Guia LGPD

LEI GERAL DE PROTEÇÃO DE DADOS

www.rbaadv.com.br

Sumário

Introdução

A Lei nº 13.709/2018 sancionada em 14 de agosto de 2018 é a Lei Geral de Proteção de Dados Pessoais - LGPD. Ela representa um grande passo no que se refere à privacidade das pessoas.

Com isso, há uma integração do Brasil com os países que já possuem legislação específica para a proteção de dados.

Após a União Europeia sancionar a *General Data Protection Regulation – GDPR*- percebeu-se aceleramento para a entrada em vigor da lei específica no Brasil.

Em 27 de agosto de 2020, foi publicado o Decreto Federal nº 10.474/2020, que aprovou a Estrutura Regimental e do Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Dados Pessoais (ANPD), com composição já definida.

Esse Decreto dispõe que a ANDP detenha autonomia técnica e decisória, sendo que o objetivo traçado é a proteção dos direitos fundamentais da liberdade, privacidade e o livre desenvolvimento da personalidade de pessoa natural.

A Lei foi promulgada em 14/8/2018. O início de sua vigência ocorreu em 18 de setembro de 2020

Cabe lembrar que as penalidades tiveram a vigência postergada para 1º de agosto de 2021.

Em 10/2/2022 foi promulgada a Emenda Constitucional 115/22 que torna a proteção de dados pessoais como direito fundamental (Art 5º, LXXIX)

Nosso guia

Este guia traz as normas consolidadas na lei, as quais devem ser seguidas e adequadas, em sintonia com as regras determinadas pela Autoridade Nacional de Proteção de Dados (ANDP), que será a guardiã do cumprimento da Lei.

Por fim, com a intenção de proporcionar conhecimento para auxiliar na adequação a esta legislação, repassamos informações que servirão de guia.

Boa leitura!

Abrangência da lei

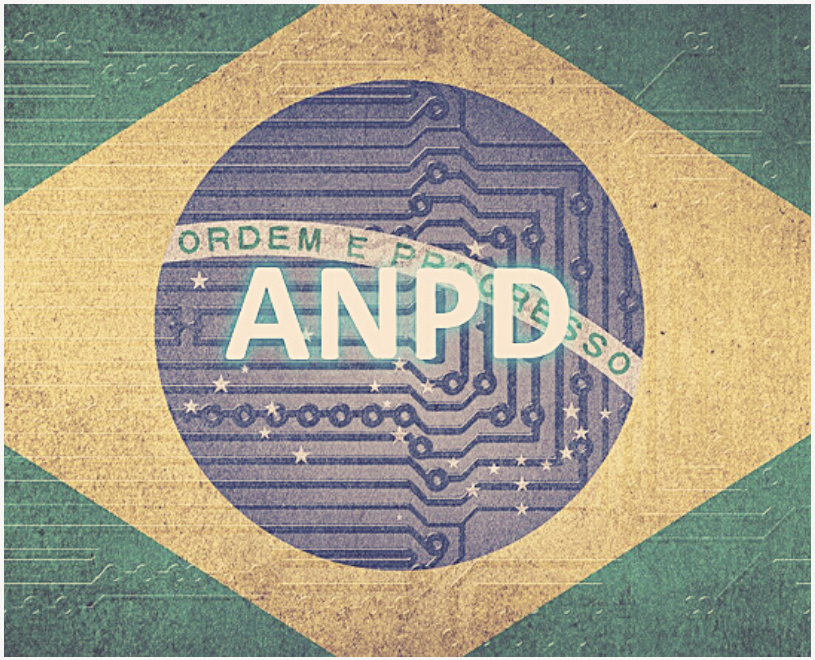
A lei geral de proteção de dados aplica-se ao Tratamento de Dados Pessoais acessados em todo território nacional, independentemente de o tratamento ocorrer no Brasil ou exterior.

Definições da LGPD

- Dado pessoal: informação relacionada à pessoa natural identificada ou identificável;
- Dado pessoal sensível: 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;
- Dado especial: são os dados de crianças (8 a 12 anos incompletos) e adolescentes (de 12 até 18 anos incompletos);
- Dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

- Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- Titular: pessoa natural a quem se referem os dados pessoais, que são objeto de tratamento;
- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- Encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador e operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
- Agentes de tratamento: o controlador e o operador;
- Tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

- **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
- **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- **Transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- **Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre estes e entes privados (reciprocamente) com autorização específica para uma ou mais modalidades de tratamento permitidas por estes entes públicos, ou entre entes privados;



- Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
- Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos, legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e
- Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Princípios da lei

BOA FÉ

Significa agir com lealdade, respeito aos interesses legítimos, agindo sem abuso, sem obstrução e sem causar lesão.

ADEQUAÇÃO

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento, evitando desvirtuação. Exemplo: O uso correto do nome do titular para firmar o contrato de trabalho.

FINALIDADE

O tratamento de dados deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com estas finalidades. Exemplo: em uma relação de consumo de produtos de telefonia, não se justifica coletar dados de saúde.

NECESSIDADE

Limitação do tratamento para a realização das finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Manter os dados até cumprir a finalidade da sua coleta. Exemplo: Coleta dos dados de responsáveis por menor, para cumprir cota de aprendiz.

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. Exemplo: (1) canal de comunicação.

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. Exemplo: (i) informar os dados de identificação do controlador.

SEGURANÇA

Utilização de técnicas e medidas administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Exemplo: (1) realizar *backup* dos dados pessoais; (2) proteger o ambiente físico onde conste dados pessoais.

NÃO DISCRIMINAÇÃO

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. Exemplo: não promover admissão (apenas) de pessoas do sexo feminino; não realizar a oferta de produtos ou serviços apenas para pessoas de determinada nacionalidade.

PREVENÇÃO

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Exemplos: (i) definir política de segurança; (ii) definir processos internos para o tratamento.

QUALIDADE DE 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. Exemplo: (i) cópia ilegível de um documento.

RESPONSABILIZAÇÃO/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. Exemplo: (i) registrar todas as atividades que envolvam dados pessoais.

Agentes de tratamento de dados

CONTROLADOR:

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

DEVERES DO CONTROLADOR: Adotar medidas de segurança, técnicas e administrativas, visando a proteção de dados pessoais nos termos da legislação. Atender as determinações exigidas pela ANP.

OPERADOR:

Pessoa natural ou jurídica, de direito público ou privado que realiza o tratamento de dados pessoais em nome do Controlador.

DEVERES DO OPERADOR: Cumprir com as instruções dos controladores, bem como adotar medidas técnicas e organizacionais apropriadas para garantir que o tratamento seja realizado em conformidade com a LGPD. Atender as determinações exigidas pela ANP.

Agentes de tratamento de dados

ENCARREGADO:

Pessoa física ou jurídica, indicada pelo controlador ou pelo operador dos dados pessoais para estabelecer a comunicação entre o controlador, os titulares dos dados e a ANPD.

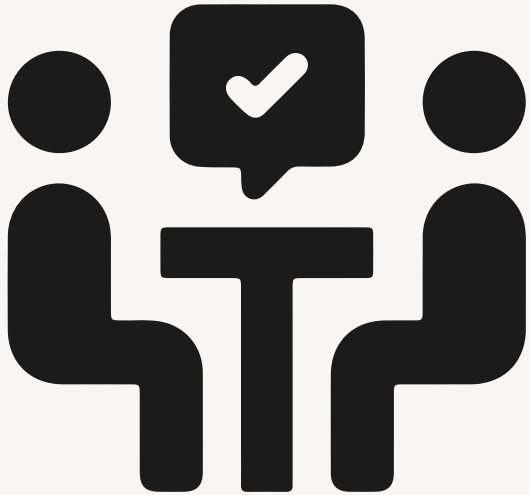
DEVERES DO ENCARREGADO: Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de Dados Pessoais; executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
O encarregado deverá ter sua identidade e informações de contato divulgadas publicamente, de forma clara, objetiva e de fácil acesso por meio de um canal de comunicação.

Responsabilidades do Controlador e Operador

CONTROLADOR OU OPERADOR que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

O operador responderá solidariamente em duas situações: caso descumpra as obrigações da legislação de proteção de dados pessoais ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador (salvo exceções do artigo 43 da LGPD).

O artigo 43, inciso III, da LGPD exonera os agentes de tratamento da responsabilidade quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro; e quando não realizarem o tratamento dos dados pessoais que lhes foram atribuídos.

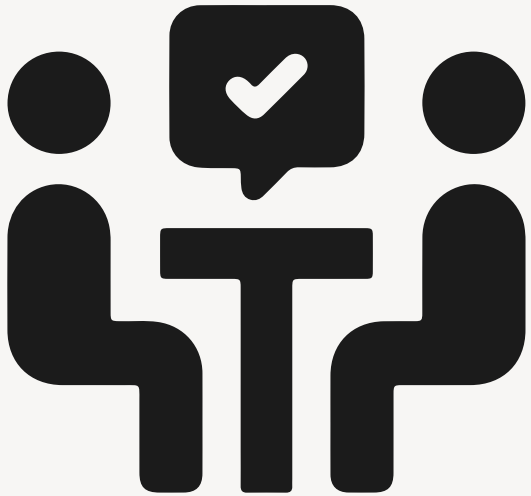


Responsabilidades do Encarregado

Quando houver falha na prestação do serviço desempenhado pelo **ENCARREGADO**, ele poderá ser responsabilizado. Ou seja, quando, diante das atribuições expostas nos incisos I, II, III e IV do parágrafo 1º do artigo 41 da LGPD e de outras normas complementares (parágrafo 3º do artigo 41 da LGPD), deixar de proceder a ato de sua competência e que, por ofício, deveria desempenhar/executar para a proteção dos danos pessoais.

No mesmo ínterim, o encarregado será responsabilizado pelos danos causados aos titulares de dados pessoais por sua ação ou omissão dolosa, quando verificar risco no tratamento de dados e deixar de sugerir e orientar funcionários para as boas práticas de proteção de dados.

A responsabilidade civil do encarregado deverá constar em contrato de prestação de serviços ou de trabalho (quando for o caso) a fim de resguardar os limites da atuação dentro da esfera legal, oportunidade em que o instrumento contratual deverá ser bastante claro nesse sentido.



Direito do titular de dados pessoais

O titular dos Dados Pessoais tem o direito de obter do controlador, a qualquer momento e mediante requisição (atendendo ao princípio da Boa-fé entre as relações), os seguintes direitos:

1 - Confirmação da existência de tratamento;
2 - Acesso aos dados;
3 - Correção de dados incompletos, inexatos ou desatualizados;
4 - Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
5 - Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
6 - Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
7 - Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
8 - Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
9 - Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei; e
10 – Peticionar contra o controlador perante a ANDP.
O titular ou seu representante legalmente constituído poderá exercer os seus direitos (supra) mediante requerimento expresso, sem custos, ao agente de tratamento.

Hipóteses legais para o tratamento de dados

CONSENTIMENTO: é uma das hipóteses legais para o tratamento de dados pessoais, sensíveis e especiais, que deve ser manifestado de forma livre, informada e a salvo de dúvidas pelo titular dos dados, por qualquer meio e em uma relação contratual, seja ela de consumo ou de trabalho (entre outras).

O consentimento por escrito deverá constar em cláusula, destacada das demais cláusulas contratuais. Igualmente, àquele prestado por "outros meios", como exemplo *token, login,* autenticação por *e-mail*, registro de áudio e vídeos (entre outros), é inequívoco à preservação da vontade do titular. Deverá ser compreensível e estar atrelado aos termos do tratamento de dados. A não observação da forma prevista para coleta do consentimento invalidará o negócio jurídico.

Ademais, tem-se que o consentimento só é válido se for direcionado a um fim específico ou determinado; termos genéricos devem ser eliminados. O consentimento poderá ser revogado a qualquer momento, mediante manifestação expressa do titular, por meios gratuitos e facilitados.

Para saber se a base legal será o consentimento é necessário fazer alguns questionamentos:

1. Qual o tipo de dado vou realizar o tratamento (sensível?, especial?, pessoal?)
2. Possuo finalidade definida?
3. O titular manifestou consentimento de forma livre e devidamente informada a finalidade?

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA: Toda vez que a relação jurídica assim o exigir, os dados pessoais poderão ser tratados, não podendo o titular se opor ao tratamento.

Esta base legal tem como fundamento o cumprimento de leis (federal, estadual, municipal), decretos, resoluções, Normas Coletivas de Trabalho, dentre outras. Observa-se que norma prevista em contratos entre particulares não poderá servir de fundamento para utilização desta base legal. Pergunta-se:

1. Há ordenamento legal que devo cumprir para que possa valer-se desta base legal para o tratamento de dados pessoais?
2. O titular do dado esta ciente de que há uma legislação a ser cumprida e por tal motivo o controlador é obrigado a realizar o tratamento dos dados pessoais?

EXECUÇÃO DE POLÍTICAS PÚBLICAS: A administração poderá realizar o tratamento de dados pessoais, desde que necessário para a execução de políticas públicas (saneamento básico, bolsa família...).

REALIZAÇÃO DE ESTUDOS DE PESQUISA: É considerado um órgão de pesquisa as entidades da administração pública direta ou indireta e as de direito privado sem fins lucrativos, como associações e fundações, sediadas no Brasil, que incluam em seu estatuto social a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

EXECUÇÃO DE CONTRATOS: Excetua-se a fase de formação do contrato, sendo que o tratamento deve ser realizado na execução do contrato. Logo, somente os dados pessoais indispensáveis à prestação dos serviços poderão ser tratados com base nessa hipótese legal. Perguntar-se:

1. Há um contrato a ser formalizado, já ajustado ou executado que contenha dados pessoais?
2. O titular do dado pessoal faz parte deste contrato?

EXERCÍCIO REGULAR DE DIREITOS: Essa hipótese é aplicável para o tratamento de dados necessário ao exercício regular de direitos do titular em processo judicial, administrativo ou arbitral, por quaisquer das partes envolvidas.

Pergunta-se: O tratamento de dados pessoais se faz necessário para o exercício de direitos do titular em processo judicial, administrativo ou arbitral?

TUTELA DA SAÚDE: O tratamento de dados, por esta hipótese, é bem mais restritivo, pois só podem se valer dela os profissionais da área de saúde ou entidades sanitárias.

INTERESSE LEGÍTIMO DO CONTROLADOR: Essa hipótese é aplicável para o tratamento de dados quando necessário para atender aos interesses legítimos do controlador, ou seja, da empresa, ou de terceiros.

Pergunta-se:

1. Qual o interesse legítimo do controlador? A empresa precisa coletar esses dados para executar suas atividades?

PROTEÇÃO DE CRÉDITO: Com o intuito de não criar riscos sistêmicos e de beneficiar o maior número de pessoas, a fim de gerar um movimento financeiro no mercado, foi estabelecida a referida hipótese.

Tratamento de dados sensíveis

Os dados sensíveis são aqueles vinculados a uma pessoa natural que dizem respeito à 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.

Estes dados tem o objetivo de evitar a discriminação do titular e, por isso são sujeitos à proteção mais rígida.

Os dados relativos à crianças e ao adolescente deverão ser tratados para o seu melhor interesse, observando a necessidade de consentimento, expressado por, pelo menos, um dos genitores ou responsável legal.

Tratamento de dados especiais

(crianças e adolescentes)

Dados anonimizados e pseudoanonimizados

Segundo a LGPD, dado anonimizado é o dado relativo ao titular que não possa ser identificado. A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta. É importante ressaltar que, ainda que o dado esteja anonimizado, uma vez observada a possibilidade de reversão do processo que obteve a anonimização, este processo deixa de ser assim considerado e passa a ser considerado pseudoanonimização.

Esses processos, de acordo com a legislação em vigor, devem ser utilizados, sempre que possível, por meio da aplicação de meios técnicos razoáveis e disponíveis na ocasião do tratamento dos dados.

Meios de tratamento de dados

O tratamento dos dados pessoais possui cinco fases: coleta, retenção, processamento, compartilhamento e eliminação.

Considerando as fases de vida dos dados pessoais é importante identificar os meios que a empresa utiliza para realizar este tratamento.

Há vários, dentre eles: bases de dados, documentos, equipamentos, locais físicos, pessoas que tem acesso a dados pessoais e sistemas.

Assim, *desde a coleta até a eliminação*, devemos considerar o que segue:

Meios de tratamento de dados

- **Base de dados:** coleções eletrônicas que armazenam grandes quantidades de informação,
- **Documento:** unidade de registro de informações: físico ou eletrônico.
- **Equipamento:** objeto ou conjunto de objetos necessário, para o exercício de uma atividade ou de uma função (computadores, arquivos, pastas, etc...)
- **Local físico:** determinado lugar no qual pode estar de forma definitiva ou temporária uma informação de identificação pessoal.
- **Pessoa:** qualquer indivíduo que executa ou participa de alguma operação realizada com dados pessoais,
- **Sistema:** qualquer aplicação, *software* ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais.

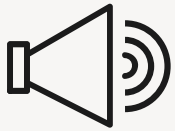
Fases de vida dos dados pessoais

COLETA: Fase da recepção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.).

PROCESSAMENTO: Esta fase significa qualquer operação que envolva classificação, utilização, reprodução, processamento de dados pessoais.

RETENÇÃO: Nela deverá ser avaliada em quais locais serão arquivados ou armazenados os dados pessoais, independente do documento ser em papel ou eletrônico, seja em banco de dados, arquivo de aço.

Na fase de Retenção, os locais nos quais permanecerão os dados deverão ser aqueles que demonstrarem maior segurança e menor chance de algum dado ter a finalidade desviada ou vazada .



COMPARTILHAMENTO: Esta fase envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhado de dados pessoais.

Nela é preciso também mapear os ativos envolvidos na distribuição ou divulgação dos dados pessoais para dentro e para fora da empesa. Quais sistemas são usados para transmitir, exibir ou divulgar dados pessoais? Quais pessoas são destinatárias dessas informações? Quais unidades organizacionais, quais equipamentos são usados para tal?

Fases de vida dos dados pessoais

ELIMINAÇÃO: Operação que visa excluir um dado ou conjunto de dados pessoais armazenados em banco de dados, bem como eliminação de documentos eletrônicos ou em papel em que constam dados pessoais. Esta fase também contempla o descarte dos ativos organizacionais (documentos, equipamentos, etc.). Na fase de eliminação, devem-se avaliar os ativos que armazenam os dados pessoais que possam ser objeto de: solicitação de eliminação de dados a pedido do titular dos dados pessoais; ou descarte nos casos necessários ao negócio da empresa. Os dados pessoais, a serem eliminados, podem estar armazenados em ativos relacionados com bases de dados, documentos físicos, equipamentos ou sistemas, tais ativos também podem ser objeto de descarte.
Assim, o término do Tratamento, nos termos da LGPD, ocorre em quatro hipóteses:

HIPÓTESES

1. Exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade;
2. Fim do período de tratamento;
3. Revogação do consentimento ou a pedido do titular, resguardado o interesse público; e
4. Determinação da autoridade nacional em face de violação do disposto na Lei.

Porém, a lei autoriza a conservação dos dados nos seguintes casos:

A) Cumprimento de obrigação legal ou regulatória pelo controlador;
B) Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados;
C) Transferência a terceiro, desde que respeitados os requisitos de tratamento dispostos em Lei;
D) uso exclusivo pelo controlador, vedado seu acesso por terceiro, e desde que anonimizados.

Segurança no tratamento de dados pessoais

O QUE É INCIDENTE?

Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais.

Por ex: acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração de dados pessoais.

AVALIANDO O RISCO

A avaliação sobre a probabilidade e o impacto do risco, deve ser realizada durante todo o ciclo de vida do dado pessoal, para evitar o incidente de segurança.

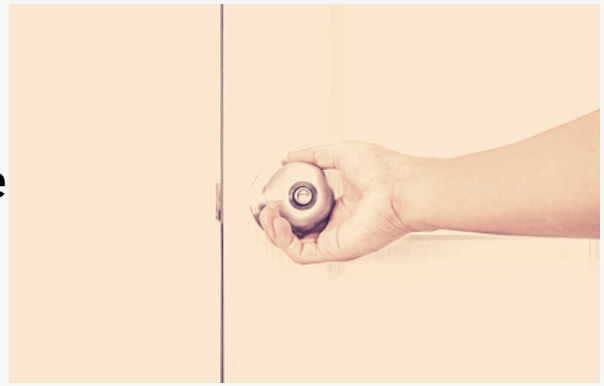
Por ex: Verificar se há finalidade para o tratamento. Se o tratamento está fundamentado em base legal. Qual a segurança implementada.

Dicas de segurança

- Verifique em documentos se os dados coletados do titular são necessários, possuem uma finalidade e uma base legal para o seu tratamento;
- Utilize os recursos computacionais estritamente dentro dos preceitos profissionais;
- Mantenha sua senha de acesso sempre confidencial;
- Não apague ou adultere, intencional ou inadvertidamente, arquivos e informações que não lhe pertençam.

Dicas de segurança

- Proteja equipamentos como: (pen drive, palm, pocket, câmeras ou qualquer tecnologia usb);
- Senhas são pessoais e intransferíveis;
- Mantenha a segurança de seus aparelhos;
- Faça backup;
- Ao utilizar o e-mail como forma de envio de informações e dados, certifique corretamente o destinatário, para evitar vazamentos;
- Não elimine informações e dados importantes, faça o devido armazenamento;
- Faça a segurança de sua sala (feche a porta, insira senha no computador, use chaves nas gavetas);
- Mantenha a mesa limpa, sem papéis que contenham informações importantes;
- Mantenha controle de acessos.



Aplicação da LGPD em Instituições Públicas

Os mecanismos de aplicação da norma são gerais, tanto para as instituições públicas quanto para as privadas, seja em meio físico ou eletrônico.

O termo “fins comerciais”, como fala a Lei, engloba atividades que não sejam eminentemente de uso restrito a um indivíduo. Assim, órgãos públicos, parlamentares, sindicatos e associações civis devem seguir os padrões gerais.

Os poderes executivos e legislativos precisam se vincular a LGPD, bem como à LAI (Lei de Acesso à Informação- 2011), a qual será central para uma efetiva e eficiente aplicação da LGPD. Nessa linha, deve-se ter atenção para a Lei Anticorrupção nos vínculos com a iniciativa privada, em especial nos contratos.

As legislações se contrabalançam entre si. De um lado, o Poder Público tem que garantir a publicidade de seus atos; de outro, ele mesmo deve agir com impessoalidade e ser eficiente, garantindo a dignidade humana para coibir crimes contra a honra e crimes contra a liberdade individual, de opção religiosa, política, sexual etc.

E, sem esquecer dos dados sensíveis, pois, até uma prefeitura em pequena localidade possui dados pessoais dos atendidos (v.g. pela saúde), eles se encontram presentes no cotidiano da Administração Pública para o exercício de atividades.

Igualmente, dados de crianças, tidos como dados especiais (até 12 anos) devem ter autorização da família para serem captados.

Os parlamentos devem aplicar a norma, assim como o parlamentar.

Boas práticas e governança

A LGPD previu que o controlador e o operador no âmbito das competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Boas práticas e governança

É preciso, portanto, criar um programa de privacidade, para compilar as boas práticas de proteção de dados adotadas pela organização. Dentro desse programa é importante destacar os responsáveis por todo o processo de tratamento de dados.

É preciso ainda, realizar o levantamento/o fluxo dos dados pessoais, em que será observado os seguintes requisitos:
(1) como se deu a forma de coleta; (2) quem coleta; (3) quais os dados são coletados; (4) qual a finalidade; (5) onde e como os dados são armazenados; (6) se há transferência internacional; (7) com quem compartilha; (8) como se dá a eliminação dos dados, entre outros questionamentos pertinentes para conhecer a forma de como a empresa trata os dados que manuseia.

Ainda, no mesmo sentido, devem-se adotar medidas hábeis a atender o titular do dado pessoal, através de um canal simples, objetivo, ágil, e acima de tudo, transparente.

Nessa senda, é importante ressaltar a necessidade de um plano de resposta a incidentes, adoção de medidas de segurança; adequação contratual; avaliação de risco; treinamento e conscientização, enfim, todas as medidas necessárias a evitar a violação da privacidade do titular.

Ao avaliar a maturidade da organização diante do levantamento das informações é possível realizar uma estrutura de governança orientada ao modelo da organização.

Definir uma abordagem de governança de privacidade apropriada é complexo e desafiante, mas quando adotada e implementada, assegurará à organização conformidade com as obrigações legais, em linha com os objetivos do negócio que devem estar suportados por todos os níveis da organização.

A adoção de um programa de boas práticas e governança pode implicar em redução de eventual sanção a ser aplicada por violação à LGPD, além de gerar valor para a organização.

Fiscalização e sanções

Em caso de infração a qualquer dispositivo da LGPD, o agente de tratamento de dados, ainda que seja órgão público, estará sujeito a sanções administrativas que poderão ser aplicadas pelo órgão fiscalizador competente. As sanções são aquelas descritas no artigo 51, vejamos:

Fiscalização e sanções

1. Advertência, com indicação de prazo para adoção de medidas corretivas;
2. Multa simples, de até 2% (dois por cento) sobre o faturamento da empresa;
3. Multa diária;
4. Publicização da infração;
5. Bloqueio dos dados pessoais;
6. Eliminação dos dados pessoais;
7. 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;
8. 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;
9. Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A aplicação das sanções ocorrerão após procedimento administrativo que oportunizem a ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados alguns parâmetros, como a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé do infrator; a vantagem auferida ou pretendida pelo infrator; a condição econômica do infrator; a reincidência; o grau do dano; a cooperação do infrator; a adoção de política de boas práticas e governança; a pronta adoção de medidas corretivas; e a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

As sanções administrativas previstas na LGPD não substituem a aplicação de sanções administrativas, civis, ou penas definidas no Código de Defesa do Consumidor e em legislação especifica.

RBA Advogados

(51) 99979.9115

rbaadvogadoseconsultores

@rbaadv

rosangela@rbaadvs.com.br

rbaadv.com.br