

Manual da Lei Geral de Proteção de dados (LGPD)



Sumário

INTRODUÇÃO	1
O QUE É A LGPD?	2
CONCEITOS	4
PRINCÍPIOS GERAIS	6
DIREITOS DOS TITULARES	8
AGENTES DE TRATAMENTO	13
TRATAMENTO DE DADOS	17
PENALIDADES (SANÇÕES)	25
APLICAÇÕES	27
LGPD NO SERVIÇO PÚBLICO	30
RESUMO: PERGUNTAS E RESPOSTAS	34
FUNDAMENTOS LEGAIS	36



Introdução

O objetivo da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709, de 14 de agosto de 2018 – é garantir a proteção aos dados pessoais, respeitados os direitos fundamentais de liberdade e de privacidade, que possam ser eventualmente violados pela má utilização dessas informações, permitindo maior confiança em relação à coleta e ao uso de dados, maior segurança jurídica e, em consequência, o fomento ao desenvolvimento econômico e tecnológico da sociedade, na medida em que estabelece regras claras sobre proteção de dados pessoais.

A norma foi aprovada em 2018 e entraria em vigor a partir de 14 de agosto de 2020. Houve pedido de adiamento da vigência da lei para maio de 2021, mas a proposta foi rejeitada pelo Congresso, entrando a legislação em vigor em 18 de setembro de 2020.

A LGPD visa trazer segurança jurídica ao tratamento dos dados pessoais e privacidade, tanto no Brasil como na relação com outros países, e impõe obrigações a pessoas físicas e jurídicas.



O que é a LGPD?

Baseada no Regulamento Geral sobre Proteção de Dados (em inglês, GDPR) – norma que regulamenta a proteção de dados na Comunidade Europeia e países associados –, a LGPD foi criada com o objetivo fundamental de fiscalizar as organizações públicas e privadas quanto ao uso de dados e garantir a privacidade dos usuários.

A LGPD estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção e penalidades para o não cumprimento, alterando a Lei nº 12.965, de 23/04/2014, que regulamentava essas transações até então.

Abrangência

A LGPD abrange as operações de tratamento de dados realizados no Brasil ou a partir de coleta de dados feita no país por empresas brasileiras ou estrangeiras. Sua fiscalização e regulação ficam a cargo da Autoridade Nacional de Proteção de Dados (ANPD) do Governo Federal.

Considerando que o tratamento de dados pessoais ocorre em todas as esferas do GDF, terão que ser adotados procedimentos para a entrada, manipulação, armazenamento e descarte dos dados.

Para isso, deverão ser adequados contratos de prestação de serviços, legislação, normativos e procedimentos a serem adotados por todos os setores envolvidos.

Com relação ao ambiente de negócios, sejam eles públicos ou privados, a LGPD é uma oportunidade para adequar o ambiente de proteção de dados e privacidade, trazendo mais segurança às transações, gerando serviços de qualidade e novos negócios.



Sua adequação é uma tarefa multidisciplinar e demandará esforços e comprometimento de diversas áreas da administração do GDF, da cúpula da gestão pública e dos servidores que atendem a população todos os dias.

Funções da Autoridade Nacional de Proteção de Dados (ANPD):

» **Função Educativa:** A ANPD deverá ter o papel de fomentar a educação acerca da LGPD, demonstrando as diretrizes de interpretação da legislação, estimulando padrões para os serviços e produtos que facilitem o controle de titulares sobre seus dados pessoais, bem como realizando estudos, em conjunto com a sociedade, de quais são as melhores práticas de proteção de dados pessoais;

» **Função Fiscalizatória:** Este é, sem dúvidas, o papel principal de uma autoridade. Assim, espera-se que a ANPD edite normas e procedimentos, bem como esclareça quais são as melhores interpretações da legislação, além de fazer requisições aos agentes de tratamento de dados sobre o tratamento de dados pessoais;

» **Função Sancionatória:**
Pela própria disposição dos artigos da LGPD, a ANPD terá o poder de instauração de processo administrativo quando do descumprimento das obrigações e deveres previstos na Lei, e terá competência exclusiva na aplicação de sanções.



Conceitos



Titular dos Dados

Toda pessoa física a quem um dado pessoal se referir.



Dado pessoal

Toda informação relacionada a uma pessoa física identificada ou identificável. Nessa categoria, podemos dizer que os dados pessoais podem ser diretos, como, por exemplo, RG, CPF, endereço, nascimento; ou indiretos, que são dados que possivelmente identifiquem pessoas, como, por exemplo, localização geográfica, perfil de consumo, comportamental, preferências, cookies, IP.



Dado pessoal sensível

É todo 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. Aos dados pessoais sensíveis a LGPD prevê tratamento restrito e especial.



Dado anonimizado

O dado anonimizado é o dado pessoal relativo a um titular que não possa ser identificado, ou seja, a partir do dado anonimizado não é possível associar qualquer pessoa física.



Tratamento de dados

É toda e qualquer operação realizada com dados pessoais, desde a coleta até o seu descarte. O art. 5º, inciso X, da Lei menciona expressamente outros exemplos: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.



Operador dos dados

Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Por exemplo, um prestador de serviços de armazenamento em nuvem (Cloud Services) - Operador de Dados -, contratado por outra empresa ou organização - Controlador de Dados - para que preste somente o serviço de armazenamento de dados.



Encarregado

Pode ser uma pessoa física ou jurídica indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Princípios Gerais

A Lei Geral de Proteção de Dados estabelece que as atividades de tratamento de dados realizadas pelos agentes de tratamento **deverão** seguir princípios, os quais são traduzidos como fundamentos que orientam a compreensão, interpretação e aplicação das regras estabelecidas na Lei e que, como determina a LGPD, devem sempre ser considerados quando houver tratamento de dados pessoais.

Princípios mais importantes:

Princípio da finalidade, adequação e necessidade

Juntos, os princípios da **finalidade**, **adequação** e **necessidade** formam o tripé principal da LGPD. Isso se deve ao fato de que em atenção a esses princípios, os dados pessoais somente poderão ser coletados e tratados para propósitos **específicos** e **legítimos** que tenham sido **informados** ao titular de dados e sejam **compatíveis** com o contexto do tratamento, o qual deverá ser **limitado** ao mínimo de dados necessários para o atingimento daquelas finalidades que foram primariamente informadas ao titular.



A observância dos princípios referidos gera nos agentes de tratamento um dever de cautela antes de coletar, armazenar ou realizar qualquer tipo de tratamento de dados pessoais, devendo averiguar:

- » Se o titular dos dados foi informado de maneira **clara** e **específica** sobre como os dados serão tratados e para quais finalidades – o motivo do tratamento;
- » Se o tratamento dos dados é adequado ao contexto em que os dados foram coletados, ou seja, se está dentro das expectativas que o titular tinha quando do fornecimento dos dados;
- » Se realmente é necessário tratar aqueles dados para atingir determinada finalidade, podendo o controlador realizar tratamento de menor número de dados pessoais para conseguir aquela finalidade.



Princípio do livre acesso e da transparência

Inspirada no Regulamento Europeu, a Lei Geral de Proteção de Dados estabeleceu garantias aos titulares dos dados para que esses tenham acesso a informações claras e facilmente acessíveis sobre como seus dados são tratados, por quem e para quais finalidades.

A recomendação é a de que a linguagem deverá ser sempre a mais clara, objetiva, sucinta e específica nas políticas de privacidade ou em outros materiais semelhantes, facilitando, inclusive, o acesso a esses materiais para os titulares.

Os agentes de tratamento também deverão oferecer um canal de comunicação acessível para que os titulares de dados possam eventualmente esclarecer suas dúvidas e solicitar informações.

Princípio da governança e prevenção

Ao realizar tratamento de dados pessoais, torna-se imprescindível implementar medidas técnicas e administrativas que são capazes de efetivamente proteger os dados de acessos não autorizados, perda, destruição, alteração ou divulgação indevida, bem como prevenir quaisquer incidentes que possam causar danos aos titulares dos dados.

Exemplos de técnicas: criptografia, análise de arquitetura dos sistemas, controles de acessos, exclusividade e separação dos bancos de dados, entre outros.

Princípio da não discriminação

O princípio da não discriminação possui a finalidade de evitar que haja tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos.



Direitos dos Titulares



Direito de confirmação de tratamento

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



Direito de acesso

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



Direito de correção de dados incompletos, inexatos ou desatualizados

Um dos principais direitos do titular de dados pessoais é o direito à correção, ou retificação, das informações a seu respeito. Esse direito é derivado do princípio da qualidade dos dados, previsto no artigo 6º, V, da LGPD, pelo qual se garante aos titulares **“exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento”**.



Direito à anonimização, bloqueio ou eliminação dos dados

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



Direito à portabilidade

O titular poderá:

- » Receber os dados pessoais que forneceram a um controlador de modo estruturado, normalmente em formato interoperável (aquele que é capaz de transitar entre diferentes plataformas) ou de uso corriqueiro e que possa ser lido automaticamente por computadores, para que possam ser utilizados por outro fornecedor de serviço ou produto;
- » Exigir a transferência direta desses dados pessoais a outro fornecedor de serviço ou produto, igualmente em formato que possibilite a utilização dos dados pessoais pelo novo fornecedor.



Importante notar que nem sempre essa segunda hipótese será tecnicamente possível, tendo em vista a grande possibilidade de incompatibilidade de sistemas ou mesmo de estruturas de banco de dados entre os controladores, situação em que os dados pessoais deverão ser fornecidos diretamente ao titular.



Direito à eliminação dos dados tratados com consentimento do titular

O titular poderá exigir, **mediante requerimento expresso**, a eliminação dos dados pessoais tratados com o seu consentimento, exceto nas hipóteses previstas no artigo 16:

- » Cumprimento de obrigação legal ou regulatória pelo controlador;
- » Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- » Transferência a terceiros, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei;
- » Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.



Direito à informação do compartilhamento dos dados

A LGPD assegura aos titulares o direito de saberem quais entidades públicas e privadas o controlador realiza ou realizou uso compartilhado de dados. O GDF deverá estar preparado para responder a essas requisições por meio da manutenção de registros de tratamento de dados pessoais, como é exigido pelo artigo 37.

Um dos elementos mais complexos do uso compartilhado de dados encontra-se na obrigação imposta pelo §6º do art. 18, que estabelece que “(...) **o responsável deverá informar de maneira imediata aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento**”.



Direito à possibilidade do não fornecimento do consentimento

A LGPD impõe aos controladores, que utilizam o consentimento como base legal para o tratamento de dados pessoais, que informem aos titulares sobre:

- » A possibilidade de não fornecer consentimento, quando factível;
- » As consequências da negativa, que em boa parte das vezes poderá significar a impossibilidade de usufruir de determinado produto ou serviço.



Direito à revogação do consentimento

É dever dos controladores informar aos titulares que eles possuem o direito de revogar seu consentimento a qualquer tempo e como podem exercer esse direito, preferencialmente por meio de um procedimento rápido e simplificado e sem serem prejudicados.



Direito de petição

A LGPD estabelece que **o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional** (art. 18, §1º), de forma a deixar claro que o órgão responsável por receber eventuais queixas ou denúncias formuladas pelos titulares de dados pessoais é a ANPD.

Vale salientar que o §8º do artigo 18 aduz que **“o direito a que se refere o §1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor”**.



Isso não significa que organismos de defesa do consumidor possam exercer o mesmo papel da Autoridade Nacional. Entende-se que, em nome da facilitação de seus direitos, o titular pode peticionar a esses organismos, cuja função nesse contexto é limitada a receber a petição com a queixa ou a denúncia e encaminhá-la à Autoridade Nacional.



Direito de oposição

A LGPD, no §2º do artigo 18, prevê que **o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei**.

Resumidamente, toda vez que a base legal de tratamento de dados **não for o consentimento** e houver algum tipo de descumprimento das normas da Lei, o titular poderá 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.



Agentes de Tratamento

A LGPD prevê expressamente os papéis dos agentes de tratamento, os quais são definidos pela Lei como sendo os **“controladores”** e **“operadores”**.

Controlador

Pela definição legal, é quem exerce controle geral sobre as finalidades pelas quais os dados pessoais são e serão tratados, seja por si só, em conjunto ou em comum com outros agentes. Dito de outra maneira, será o controlador que decidirá o “porquê” e o “como” da atividade de tratamento de dados sendo, portanto, o agente responsável por todo o ciclo de vida dos dados – da sua coleta ao seu descarte.

Responsabilidades

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

Vale dizer que o controlador não apenas representa a figura central na proteção dos direitos dos titulares – devendo observar a legislação e garantir que as atividades de processamento exercidas por todos os agentes envolvidos estejam em conformidade com a lei – mas também exerce funções relevantes para **toda a cadeia de tratamento de dados**.



Principais deveres

- » Elaboração do relatório de impacto de dados pessoais;
- » Nomeação do Encarregado pelo tratamento de dados pessoais para atuar como canal de comunicação entre o controlador e a ANPD, bem como entre o controlador e os titulares dos dados;
- » Obtenção do consentimento específico do titular, quando necessário
- » Informação e prestação de contas, e pela garantia de portabilidade dos dados;
- » Garantia de transparência no tratamento de dados baseado em legítimo interesse;
- » Manutenção de registro das operações de tratamento de dados pessoais, especialmente quando baseado no legítimo interesse;
- » Reparação de danos patrimoniais, morais, individuais ou coletivos causados por violação à legislação de proteção de dados pessoais
- » Comunicação à Autoridade Nacional e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

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 poderá alterar a finalidade ou o uso do conjunto particular dos dados relacionados a determinado tratamento, devendo tratar tais dados de acordo com as instruções e dentro das finalidades definidas e impostas pelo controlador.

De modo ilustrativo, um operador poderá ter a liberdade de utilizar a sua experiência na área de operação de tratamento de dados, com seus conhecimentos técnicos sobre o assunto, para decidir como conduzir certas atividades em nome do controlador.

Responsabilidades

Apesar de o operador atuar em nome do controlador e obedecendo as suas decisões, é comum que o controlador de dados conceda ao operador um determinado grau de discricionariedade e liberdade sobre o processo de tratamento dos dados, permitindo que exerça controle sobre o modo como os dados serão tratados.

Nesse contexto, o operador poderá, por exemplo, exercer certo controle principalmente sobre os aspectos técnicos relativos a como um serviço específico será prestado.



O operador não poderá tomar quaisquer decisões relevantes sobre os dados, a exemplo: quais dados serão usados para quais finalidades; qual o conteúdo dos dados; ou de que forma tais dados serão utilizados. Esses tipos de decisões somente poderão ser tomadas pelo controlador, pois é ele quem possui poder decisório sobre os dados.

Encarregado (DPO)

É a pessoa indicada pelo controlador e pelo operador para atuar como **canal de comunicação** entre o controlador, os titulares dos dados e a ANPD.

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

Funções

- » Orientar servidores, funcionários ou colaboradores a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- » Receber comunicações da Autoridade Nacional e adotar providências;
- » Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- » Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.



Tratamento de Dados



O tratamento de dados pessoais somente poderá ser realizado nas dez hipóteses estabelecidas na Lei. Essas hipóteses são chamadas de bases legais para o tratamento de dados.

Consentimento

A principal base, e mais conhecida, é o **consentimento do titular**, ou seja, a concordância com o tratamento de seus dados pessoais para uma finalidade determinada.

Contudo, vale destacar que todas as bases legais são independentes entre si, ou seja, basta o controlador preencher uma delas que estará apto a realizar o tratamento dos dados pessoais.



Importante!

O consentimento precisa respeitar alguns requisitos para que ele seja considerado válido:



LIVRE

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

INFORMADO

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



INEQUÍVOCO

O consentimento deve ser demonstrado de maneira inequívoca. Isso pode ser feito por escrito ou por outros meios que demonstrem a vontade do titular, desde que não deixem dúvidas - por exemplo, gravação de uma ligação telefônica.

FINALIDADE DETERMINADA

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



Interesse Legítimo

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

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

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



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

Isso significa que, em tese, o tratamento de dados pessoais para finalidades atreladas a atividades de concessão de crédito e financiamentos, por exemplo, poderia ser realizado com fundamento no legítimo interesse, desde que observados os requisitos e os elementos indicados acima.

Na prática, sempre será necessária uma análise detalhada de cada operação e das maneiras e finalidades do tratamento para confirmar se é possível ou não utilizar o legítimo interesse como base legal.

Relatório de Impacto para Proteção de Dados Pessoais

Uma vez verificada a possibilidade de tratar dados pessoais com base no legítimo interesse, é necessário elaborar um relatório de impacto para a proteção de dados pessoais (Data Protection Impact Assessment – DPIA).

Esse relatório deve descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades e aos direitos dos titulares de dados, bem como medidas, salvaguardas e mecanismos de mitigação de risco adotados. A **Autoridade Nacional de Proteção de Dados** poderá solicitar a apresentação deste relatório.

Três elementos deverão ser considerados:

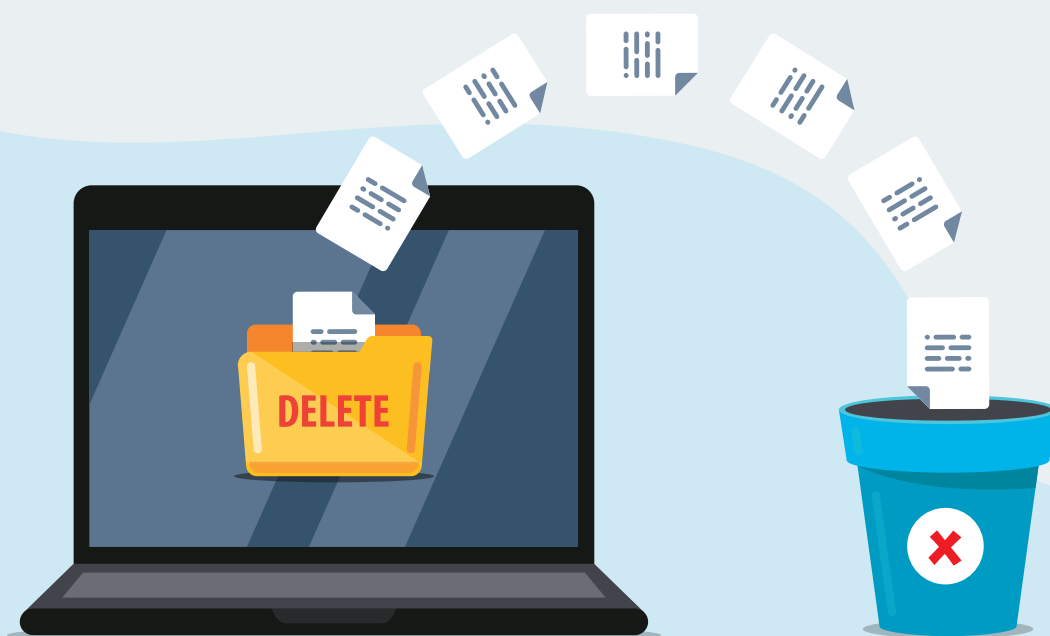
- » Identificar para quais finalidades o tratamento será realizado, e se essas finalidades são legítimas e consideradas a partir de situações concretas;
- » Verificar se é realmente necessário realizar o tratamento de dados para atingir aquela finalidade;
- » Balancear o interesse legítimo identificado com os direitos e as liberdades fundamentais dos titulares de dados que sejam impactados por esse tratamento.

Término do tratamento de dados

A Lei Geral de Proteção de Dados estipula a obrigatoriedade de eliminação dos dados pessoais ao término do tratamento.

Isso ocorre nas seguintes hipóteses:

- » Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- » Fim do período de tratamento;
- » Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público;
- » Determinação da autoridade nacional, quando houver violação da lei.





Importante!

A LGPD estipula que a conservação dos dados pessoais será autorizada em alguns casos:

- » Cumprimento de obrigação legal ou regulatória pelo controlador;
- » Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- » Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na lei;
- » Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Governança

No contexto de adequação à LGPD e para garantir o efetivo cumprimento das suas disposições, é altamente recomendável que os órgãos da administração direta e indireta do Governo do Distrito Federal 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**.

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.

É também muito importante que todos os processos, decisões, esforços e ações relacionados à governança de dados pessoais no GDF sejam documentados e mantidos em arquivo para apresentação à ANPD, se necessário.

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

Na prática, um programa de governança adequado deverá:

- 1 Demonstrar o comprometimento da organização em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.
- 2 Ser aplicável a todo conjunto de dados pessoais que estejam sob o controle da organização, independentemente do modo como se realizou a coleta.
- 3 Contar com planos de resposta a incidentes e remediação.
- 4 Ser adaptado à estrutura, à escala e ao volume das operações da organização, bem como à sensibilidade dos dados tratados.
- 5 Estabelecer políticas de salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade.
- 6 Ser atualizado constantemente com base em informações obtidas a partir do monitoramento contínuo e avaliações periódicas.

7 Ter o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular.

8 Estar integrado a sua estrutura geral de governança, que estabeleça e aplique mecanismos de supervisão internos e externos.

Transferência internacional

A Lei Geral de Proteção de Dados estabelece limitação à transferência internacional de dados pessoais para países que não ofereçam grau de proteção de dados pessoais adequados aos previstos na LGPD. Tais limitações se aplicam inclusive às transferências internacionais decorrentes de serviços de nuvem (*cloud*) e *datacentres* localizados em outros países.

Esse sistema é conhecido como “adequação”, e sua intenção é evitar que os dados pessoais protegidos pela Lei sejam enviados para países que ofereçam risco à privacidade dos seus titulares, sem que a Autoridade Nacional de Proteção de Dados possa intervir. Por isso, a ANPD deverá indicar quais países oferecem grau adequado de proteção aos dados pessoais.



Hipóteses permitidas

A LGPD prevê hipóteses nas quais são permitidas a transferência de dados para outros países mesmo que não tenham sido reconhecidos como adequados pela ANPD.

Um exemplo: as empresas que efetuam regularmente transferências internacionais deverão oferecer garantias por meio de contratos (cláusulas-padrão criadas pela ANPD ou normas corporativas globais criadas pela empresa e aprovadas, posteriormente, pela Autoridade).

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



Em termos práticos, antes de realizar qualquer transferência internacional de dados pessoais – mesmo que decorrentes da utilização de serviços em nuvem – é importante analisar cuidadosamente se a transferência é permitida e qual o mecanismo legal será utilizado para justificá-la.





Penalidades (Sanções)

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

Em outras palavras, além de eventual prejuízo financeiro, violar a LGPD poderá acarretar danos reputacionais significativos, prejudicando a imagem governamental perante seus cidadãos.

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

O artigo 52 da Lei Geral de Proteção de Dados prevê nove sanções:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

[...]

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.





Aplicações

Quando a LGPD não é aplicável?

- » Não se aplica ao tratamento de dados de pessoas jurídicas e nem de dados anonimizados, já que nenhum desses dados é considerado dado pessoal;
- » Não se aplica ao tratamento de dados pessoais realizado: por pessoa natural para fins exclusivamente particulares e não econômicos; para fins exclusivamente jornalísticos, artísticos ou acadêmicos; para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Existem dados pessoais que exigem mais proteção do que outros?

Sim. O tratamento de algumas categorias de dados pessoais oferece maiores riscos de danos aos respectivos titulares e por isso são tratados pela LGPD como “**dados sensíveis**”.

São considerados dados sensíveis pela LGPD:

- » Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política;
- » Filiação a sindicato ou organização de caráter religioso, filosófico ou político;
- » Dado referente à saúde ou à vida sexual;
- » Dado genético ou biométrico.



É importante observar que a fotografia do rosto de uma pessoa pode ser considerada dado biométrico.

O GDF poderá reaproveitar bases de dados existentes para desenvolver novos produtos ou serviços?

Este ponto merece um pouco de cuidado. 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, provavelmente será necessário obter um novo consentimento dos titulares de dados pessoais.

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

Posso usar dados públicos à vontade?

Os dados pessoais publicamente disponíveis – seja porque foram tornados públicos pelo titular, seja porque se encontram em bases de acesso público – **não deixam de ser dados pessoais**.

Nesses casos, a LGPD permite que os dados pessoais sejam utilizados sem a necessidade de obtenção de consentimento do titular, mas continua sendo necessário enquadrar esse tratamento em outras bases legais disponíveis e observar todos os direitos dos titulares de dados e os princípios elencados na Lei.

Resumidamente, é necessário dar transparência ao tratamento desses dados publicamente disponíveis e às suas finalidades; enquadrar o tratamento em uma base legal, franquear ao titular acesso a informações sobre quais dados pessoais estão sendo tratados, como e por qual motivo, entre outras obrigações aplicáveis.

E os dados anônimos?

Os dados anônimos não são considerados dados pessoais e, em princípio, **não estão sujeitos à incidência da Lei**. É importante, no entanto, confirmar se os dados poderão realmente ser considerados anônimos. Isso porque, em muitos casos, dados aparentemente anônimos podem ser reidentificados.

Exemplo são os procedimentos que removem identificadores pessoais, como o nome e o CPF, os quais são substituídos por números, códigos ou hashes, criando-se uma nova base de dados.

Porém, se o detentor dessa base de dados também tiver acesso à base original identificada (como, por exemplo, quando um mesmo órgão cria diferentes bases de dados com informações pessoais removidas para que diferentes áreas de negócio trabalhem com elas) ou possa cruzar informações de outras bases de dados às quais têm acesso para identificar os titulares, essa base de dados supostamente anonimizada será, em verdade, considerada apenas pseudonimizada, **aplicando-se normalmente a LGPD**.

O GDF poderá ser responsabilizado por atos de terceiros?

Sim. Todos os servidores ou órgãos que tomarem decisões e estiverem diretamente envolvidos nas atividades de tratamento de dados pessoais realizadas em violação à lei serão solidariamente responsáveis pelo ressarcimento dos danos causados aos titulares, salvo se puderem provar que:

- » Não realizaram o tratamento de dados pessoais que lhes é atribuído;
- » Embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados;
- » O dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.

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



LGPD no Serviço Público

De acordo com a LGPD, o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais.

Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observam o disposto em legislação específica, em especial as disposições constantes nas leis:

- » [Lei nº 9.507, de 12 de novembro de 1997 \(Lei do Habeas Data\)](#)
- » [Lei nº 9.784, de 29 de janeiro de 1999 \(Lei Geral do Processo Administrativo\)](#)
- » [Lei nº 12.527, de 18 de novembro de 2011 \(Lei de Acesso à Informação\)](#)

A quem se aplica?

- » Aos órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
- » Às autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios;
- » Aos serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público;
- » Às empresas públicas e às sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.
- » Às empresas públicas e às sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público.

Responsabilidades

Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.



Importante!

É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

- » Em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)
- » Nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
- » Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;
- » Na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

LGPD no GDF

Antes de iniciar o projeto para a conformidade com a LGPD é muito importante garantir o comprometimento da alta gestão da Secretaria, Autarquia, Fundação ou Empresa Pública. Talvez esse seja o fator mais importante para um projeto bem-sucedido.

Provavelmente, o ponto mais importante é que a conformidade com a LGPD não é opcional e as multas em potencial são vultosas.

O apoio dos gestores deve ser demonstrado publicando por Decretos, Portarias, Instruções Normativas ou processos específicos no SEI.

Desafios

O GDF deve garantir que a privacidade seja incorporada ao sistema durante todo o ciclo de vida, proporcionando a segurança das informações de ponta a ponta. Além disso, o Estado deve assegurar ao cidadão que as configurações de privacidade devem ser aplicadas por padrão, sem nenhuma entrada manual do usuário final nos serviços oferecidos.

Certamente, vamos nos deparar e identificar eventos críticos (com riscos mitigáveis) durante a autoavaliação que geram riscos de privacidade e proteção de dados nas instituições, nos cidadãos, nos fornecedores e nas demais partes interessadas do GDF.

É muito importante registrar esses eventos, áreas ou unidades de negócio, bem como seus processos relacionados. Portanto, a LGPD exige uma avaliação de impacto, uma identificação das probabilidades de ocorrência de vulnerabilidade e uma análise de riscos relevantes à privacidade e à proteção de dados.



Resumo: Perguntas e Respostas



Quem é o titular de dados pessoais?

É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

O que é a Autoridade Nacional de Proteção de Dados (ANPD)?

A ANPD é o “órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional”.

Quais as obrigações e os direitos?

Respeito com os titulares dos dados: as pessoas. As instituições devem ter cuidado desde a coleta até o descarte, oferecendo o máximo de transparência e de segurança. As pessoas terão direito a receber informações explícitas, legítimas e específicas sobre como os dados serão tratados. Os indivíduos poderão consultar, de forma fácil e gratuita, como seus dados estão sendo tratados. E, a qualquer momento, elas podem revogar o consentimento e exigir a eliminação dos dados.

O que é tratamento de dados pessoais?

A LGPD define tratamento de dados pessoais e toda operação realizada com dados pessoais, como as que se referem 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.

Quem são os agentes de tratamento de dados previstos na LGPD?

O controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Quem é o encarregado de dados pessoais ou DPO (Data Protection Officer)?

É a pessoa (física ou jurídica) indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

Quais as sanções previstas, em caso de descumprimento?

Multa de até R\$ 50 milhões. A suspensão, ou proibição, “do exercício de atividades relacionadas a tratamento de dados”.

Existem exceções?

A LGPD não se aplica ao tratamento de dados realizado por pessoas para fins exclusivamente particulares e não econômicos, ou para fins jornalístico e artístico; acadêmicos; de segurança pública; defesa nacional ou segurança de Estado; de investigações e repressão de crimes; ou provenientes de fora do país.



Fundamentos Legais

Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Constituição da República Federativa do Brasil. Brasília, DF, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Último acesso em: 06 jan. 2021

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 01, de 27 de maio de 2020. Brasília, DF, GSI/PR, 2020. Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215>. Último acesso em: 11 jan. 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Portaria Nº 93, de 26 de setembro de 2019. Brasília, DF, GSI/PR, 2019. Aprova o Glossário de Segurança da Informação. Disponível em: <http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Último acesso em: 19 dez. 2020.

____. GDF. Governadoria. Decreto nº 40.169, de 11/10/2019, Institui o Comitê Intersecretarial de Análise da Aplicação da Lei Geral de Proteção de Dados no Distrito Federal. Disponível em: sinj.df.gov.br. Último acesso em: 06 jan. 2021.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm#art1>. Acesso em: 09 nov. 2020.

BRASIL. Presidência da República. Casa Civil. Decreto Nº 9.637, de 26 de dezembro de 2018. Institui a Política de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/-Decreto/D9637.htm>. Último acesso em: 08 dez. 2020.

Referências

GOVERNO FEDERAL. Lei Geral de Proteção de Dados (LGPD). [Guia de boas práticas para implementação na Administração Pública](#). Acesso em: abr. 2020.

GOVERNO FEDERAL. Lei Geral de Proteção de Dados (LGPD). [Guias Operacionais para adequação à LGPD](#). Acesso em: dez. 2020

PARANÁ. Cartilha da Lei Geral de Proteção de Dados. Disponível em: <http://www.cge.pr.gov.br/Pagina/Cartilha-da-Lei-Geral-de-Protecao-de-Dados-LGPD>. Acesso em: jan. 2021

Kimberly Anastácio, Bruna Santos e Joana Varon. Aplicação da Lei de Proteção de Dados Pessoais. Rio de Janeiro, Junho 2020. <https://www.codingrights.org/>.



GDF

É tempo de ação.

CONTATO



Endereço

Palácio do Buriti, Sala
203- A, Brasília/DF
CEP: 70.075-900



Telefone

(61) 3425-4758



E-mail:

lgpd@buriti.df.gov.br



Site:

www.lgpd.df.gov.br