

Os seguintes pontos devem ser avaliados para que o Encarregado possa elaborar um parecer quanto à possibilidade ou impossibilidade da contratação e o risco atrelado:

- Quais os sistemas e aplicativos de TI utilizados na atividade de Tratamento?
- A atividade de Tratamento usará Dados Pessoais para a tomada de decisões automatizadas sobre os Titulares?
- A atividade de Tratamento será realizada por subcontratados? Em caso positivo, quantos?
- Haverá armazenamento ou transferência de Dados Pessoais para outro país? Se sim, quais? Se EUA, para qual Estado?
- Existe um processo para descarte ou a devolução dos Dados Pessoais após o término do tratamento? Como é o processo e quais evidências são criadas?
- Existe o Registro das Operações de Tratamento de Dados Pessoais?
- Os colaboradores possuem cláusulas de confidencialidade em seus contratos de trabalho? Os prestadores de serviço assinaram acordos de confidencialidade?
- Existe um procedimento para assegurar o desenvolvimento de novos produtos ou serviços considerando a privacidade desde a concepção (Privacy by Design)?
- Há uma política ou norma de proteção de dados que aborde as formas adequadas de Tratamento de Dados Pessoais pelos colaboradores e terceiros, bem como que aloque responsabilidades sobre os Tratamentos?
- São gerados e armazenados os documentos que comprovam a regularidade da atividade de Tratamento de Dados Pessoais (como RIPD, LIA, gestão de consentimento)?
- Existe procedimento periódico de avaliação do Programa de Governança em Privacidade de terceiros com quem guarda vínculo para execução das atividades de Tratamento de Dados Pessoais?
- Existem procedimentos/mecanismos para garantir que as solicitações

de requisição dos Titulares sejam atendidas de forma segura, bem como comunicadas, quando aplicável, à contratante?

o Há uma Política de Segurança da Informação atualizada e implementada, com revisão periódica, bem como a adoção de outros controles de segurança relacionados?

o São adotadas normas de acesso restrito e controles de autenticação no ambiente onde se tratam Dados Pessoais?

o Um plano para garantir a disponibilidade dos dados, por exemplo um plano de backup e restore, foi desenvolvido e implementado?

o Existe um plano de respostas a incidentes de segurança, plano de continuidade de negócios e condução de testes de recuperação após incidentes?

o A criptografia nos dispositivos que irão armazenar Dados Pessoais é adotada?

o Os contratos da contratada possuem cláusulas revisadas sobre proteção de Dados Pessoais? Os contratos já existentes estão sendo aditados com essas cláusulas?

o Existem mecanismos/procedimentos que requeiram a comunicação/notificação da contratante caso haja um tratamento indevido por parte de um subcontratado?

o O procedimento formal de reporte ao Controlador, à ANPD e/ou aos Titulares, quando cabível, em caso de incidentes de segurança que envolvam Dados Pessoais foi elaborado e implementado?

o Quais os atestados ou certificações de Segurança da Informação ou Privacidade que a empresa possui (ex. SOC1, SOC2, ISO 27001 etc)?

Checklist De Avaliação De Maturidade

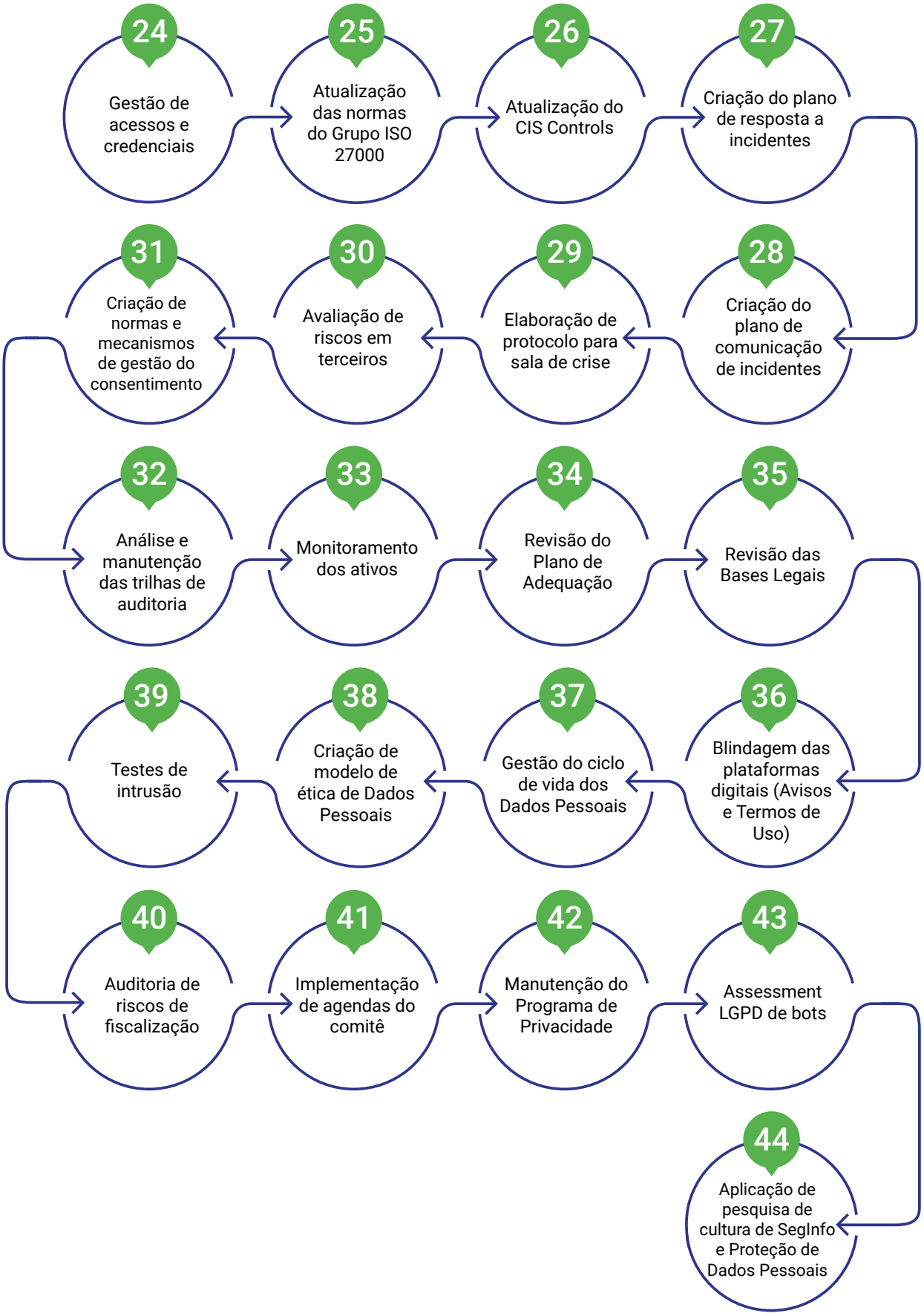
Para avaliar a maturidade do Controlador, indicamos a verificação da checklist a seguir, para permitir o entendimento do estado atual da empresa em comparação com o que usualmente vem sendo implementado no mercado.

A checklist abaixo foi dividida em três fases. Enquanto o preenchimento dos indicadores das duas primeiras fases é essencial para atingir um nível de maturidade satisfatório em relação à proteção de Dados Pessoais, a terceira fase consiste basicamente em melhorias e manutenção do Programa de Governança em Privacidade, e sua adoção revela-se como uma boa-prática.

Para essa avaliação, a seguinte matriz deve ser considerada:

Primeira Fase

Segunda Fase



Terceira Fase