quickLGPD
sua empresa adaptada

MANUAL DE BOAS PRÁTICAS E PROTEÇÃO DE DADOS PESSOAIS

com base na LGPD – Lei nº 13.709/2018

Neste Manual você encontrará os principais conceitos da legislação, medidas de segurança e boas práticas relacionadas ao tratamento de dados pessoais a serem aplicadas às suas rotinas de trabalho em sua organização

Histórico de Versões	
Ago-2021	Versão inicial
Set-2021	Inclusão de 2 novas boas práticas em VIII

Contents

I – APRESENTAÇÃO

Desde o ano de 2018, existe no Brasil uma Lei que disciplina a forma com que as empresas ou até mesmo pessoas físicas tratam dados de outras pessoas físicas quando fornecem produtos ou serviços, a Lei Geral de Proteção de Dados Pessoais (LGPD) Lei Federal nº 13.709.

quickLGPD é uma ferramenta cuidadosamente pensada e estruturada para que as empresas realizem sua adequação de modo personalizado (ajustado de acordo com a configuração do negócio), totalmente descomplicado, seguro e efetivo.

Contudo, também é muito importante que você e todos os colaboradores da sua organização conheçam os conceitos, definições e boas práticas relacionadas à LGPD, pensando nisso, elaboramos este Manual, para você seja capaz de aplicar a Lei em seu dia-a-dia, e orientar suas ações de acordo com o que é considerado correto sob o ponto de vista da adequada proteção aos dados pessoais em sua organização.

Em caso de dúvidas a respeito da LGPD e sua aplicação, você deve entrar em contato com o DPO (Data Protection Officer) ou EPD (Encarregado da Proteção dos Dados) que é o profissional responsável por garantir a conformidade da sua organização com a LGPD.

II – DEFINIÇÕES DA LGPD

2.1. Atores no processo de tratamento

a) Titular: É o **"dono" dos dados pessoais** que uma empresa trata. O titular necessariamente será uma pessoa física e deve estar viva, pois a lei não protege os dados de indivíduos já falecidos. O titular, possui também uma série de direitos, os quais analisaremos na sequência.

b) Controlador: A sua organização é um exemplo de controlador, quando ela é a **responsável por definir qual o tratamento** que será realizado com dados pessoais.

c) Operador: A sua organização poderá ser considerada um operador, quando for **contratada por uma empresa controladora, para manipular dados pessoais**, por exemplo, o provedor de acesso à *internet*, o desenvolvedor de *software*, o contador, o advogado etc. **Importante:** o operador deverá realizar o tratamento estritamente segundo as instruções fornecidas pelo controlador, que por sua vez é responsável por verificar a observância das próprias instruções e das normas sobre a matéria.

d) Encarregado (DPO: Data Protection Officer ou EPD: Encarregado de Proteção de Dados): É a pessoa física ou jurídica definida pelo controlador como canal de comunicação entre os titulares, a Autoridade Nacional de Proteção de Dados (ANPD) e o controlador.

e) ANPD (Autoridade Nacional de Proteção de Dados): É o órgão governamental responsável por elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, fiscalizar e aplicar sanções, servindo como ouvidoria, prestando aconselhamento jurídico sobre o tema.

2.2. Sobre os Dados Pessoais e Tratamento

a) Dados pessoais: São todas as **informações capazes de identificar** diretamente, ou que de alguma outra forma permitam identificar uma pessoa física. São exemplos de dados pessoais: o nome, sobrenome, número de RG, CPF, telefone, cartão de crédito, o endereço residencial ou de *e-mail*, um retrato em fotografia de alguém, assim como o perfil, hábitos e interesses de consumo.

Nem todos os dados coletados pelas empresas são considerados pessoais, como por exemplo, um número de CNPJ lançado em cadastro de cliente, que em regra não é um dado pessoal, bem como qualquer dado de especificação técnicas contábeis ou de produtos e serviços. Assim, sempre que a partir de determinada informação não for possível relacioná-la ou identificar uma pessoa, estaremos diante de um **dado não pessoal**, e, portanto, que não é protegido pela LGPD.

b) Dados pessoais sensíveis: São aqueles dados pessoais que podem **causar constrangimentos** ao seu "dono" (titular) caso sejam divulgados, como por exemplo: etnia, religião, vida sexual, saúde, convicção política, filiação sindical, bem como dado genético ou biométrico.

c) Tratamento de Dados: É considerado tratamento praticamente **qualquer manipulação de dados pessoais**, tanto em meios físicos, quanto digitais. A LGPD cita mais de 20 verbos que podem caracterizar o tratamento de dados, por exemplo: a coleta de endereço de *e-mails* de clientes para alimentação de lista de contatos da empresa é um exemplo de tratamento.

d) Dados Anonimizados: São dados que originalmente eram relativos a uma pessoa, mas que passaram por **processos que impossibilitaram realizar a identificação da pessoa** a qual se referiam.

III – PRINCÍPIOS DA LGPD

A LGPD trouxe também 10 (dez) princípios (fundamentos) que regem o tratamento dos dados pessoais. Esses princípios são importantíssimos, pois lhe darão a direção às melhores práticas de governança a serem adotadas para um tratamento de dados de forma correta, ou seja, em conformidade com a Lei.

Todo tratamento de dado pessoal a ser realizado em sua rotina dentro da organização precisa necessariamente se relacionado aos princípios da LGPD.

Importante: Caso constate que algum princípio não é, ou não está sendo observado em alguma rotina da sua organização você deve **necessária e imediatamente** contatar o DPO, que é o profissional responsável por avaliar a situação e implementar as melhorias necessárias, pois como veremos adiante, o descumprimento da LGPD pode gerar às empresas sérias consequências.

1/10 - FINALIDADE

- O tratamento deve ser feito com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento pelo controlador, inclusive posteriormente, de forma incompatível com essas finalidades.

2/10 - ADEQUAÇÃO

- Obrigatoriedade de que o tratamento seja feito de acordo com aquelas finalidades informadas ao titular e de acordo com o contexto do tratamento informado.

3/10 - NECESSIDADE

- Limitação do tratamento e dos dados coletados ao mínimo necessário para a realização de suas finalidades, de modo proporcional e não excessivos em relação às finalidades do tratamento de dados.

4/10 - 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 em poder do controlador.

5/10 - QUALIDADE DOS DADOS

- Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados tratados, de acordo com a necessidade e para o cumprimento da finalidade do tratamento.

6/10 - TRANSPARÊNCIA

- Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

7/10 - 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 divulgação.

8/10 - PREVENÇÃO

- Adoção de medidas para prevenir a ocorrência de danos ao titular em virtude do tratamento de dados pessoais.

9/10 - NÃO DISCRIMINAÇÃO

- Impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

10/10 - RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

- Demonstração, pelo controlador, 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.

IV – APLICABILIDADE DA LGPD

A LGPD se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que os dados pessoais sejam coletados ou o tratamento seja realizado no território nacional ou, ainda, que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional.

Importante: A LGPD não se aplica ao tratamento de dados pessoais realizado para fins particulares e não econômicos, jornalísticos, artísticos, acadêmicos ou para fins de segurança pública, defesa nacional e investigações penais.

V – BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Além dos princípios norteadores da LGPD, a Lei dispõe ainda de bases legais, estabelecendo que o tratamento de dados pessoais **somente** poderá ser realizado nas hipóteses a seguir, sendo que não há uma base legal melhor que outra, e sim a **mais indicada** para cada situação de tratamento.

Importante: Caso constate que algum processo de tratamento de dado pessoal realizado por sua organização não observa nenhuma das bases legais a seguir, você deve **necessária e imediatamente** contatar o DPO, que é o profissional responsável por avaliar a situação e implementar as melhorias necessárias, pois como veremos adiante, o descumprimento da LGPD pode gerar às empresas sérias consequências.

CONSENTIMENTO

Declaração clara e expressa de uma pessoa manifestando concordância com o uso dos seus dados

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADOR

Armazenamento de dados pessoais para a emissão de nota fiscal, transmissão de dados de colaboradores para autoridades governamentais

EXECUÇÃO DE POLÍTICA PÚBLICA

REALIZAÇÃO DE ESTUDOS POR ÓRGÃOS DE PESQUISA

EXECUÇÃO DE CONTRATOS

Substitui o consentimento e resguarda o controlador para manter os dados fornecidos pelo titular enquanto durar a vigência do contrato

EXERCÍCIO REGULAR DE DIREITOS

O controlador pode utilizar os dados para o exercício regular de direitos em processo judicial, administrativo ou arbitral

PROTEÇÃO DA VIDA

Com o intuito de proteger a vida ou a incolumidade física do titular dos dados ou de terceiros, desde que devidamente comprovada essa necessidade e exposta a finalidade do tratamento

TUTELA DA SAÚDE

Em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

INTERESSE LEGÍTIMO DO CONTROLADOR OU TERCEIRO

Desde que a finalidades seja legítima e sejam utilizados apenas os dados estritamente necessários

PROTEÇÃO DO CRÉDITO

A LGPD permite realizar o tratamento de dados pessoais para a prevenção a fraudes

VI – TRATAMENTO DE DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

O tratamento de dados pessoais de crianças e adolescentes deverá ser realizado com o **consentimento específico e em destaque** dado por pelo menos um dos pais ou responsável legal do menor.

VII – DIREITOS DOS TITULARES

A LGPD confere uma série de Direitos aos titulares de dados, que por sua vez devem ser observados pelo controlador, que atenderá as requisições dos titulares em prazo razoável, dentre as quais:

- Confirmação da existência de tratamento de dados pessoais do titular;
- Acesso do titular aos seus dados pessoais tratados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- Portabilidade dos dados a outro fornecedor de serviço ou produto;
- Eliminação dos dados pessoais tratados com base consentimento;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
- Revogação do consentimento.

VIII – MEDIDAS DE SEGURANÇA E BOAS PRÁTICAS

8.1. Fazer um mapeamento de dados

O mapeamento de dados, também chamado de *data mapping* é uma etapa essencial para garantir a conformidade de sua organização com a LGPD.

Trata-se do processo realizado para conhecer o ciclo de vida dos dados pessoais que sua organização trabalha, e deve ser realizado por todos os departamentos internos, com a finalidade de entender quais são os canais de coleta, locais de armazenamento, com quem são compartilhados, quem possui acesso, período de armazenamento e destinação final dos dados pessoais, classificação das operações de acordo com sua base legal e a sua finalidade, dentre outras questões.

Este procedimento, muito embora seja conduzido pelo DPO, juntamente com eventual Comitê composto por colaboradores da empresa especialmente eleitos para implementar a LGPD dentro da organização, deve ser adotado como um procedimento perene e rotineiro em todos os departamentos, pois sem o *data mapping*, não é possível identificar os riscos aos quais a empresa está exposta com o tratamento irregular de dados pessoais.

O registro do resultado deste mapeamento é fundamental para demonstrar a órgãos de fiscalização, como a ANPD, que o tratamento de dados é feito de forma legal e que a empresa está comprometida com a proteção de dados e a adequação à Lei.

8.2. Investir em Privacy by Design (privacidade incorporada ao projeto)

O *Privacy by Design* é conceito desenvolvido na década de 90, cuja proposta central é incorporar a privacidade e a proteção de dados pessoais em todos os projetos desenvolvidos pela organização, desde a sua concepção.

A LGPD, por sua vez, também determina que os controladores adotem medidas de segurança desde a fase de concepção do processo, produto ou serviço até a sua execução, uma das facetas do *Privacy by Design*.

Outro aspecto importante do *Privacy by Design* é a prevenção ao invés de remediação, deve-se sempre prever e antecipar eventos que possam comprometer a privacidade dos titulares. Dessa forma é necessário monitoramento constante, análise de riscos e desenvolvimento de correções sempre que alguma possível falha seja identificada, tomando precauções para evitar que a mesma ocorra.

8.3. Anonimizar dados pessoais sempre que possível

Segundo a LGPD, a anonimização de dados é a “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”.

Ou seja, a anonimização é o processo de fazer com que seja impossível identificar uma pessoa a partir do dado disponível. Assim, deixando de ser dado pessoal, a informação fica fora do escopo de aplicação da LGPD.

Para as empresas, a anonimização é uma opção recomendada nas hipóteses em que ainda seja possível usufruir do valor da informação sem a necessidade de identificar o titular. Essa é uma situação comum, por exemplo, na realização de estudos estatísticos.

Um ponto importante a destacar é que, por lei, o processo de anonimização deve ser irreversível. Ou seja, o dado não pode ser restaurado nem recuperado, de modo a permitir a identificação do titular.

8.4. Escolher parceiros comprometidos com a proteção de dados

Por mais que uma organização invista em proteção de dados e privacidade, todos os esforços podem ser em vão caso os parceiros comerciais não adotem a mesma postura.

Um vazamento de dados ocorrido após uma falha de um parceiro comercial, por exemplo, traz implicações legais e danos de reputação inclusive para sua organização.

Portanto, é uma boa prática fundamental estabelecer critérios para avaliar e exigir o cumprimento de medidas de proteção de dados e privacidade de todos os parceiros.

Isso pode ser feito através de medidas jurídicas, com a revisão de contratos, a inclusão de cláusulas específicas e a assinatura de acordos de confidencialidade. No entanto, o ideal é que a organização vá além e procure entender, de fato, como seus parceiros tratam a questão da proteção de dados.

Alguns questionamentos iniciais antes de escolher um parceiro comercial podem auxiliar na avaliação em relação à maturidade deste em relação a privacidade e o grau de segurança de dados pessoais que ele possui em seus procedimentos: O parceiro já indicou um DPO (encarregado)? Adota medidas de proteção de dados e segurança da informação? Controla o acesso de colaboradores a dados pessoais? Treina a equipe para sensibilizá-la a respeito do assunto?

8.5. Atender os direitos dos titulares de dados

A LGPD estabeleceu uma série de direitos aos titulares dos dados, que podem a qualquer momento serem exercidos perante o controlador.

Por isso, é ideal que a organização já tenha de antemão estabelecido um processo de resposta às requisições dos titulares, possuindo um canal de comunicação com estes e padronizado suas respostas para cada tipo de solicitação bem como critérios para que a requisição seja atendida ou recusada.

Além disso, o processo para responder às demandas dos titulares deve preocupar-se com a confirmação da identidade do titular, sob pena de gerar um incidente de segurança.

8.6. Notificação de incidentes de segurança envolvendo dados pessoais

Toda organização precisa estar preparada para lidar com um incidente de segurança envolvendo dados pessoais. Vazamento, acesso indevido, alteração ou eliminação de dados, tratamentos irregulares, etc.

Portanto, é uma boa prática criar um protocolo interno dispondo que todos os incidentes de segurança envolvendo dados pessoais, devem ser imediatamente reportados ao DPO, que é o profissional responsável por tomar as providências necessárias face à ANPD e os titulares eventualmente atingidos pelo incidente.

8.7. Treinar e conscientizar a equipe

Treinamento e conscientização da equipe a respeito da proteção de dados pessoais, conforme as disposições da LGPD e boas práticas de mercado é uma eficiente forma de, não somente facilitar a adequação da organização como um todo à LGPD, mas também de reduzir incidentes de segurança envolvendo dados pessoais.

Afinal, uma equipe consciente do papel e das exigências da LGPD consegue identificar situações de tratamento irregular de dados, e atuar de forma preventiva, protegendo as informações com as quais a organização lida.

Além disso, treinar a equipe regularmente é uma forma de demonstrar à ANPD que a organização atua para garantir a conformidade com a Lei.

Recomendamos que os treinamentos sejam constantes, a fim de reiterar a equipe sobre as medidas necessárias à proteção de dados pessoais, bem como garantir que eventuais novos colaboradores tomem conhecimento da LGPD e da necessidade de observação das medidas assecuratórias, além de

atualizar todos os colaboradores sobre eventuais novidades legislativas a respeito de privacidade e proteção de dados.

8.8. Segurança da informação

A Segurança da informação é uma medida necessária para garantir a proteção de dados pessoais contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Além disso, consulte sempre o DPO ou departamento de Tecnologia da Informação quando houver dúvida a respeito da segurança na utilização de dispositivos eletrônicos, tais quais *smartphones*, *tablets*, *notebooks*, *pen drives* etc, especialmente os particulares, ou seja, aqueles dispositivos não fornecidos pela sua organização.

8.9. Cuidado com documentos da empresa em formato físico e digital

Todos os colaboradores da organização devem ter especial cuidado com todos os documentos, papéis e acesso visual a telas e sistemas informatizados da empresa que contenham dados pessoais. Para tanto, em hipótese alguma, ao se ausentar, deve-se deixar à vista, sobre a mesa de trabalho ou qualquer outro ambiente, documentos ou quaisquer outros papéis contendo dados pessoais ou informações da empresa, bem como sair da mesa de trabalho, por qualquer motivo que seja, e não bloquear o sistema operacional do computador, deixando seu acesso livre a qualquer terceiro, seja ele colaborador da organização ou não.

Além disso, devem todos os colaboradores observar integralmente eventuais regras e políticas de utilização de dispositivos eletrônicos da empresa, somente utilizando nestes equipamentos senhas dentro do padrão de segurança exigido pela organização, sendo estas pessoais e intransferíveis, sob pena de responsabilização do usuário por qualquer acesso não autorizado ao dispositivo.

8.10. Cuidados com a transmissão de dados pessoais e informações da empresa em comunicação com clientes, colegas de trabalhos e quaisquer terceiros

Todos os colaboradores devem ter especial cuidado com a transmissão de dados pessoais ou qualquer informação da empresa, em qualquer tipo e meio de comunicação eventualmente utilizado com clientes, colegas de trabalho ou quaisquer outros terceiros, seja em conversas e/ou reuniões formais ou informais, e especialmente por escrito, em papel, via *e-mail* corporativo ou qualquer outra aplicação que permita a transmissão telemática de dados pessoais e informações confidenciais da organização.

Os cuidados se estendem a necessidade de assegurar que os destinatários dos dados ou informações da organização que se pretende transmitir estão corretos.

IX – FISCALIZAÇÃO E SANÇÕES

Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na LGPD, ficam sujeitos a algumas sanções administrativas aplicáveis pela ANPD, além de outras de natureza judicial em razão de possíveis demandas de titulares levadas ao Poder Judiciário:

- Advertência com indicação de prazo para a medida corretiva;
- Multa simples de até 2% do faturamento limitada a R$ 50 milhões por infração;
- Multa diária com o mesmo limite acima; e
- Publicização da infração (após devidamente confirmada e apurada).

Além disso, outras autoridades públicas (como Ministério Público, Procon, Senacon, Bacen) há muito têm se socorrido na LGPD para exigir o correto tratamento de dados pessoais e buscar a punição, com multas altíssimas, por inconformidades e falhas das empresas.