



CRCBA

CARTILHA

**LEI GERAL DE PROTEÇÃO DE DADOS
(LGPD)**



A thick green line starts at the top right, curves down and left, then curves down and right, then curves down and left, then curves down and right, ending at the bottom right. It forms a large, stylized 'C' or 'G' shape.

GLOSSÁRIO

Para efeitos desta Cartilha Informativa considera-se:

LGPD – Lei Geral de Proteção de Dados

ANPD – Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento dos dispositivos da LGPD. Responsável, também, pela aplicação de sanções previstas na LGPD.

TITULAR – pessoa física, a quem se referem os dados pessoais.

CONTROLADOR – pessoa Jurídica ou Física que coleta dados pessoais e toma todas as decisões em relação a forma e finalidade do tratamento dos dados.

OPERADOR/PROCESSADOR – pessoa Jurídica ou Física que realiza o tratamento de dados pessoais sob as ordens do Controlador.

AGENTES DE TRATAMENTO – Controlador e operador.

BANCO DE DADOS – Conjunto estruturado de dados pessoais que são objeto de tratamento.

ENCARREGADO(DPO) – pessoa Física indicada pelo Controlador para ser a ponte entre o Controlador, os Titulares e a ANPD (ou órgão que o substituir), bem como orientar os funcionários do Controlador sobre práticas de tratamento de dados, entre outras.

INCIDENTE DE SEGURANÇA – É a ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de Segurança da Informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação.

TRATAMENTO DE DADOS – O tratamento abrange um amplo conjunto de operações efetuadas sobre dados pessoais, por meios manuais ou automatizados. Inclui a obtenção, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o bloqueio ou a destruição de dados pessoais.

VAZAMENTO DE DADOS – Situações acidentais ou ilícitas de acessos não autorizados a dados pessoais.

ANONIMIZAÇÃO – utilização de técnicas de conversão de dados pessoais em dados anônimos, ou que assegurem, de forma robusta, que os dados não permitam a identificação da pessoa do titular. Também é definida como o processo pelo qual a informação pessoal identificável é irreversivelmente alterada, de tal forma que a informação pessoal identificável principal não pode mais ser identificada direta ou indiretamente.

BLOQUEIO – Suspensão temporária de qualquer operação de tratamento.

ELIMINAÇÃO – Exclusão de dado ou de conjunto de dados armazenados em bancos de dados, independentemente do procedimento empregado.

TRANSFERÊNCIA INTERNACIONAL DE DADOS – Transferência de dados pessoais para estrangeiro ou organismo internacional do qual o país seja membro.

PSEUDONIMIZAÇÃO – Tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

1. A nova Lei Geral de Proteção de Dados Pessoais - LGPD se aplica a quem?

A Lei Geral de Proteção de Dados (LGPD) se aplica a pessoas físicas e jurídicas de direito público e privado, que realizam o tratamento de dados, bem como às pessoas físicas que tem seus dados



coletados, independentemente do meio (físico ou digital), do país de sua sede ou do país onde estejam localizados os dados.

2. Quando a nova Lei Geral de Proteção de Dados Pessoais entra em vigor?

Conforme definição da Lei 13.853/2019, a Lei entra vigor em agosto de 2020, 24 meses após a publicação original, a fim de possibilitar às entidades públicas e privadas se adequarem as regras de usos e tratamento dos dados pessoais.

3. O que são dados pessoais?

Quaisquer informações que possam levar a identificação de uma pessoa natural, de maneira direta ou indireta (identificada ou identificável), por referência a um nome, a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, econômica, cultural ou social.

São exemplos de dados pessoais: nome, endereço, e-mail, identidade, CPF, dados de localização (função de dados de localização em telefones ou GPS), endereço de IP (protocolo de internet); testemunhos de conexão (cookies), etc.

4. O que são dados pessoais sensíveis?

São 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, à vida ou orientação sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

São aqueles que, se expostos ou compartilhados, podem causar impacto para a vida pessoal e/ou profissional, como por exemplo os dados registrados por um hospital ou médico.

5. O que são dados anônimos, dados anonimizados e dados pseudonimizados?

Dados anônimos são os dados pessoais cujo Titular não pode ser identificado.

Dados pseudonimizados são aqueles dados que, submetidos a tratamento, não oferecem a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Os dados anonimizados são aqueles identificados que, a partir da utilização de meios técnicos pelos agentes de tratamento de dados, passam a ser anônimos, ou seja, não passíveis de associação a um indivíduo, direta ou indiretamente.

Por não permitirem a identificação do seu respectivo Titular, os dados anonimizados não ficam sujeitos à aplicação da LGPD, exceto quando houver reversão do processo de anonimização ao qual tais dados foram submetidos.

6. A LGPD aplica-se apenas ao tratamento de dados pessoais coletados na Internet?

Não. A LGPD é aplicável a qualquer operação de tratamento de dados pessoais que tenham sido coletados dentro do território brasileiro ou que tenha como objetivo oferecer bens ou serviços a pessoas localizadas no Brasil, independentemente destes dados pessoais terem sido coletados offline ou online, em meios físicos ou digitais.

7. A LGPD apresenta alguma definição para “consentimento”?

Sim. A lei define consentimento como a “manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

8. Em quais casos de tratamento de dados pessoais, a LGPD não será aplicada?

São os casos em que o tratamento de dados pessoais for feito:

- (i) por uma pessoa física, para fins particulares, e não comerciais, p.ex., coleta de dados pessoais dos integrantes da família para a montagem de uma árvore genealógica;
- (ii) para fins exclusivamente jornalísticos, artísticos e acadêmicos;
- (iii) pelo Poder Público - no caso de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais.

Podem não estar sujeitos a aplicação da LGPD os dados provenientes e destinados a outros países, que apenas transitem pelo território nacional, sem que aqui seja realizada qualquer operação de tratamento e desde que o país de origem tenha nível de proteção similar ao previsto na LGPD.

9. Quais os principais atores no tratamento de dados pessoais, de acordo com a LGPD?

Os principais atores são o Titular, o Controlador, o operador e o encarregado.

TITULAR: Pessoa Física, a quem se referem os dados pessoais.

CONTROLADOR: Pessoa Física ou Jurídica que toma todas as decisões em relação a forma e finalidade do tratamento de dados pessoais. O controlador deve orientar e monitorar os procedimentos e condições para o tratamento por parte do operador.

OPERADOR/PROCESSADOR: Pessoa Física ou Jurídica que realiza o tratamento de dados pessoais sob as ordens do Controlador.

ENCARREGADO (DPO): Pessoa Física indicada pelo Controlador para ser o canal de comunicação entre o Controlador, os Titulares e a ANPD (ou órgão que a substituir).

10.O Titular tem direito de solicitar anonimização?

Sim. Constitui direito do Titular exigir a anonimização de seus dados, quando coletados de forma desnecessária, excessiva ou em desconformidade com a LGPD.

11.O Titular do dado pessoal pode solicitar que os seus dados sejam apagados?

Sim. A eliminação dos dados pessoais pode ser solicitada a qualquer tempo, mediante requisição formal do Titular, mesmo com relação aos dados que tenham sido tratados com consentimento prévio.

O Titular pode ainda exigir a eliminação quando houver coleta de dados desnecessários, excessivos ou que tenham sido tratados em desconformidade com as diretrizes da LGPD.

O Controlador do dado pessoal deverá acolher o pedido, exceto quando a LGPD autorizar a sua conservação, tais como para cumprimento de obrigação legal ou regulatória pelo Controlador, estudo por órgão de pesquisa ou para transferência a terceiros e uso exclusivo do Controlador, desde que anonimizados.

12. O Titular pode, sem motivação, se opor ao tratamento de seus dados pela Administração Pública?

Não. A oposição ao tratamento de dados não poderá ser imotivada, já que só poderá ser exercida em caso de descumprimento ao determinado na LGPD.

Além disso a LGPD determina a continuação do tratamento quando necessária a proteção do interesse público, mesmo após o recebimento de comunicação expressa do Titular.

13. É possível utilizar os dados pessoais armazenados antes da vigência da LGPD?

O recomendável é que seja implantado um programa para proteção de dados e coletadas autorizações/consentimentos específicos para o uso destes dados anteriormente armazenados, em conformidade com a LGPD.

Nos casos em que seja requerido o consentimento, podem ocorrer as seguintes situações:

- a) os dados poderão ser utilizados, desde que previamente consentido o seu uso, e se utilizados para a mesma finalidade para a qual foram coletados;
- b) no caso de alteração da finalidade, o tratamento somente poderá ser efetuado se houver novo consentimento ou se a finalidade for compatível com o consentimento original;
- c) havendo mudança de finalidade e esta não seja compatível com o consentimento original, o Controlador deverá informar previamente o Titular sobre as mudanças de finalidade, podendo o Titular revogar o consentimento, caso discorde das alterações.

Nos casos em que o tratamento de dados pessoais for baseado no interesse legítimo, o Controlador deve adotar medidas para garantir a transparência de tal tratamento.

14. Qual órgão será responsável pela aplicação e fiscalização do cumprimento da LGPD?

A LGPD estabelece que a Autoridade Nacional de Proteção de Dados – ANPD será o órgão responsável por zelar, implementar e fiscalizar o cumprimento da legislação de proteção de dados regulando a atuação de empresas e do setor público.

A ANPD, órgão vinculado a Presidência da República, é formada por um Conselho Diretor, responsável pela direção da ANPD e cujos integrantes são escolhidos pelo presidente do país; um Conselho Nacional, responsável por estudos, análises e sugestões ao Conselho Diretor, constituído de autoridades e membros da sociedade civil; uma Corregedoria, e unidades administrativas para a aplicação da lei.

A ANPD tem, entre outras atribuições, elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade; fiscalizar e aplicar sanções; promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança; e promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transacional.

15. Quando o Controlador e/ou o operador podem fazer o tratamento dos dados pessoais?

A LGPD estabelece um rol taxativo das hipóteses que autorizam o tratamento de dados pessoais, quais sejam:

- Mediante o consentimento do Titular;
- Para o cumprimento de obrigação legal ou regulatória pelo Controlador dos dados;
- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos;
- Para a realização de estudos por órgão de pesquisa, garantido, sempre que possível, que os dados pessoais permaneçam anônimos;
- Quando necessário para a execução de contrato ou de procedimentos contratuais preliminares;
- Para a proteção da vida ou da incolumidade física do Titular ou de terceiro;
- Para o exercício regular de direito em processo judicial, administrativo ou arbitral;
- Para atendimento de interesses legítimos do Controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do Titular que exijam a proteção dos dados pessoais;
- Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde, serviços de saúde ou por entidades/autoridades sanitárias;
- Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

16. O tratamento de dados pessoais sensíveis pode ser realizado em quais condições?

Os dados pessoais sensíveis podem ser objeto de tratamento quando o Titular ou seu representante legal autorizá-lo, mediante a formalização de consentimento para finalidades específicas.

Caso não haja consentimento do Titular, o tratamento dos dados pessoais sensíveis somente poderá ocorrer quando for indispensável para:

- a) Cumprimento de obrigação legal ou regulatória pelo controlador;
- b) Tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos;
- c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, que os dados pessoais permaneçam anônimos;
- d) Exercício regular de direitos;
- e) Proteção da vida ou da incolumidade física do Titular ou de terceiros;
- f) Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; e
- g) Garantia da prevenção à fraude e à segurança do Titular.

A LGPD não permite o tratamento de dados pessoais sensíveis para atender ao interesse legítimo do Controlador ou de terceiros ou mesmo para proteção do crédito, tal como ocorre com os dados pessoais em geral, não qualificados como sensíveis.

A Lei veda às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

A Lei também veda expressamente a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: (i) a portabilidade de dados quando solicitada pelo titular; ou (ii) as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

O tratamento de dados pessoais de crianças e adolescentes deve ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. A única hipótese em que a LGPD permite a coleta de dados pessoais

sem o consentimento de pais ou responsável legal é no caso da coleta necessária para realizar contato com os pais ou responsável legal.

17. É permitido pela LGPD, o uso compartilhado de dados entre órgãos da Administração Pública?

Sim. Entretanto, o uso compartilhado de dados pessoais pelo Poder Público deve atender as finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, como por exemplo informações ao INSS, e-social, fiscalizações, etc.

18. Existe disposição na LGPD sobre a transferência de dados entre o Poder Público e o setor privado?

A LGPD veda a transferência de dados entre o Poder Público e as empresas e instituições privadas, exceto nos seguintes casos:

- (i) em que os dados forem acessíveis publicamente;
- (ii) na execução descentralizada de atividade pública que exija essa transferência, exclusivamente para esse fim específico;
- (iii) Quando houver previsão legal e a transferência for respaldada em contratos, convênios ou acordos;
- (iv) se o objetivo for a prevenção de fraudes e de proteção dos titulares dos dados.

19. Em quais casos os dados pessoais poderão ser transferidos para fora do Brasil?

A transferência internacional de dados pessoais somente será permitida para os casos em que o país ou organismo internacional proporcionarem um grau de proteção de

dados adequado ao previsto na LGPD, ou quando forem oferecidas pelo Controlador garantias de cumprimento dos princípios, dos direitos e do regime da proteção da LGPD.

A transferência de dados também poderá ocorrer em outras hipóteses:

- (a) para fins de cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução;
- (b) para os casos em que for necessária para proteger a vida ou a integridade física do Titular dos dados pessoais ou deterceiros;
- (c) quando a autoridade nacional autorizar a transferência;
- (d) quando a transferência decorrer de acordo de cooperação internacional;
- (e) quando for necessária para a execução de política pública ou atribuição legal do serviço público;
- (f) quando o Titular tiver fornecido seu consentimento específico e em destaque para a transferência internacional;
- (g) quando servir para o cumprimento de obrigação legal ou regulatória pelo Controlador;
- (h) quando necessário para a execução de contrato;
- (i) quando servir para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

20. Como a LGPD protege as pessoas de decisões automatizadas, baseadas exclusivamente em meios tecnológicos?

O Titular tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Além disso, o Controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

Se, ainda assim, não forem fornecidas as informações por motivo de segredo industrial ou comercial, a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios no tratamento automatizado.

A defesa dos interesses dos Titulares poderá ser exercida em juízo, individual ou coletivamente.

21. Em caso de vazamento de dados, qual o procedimento previsto na LGPD?

A LGPD determina que o Controlador deverá comunicar tanto ao Titular quanto a ANPD sobre a ocorrência de algum incidente de segurança, que venha a resultar em um risco ao Titular. Assim, caberá ao Controlador implementar procedimentos ou práticas para gerir incidentes materializados e notificar brechas de segurança e vazamentos de dados.

Essa comunicação será devida nos casos em que dados pessoais tenham vazado acidental ou ilícitamente a destinatários não autorizados, que fiquem temporária ou permanentemente indisponíveis, ou ainda sejam alterados.

A notificação ao titular dos dados deve ocorrer sem demora injustificada, tendo a norma estipulado o prazo de 72 horas para a comunicação do ocorrido à Autoridade Nacional de Proteção de Dados.

Vazamentos e acessos não autorizados a dados pessoais podem ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o Controlador estará sujeito à aplicação das penalidades da LGPD.

22. Como o Titular deve proceder ao identificar o vazamento de seus dados?

Essa questão ainda depende da regulamentação. O Titular poderá entrar em contato com o Controlador do dado vazado, solicitando formalmente as devidas correções e controles.

23. Caso o tratamento de dados pessoais não ocorra de acordo com a LGPD, quem será responsabilizado?

O Controlador ou o Operador respondem por danos decorrentes de violação a LGPD.

O Operador responderá conjuntamente com o Controlador quando descumprir a LGPD ou quando não tiver seguido as instruções dadas previamente pelo Controlador.

A Autoridade Nacional poderá enviar ao responsável informe com medidas cabíveis para fazer cessá-la.

24. Quais são as penalidades que podem ser aplicadas àqueles que violarem a LGPD?

São as seguintes sanções administrativas, previstas na nova lei:

- I – advertência, com a indicação de prazo para adoção de medidas corretivas;
- II – multa simples de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, no último exercício, excluídos os tributos e limitada a R\$50.000.000,00, por infração;
- III – multa diária, observado o limite total a que se refere o inciso anterior;
- IV – publicização da infração, após apuração e confirmação;
- 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.

As sanções serão aplicadas de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerando sua gravidade e a natureza. Além

das sanções administrativas, o infrator poderá responder judicialmente por repercussões decorrentes do descumprimento da LGPD, individual ou coletivamente.

IMPORTANTE:

Esta cartilha foi atualizada em 25 de Outubro de 2020.





www.crcba.org.br