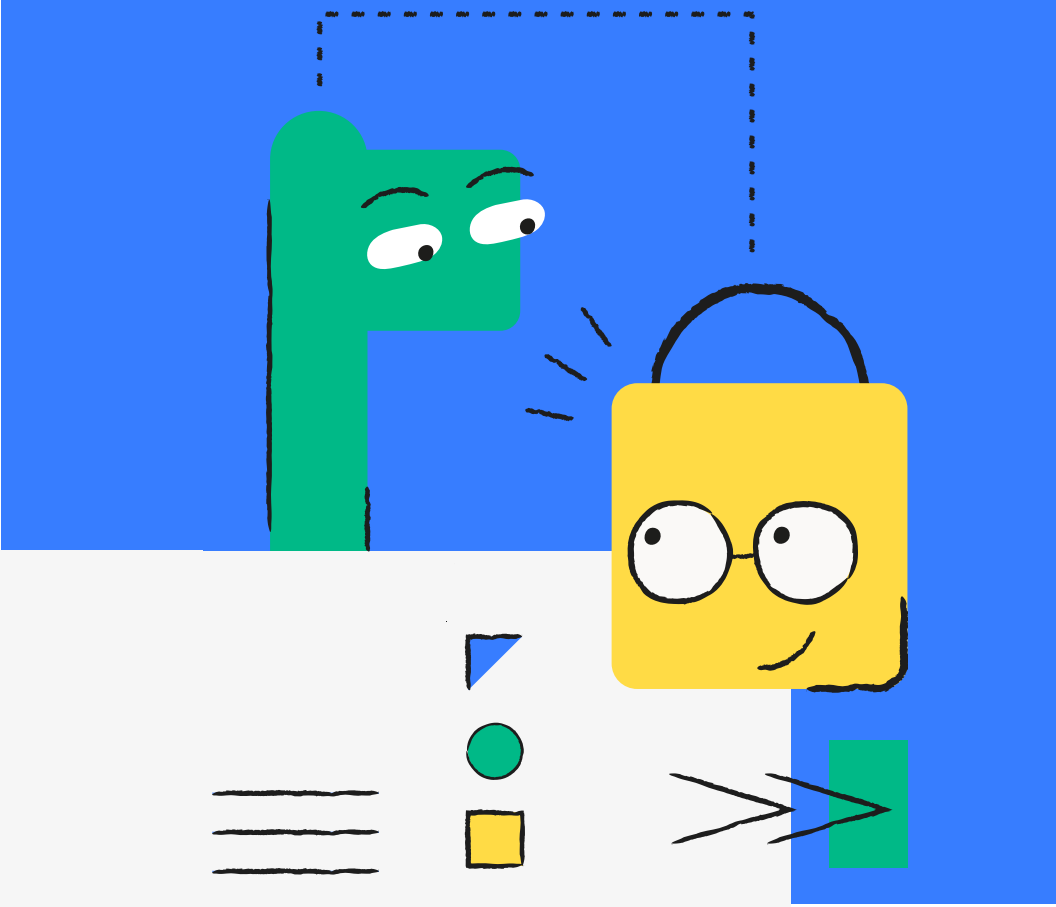
lgpd

lei geral de proteção de dados



wegov

Súmario

1

O que é a lei geral de proteção de dados

1.1 O que é a lei geral de proteção de dados – LGPD

Em virtude dos avanços tecnológicos, o processamento de dados alcançou proporções jamais antes vistas, apresentando, além de benefícios para diversos setores da sociedade, riscos e ameaças até então inimagináveis. No contexto da economia movida a dados, os dados pessoais apresentam-se como o principal insumo para a economia, provocando a atenção de especialistas e autoridades para a necessidade de se garantir a devida proteção dos direitos e liberdades individuais dos cidadãos na Era Digital.

Em 1995, a União Europeia adotou a Diretiva 95/46/CF, relativa à proteção dos cidadãos do bloco europeu no que diz respeito ao tratamento e a circulação de dados pessoais. Em 2016, a diretiva veio a ser substituída pelo Regulamento

Geral de Proteção de Dados (General Data Protection Regulation – GDPR).

O GDPR teve como finalidade primordial harmonizar as leis de proteção de dados e privacidade em todos os Estados membros da União Europeia, garantindo que todas as pessoas que se encontrem em seus territórios tenham a proteção contra o uso indevido de seus dados pessoais e a violação à sua privacidade, estabelecendo, inclusive, sanções em casos de descumprimento.

Embora tenha sido editado pela comunidade europeia, o regulamento europeu possui um alcance de aplicação extraterritorial, ou seja, o GDPR é aplicável a todo o tratamento de dados pessoais de pessoas físicas que se achem na União Europeia, não dependendo, portanto, de sua nacionalidade, cidadania, domicílio ou residência. Isso significa que o âmbito de aplicação do regulamento europeu alcança, inclusive, todas as empresas que possuem filiais na União europeia ou que ofertem bens e servidos dirigidos ao mercado europeu.

Nesse sentido, todos os países que pretendem estabelecer relações comerciais com a União Europeia devem observar os critérios e parâmetros fixados normativa europeia, razão pela qual diversos Estados têm adotado uma legislação de proteção de dados compatível com o GDPR, incorporando princípios e regras do regulamento europeu.

No contexto brasileiro, a Lei Geral de Proteção de Dados Pessoais (LGPD), inspirada na experiência regulatória europeia, foi sancionada em agosto de 2018, dispondo sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2

Principais conceitos trazidos pela LGPD

2.1 Dado pessoal

É toda informação, seja em meio físico ou digital, capaz de identificar direta ou indiretamente uma pessoa natural. o conceito de dado pessoal inclui não somente informações diretamente ligadas a uma pessoa, mas também informações que tenham o potencial de tornar alguém identificável: nome, prenome, RG, CPF, título de eleitor, número de passaporte, endereço, estado civil, gênero, profissão, números de telefone, registros de ligações, protocolos de internet, registros de conexão, registros de acesso a aplicações de internet, contas de e-mail, cookies, hábitos, gostos e interesses, são apenas alguns exemplos de dados pessoais que pautam a atual vida em sociedade.

2.2 Dado pessoal sensível

Qualquer dado pessoal capaz de revelar alguma informação 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.
Em outras palavras, são dados capaz de ensejar um prejuízo ao titular em decorrência de um ato discriminatório.

Como o dado pessoal é um conceito contextual, pode-se estar diante de uma informação que, a princípio, não seja sensível, mas naquele determinado contexto possa revelar um dado sensível de um indivíduo, como uma condição de saúde, um dado biométrico ou uma referência a aspectos da vida sexual.

2.3 Titular dos dados

O titular dos dados é a pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento.

Exemplo: o cliente e/ou colaborador de uma empresa

2.4 Tratamento

Tratamento é 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.

2.5 Agentes de tratamento

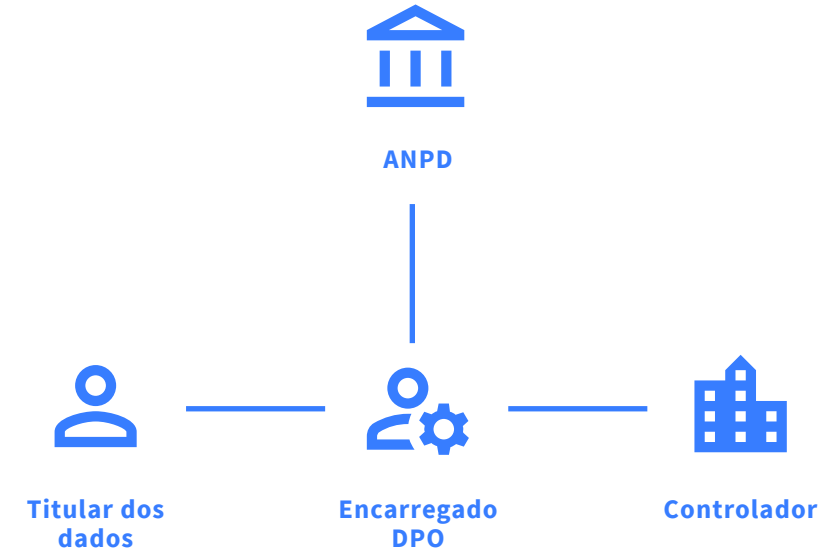
São os agentes de tratamento que realizam o tratamento de dados pessoais. Dependendo da situação ou circunstância, o agente de tratamento será considerado Controlador ou Operador.

Controlador é a Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Art. 5º, VI, da LGPD).

Operador é a Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Art. 5º, VII, da LGPD).

2.6 Encarregado de dados pessoais

Segundo o art. 5º, VIII, da LGPD, o **Encarregado de Dados Pessoais** é o profissional indicado 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).



O DPO possui as seguintes responsabilidades:

- Receber as reclamações e solicitações dos titulares, prestar esclarecimentos e adotar providências.

- Receber os comunicados emitidos pela Autoridade Nacional e adotar providências.

- Orientar todo o quadro de colaboradores da instituição 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.

2.7 Autoridade nacional de proteção de dados

Segundo o art. 5º, XIX, da LGPD, a ANPD é o órgão da administração pública federal, integrante da presidência da República, responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. Além disso, a ANPD poderá aplicar sanções administrativas para os agentes de tratamento que não observarem as normas estabelecidas pela legislação.

Dentre as atribuições da ANPD elencadas pelo art. 55-J da LGPD, pode-se destacar 3 principais objetivos estratégicos:

- Promover o fortalecimento da cultura eficaz para a proteção de dados pessoais.
- Estabelecer ambiente normativo eficaz para a proteção de dados pessoais.
- Aprimorar as condições para o cumprimento das competências legais.

2.8 Princípios, diretrizes e obrigações impostas pela LGPD

Princípio significa “início, começo, o que serve de base a alguma coisa”. Nesse sentido, os princípios norteiam a aplicação da lei, indicando a direção que deve ser seguida pelo intérprete da lei.

O art. 6º, da LGPD, estabelece os princípios que devem nortear todas as atividades de tratamento de dados pessoais.

Boa-fé objetiva: Denota honestidade, boa intenção e estabelece padrão ético de conduta nas relações. Por ser primordial, a boa-fé foi trazida antes de todos os princípios da LGPD, devendo, assim, regrar os agentes em suas condutas ao longo de toda cadeia de tratamento de dados pessoais

Finalidade: Propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Necessidade: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

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.

Qualidade dos dados: Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

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.

Segurança: Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Não discriminação: Proibição de realização do tratamento de dados pessoais para finalidades discriminatórias, ilícitas ou abusivas.

Responsabilização e prestação de contas: Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Além dos princípios, a LGPD impõe uma série de obrigações para os agentes de tratamento de dados pessoais, tais como:

- Observação das bases legais dispostas nos arts. 7º e 11, da LGPD.
- Manutenção do registro de operações de tratamento de dados pessoais, especialmente quando o tratamento for baseado no legítimo interesse.
- Indicação do encarregado pelotratamento de dados pessoais.
- Adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentes ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado.
- Comunicação, pelo controlador, à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

3

Direitos do titular

3.1 Direitos do titular

Um dos pontos mais importantes da LGPD é a garantia dos direitos dos titulares. Em seu art. 18, a LGPD estabelece que o titular dos dados pessoais tem direito a obter do controlador:

- Confirmação da existência de tratamento dos dados (inciso I);
- Acesso aos dados (inciso II);
- Correção dos dados incompletos, inexatos ou desatualizados (inciso III);
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei (inciso IV);

- 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 (inciso V);

- Eliminação dos dados pessoais tratados com consentimento do titular, exceto nas hipóteses previstas no art. 16, da LGPD (inciso VI);

- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado dos dados (inciso VII);

- Informação sobre a possibilidade de não fornecer o consentimento e sobre as consequências da negativa (inciso VIII);

- Revogação do consentimento (inciso IX);

4

Como a instituição deve se organizar internamente pela LGPD

4.1 Como a instituição deve se organizar internamente pela LGPD

Para cada empresa, uma estratégia. É importante ter consciência de que a metodologia a ser adotada para adequação à LGPD está diretamente relacionada com a realidade da própria organização, ou seja, o procedimento deve ser feito “sob medida”.

Para iniciar um projeto de adequação regulatória à LGPD, é necessário, antes de tudo, analisar detalhadamente os processos de rotina da Instituição em relação da captação de dados pessoais, o fluxo e as formas de tratamento dispensadas.

Nesta etapa inicial, deve-se atentar ao porte da organização, os procedimentos de proteção de dados já implementados, a qualificação da equipe, os recursos tecnológicos disponíveis, os níveis de risco e o prazo existente pata a conformidade. Todos esses fatores influenciarão a tomada de decisão em

relação aos procedimentos a serem a dotados para a adequação.

Para operacionalizar toda a gama de obrigações e direitos que a LGPD criou, a instituição deve estruturar uma cadeia de governança em privacidade e dados pessoais.

Comitê de Privacidade >

trata-se do comitê responsável pela tomada de decisão estratégica envolvendo o tema privacidade e proteção de dados pessoais.

Encarregado de dados pessoais >

trata-se da função criada pela LGPD, que servirá como ponto de contato entre a empresa, os títulares de dados e a ANPD

Diretoria e Presidência

5

O papel do agente público

5.1 O papel do agente público

O agente público, como a pessoa responsável pelo exercício da função pública, exerce um papel central para que o projeto de adequação regulatória à LGPD seja aderente nas instituições públicas.

Considerando que os dilemas relacionados à proteção de dados se apresentam no cotidiano da organização, é essencial que o agente público absorva os conceitos trazidos pela LGPD e desempenhe a sua atividade de modo colaborativo, cumprindo as disposições estabelecidas pelos seus supervisores, reforçando uma cultura consistente de privacidade e proteção de dados pessoais.

Lembre-se, toda atuação do agente público deve ser imputada ao órgão que ele representa, ou seja, à pessoa jurídica para a qual trabalha. Por essa razão, o agente público é responsável por garantir que o seu ambiente de trabalho siga as diretrizes impostas pela lei.

6

LGPD e o setor público

6.1 LGPD e o setor público

Aspectos gerais e desafios (LGPD x LAI x ISO)

Na atualidade, um dos grandes desafios do Poder Público é tentar atender às regras de transparência e publicidade exigidas pela chamada Lei de Acesso à Informação – LAI (Lei n. 12.527, de 18 de novembro de 2011) e, ao mesmo tempo, respeitar as necessárias restrições quanto à proteção de dados pessoais, regulamentada pela Lei Geral de Proteção de Dados Pessoais – LGPD (Lei n. 13.709/2018)

Diante disso, é necessário estabelecer breves distinções e semelhanças entre a LAI e a LGPD.

Simplificada	LAI (Lei n. 12.527/2011)	LGPD (Lei n.13.709/2018)
Interesse	Interesse público ou coletivo	Interesse público, quando o tratamento de dados ocorre na esfera pública. Interesse privado, quando o tratamento de dados ocorre na esfera da relação entre particulares.
Objeto de tutela jurídica	Acesso à informação, pessoal ou não.	Proteção de dados pessoais.
Fundamentos contitucionais		Inviolabilidade da intimidade, da vida privada, da honra e da imagem (art. 5º, X, da CF); Autodeterminação informativa (ADI nº 6.387). Proteção de dados pessoais (ADI nº 6.387). Liberdade de expressão e opinião (art. 5º, IV, VIII da CF). Desenvolvimento econômico (art. 170, parágrafo único, da CF)

Segundo as diretrizes da LGPD, o Poder Público, no exercício de suas funções, é considerado um agente de tratamento. Nesse sentido, cabe destacar a importância do tratamento de dados pelo setor público, abrangendo desde o oferecimento de serviços públicos até o planejamento e a aplicação de políticas públicas.

No caso do setor público, o tratamento de dados pessoais obedecer, rigorosamente, às disposições da LGPD e da Lei Federal n. 8.159/199, que dispõe sobre a política nacional de arquivos públicos e privados.

Isso porque, os dados pessoais coletados pelo Poder Público passam a integrar o que se denomina “arquivo público” do órgão ou da entidade.

7

Políticas de proteção de dados para área meio e área fim

7.1 Políticas de proteção de dados para área meio e área fim

No que tange à adequação do Poder Público às disposições da LGPD, deve-se garantir que tanto as atividades-meio (administrativas e diárias de manutenção de seu sistema de atendimento e trabalho) quanto as atividades-fim (assistência ao jurisdicionado, promoção de políticas públicas e da justiça de modo geral).

7.2 Atividades-meio

a) Gestão de recursos (SI e TI)

As áreas de Segurança da Informação e Tecnologia da Informação são chaves importantes de um projeto de adequação. Antes de tudo, é necessário que exista a percepção de que as áreas de TI e SI possuem um potencial estratégico que transborda sua tarefa de garantir o funcionamento da estrutura informática de um órgão público. Pensar nos dados abre margem para que as atividades desses profissionais sejam

utilizadas da melhor forma possível para impactar de forma mais direta o trabalho dos órgãos.
A participação desses profissionais é essencial para implementar formas inteligentes de integração dos sistemas e para a criação de padrões de consolidação de informações, o que evitaria retrabalho e permitiria a concentração de conhecimentos.

Criação de uma coordenadoria responsável pelos processos de informatização e gestão de recursos tecnológicos.

- Determinação de regras e boas práticas para aquisição de recursos da área de tecnologia da informação.
- Determinação de regras e boas práticas para o uso dos recursos TIC.
- Determinação de regras e boas práticas para uso de recursos disponíveis na web.

---

[1] Lei Estadual n. 8.543/2017: "Art. 1° - Entende-se por arquivos públicos as documentações produzidas, recebidas e acumuladas por órgãos públicos da administração direta, autarquias, fundações, empresas públicas pelo Poder Público, bem como entidades privadas encarregadas da gestão de serviços públicos"

- Determinação de parâmetros mínimos de segurança da informação, como o atendimento aos padrões ISO.

- Estabelecimento de protocolos de respostas a incidentes, incluindo medidas preventivas e mitigadoras.

- Estabelecimento de medidas concretas a serem adotadas para garantir o atendimento aos princípios do privacy by design.

Gestão de Pessoas

Planejar a consolidação de um sistema integrado e padronizado também é oportunidade para as equipes que cuidam da gestão de pessoas nos órgãos públicos. Um ambiente organizado permite uma gestão interna mais eficiente ao traçar um quadro com maior fidedignidade sobre o trabalho que tem sido realizado pelos órgãos. Isso serve para, por exemplo, uma melhor alocação de funcionários, distribuição

de tarefas, percepção de sobrecargas etc., e pode ser útil também para a simplificação de algumas tarefas mecânicas como, por exemplo, automatização de férias, controle de ponto e entrada de processos administrativos, o que abre espaço para que esses profissionais tenham mais disponibilidade para cuidar das estratégias de funcionamento eficiente da instituição.

- Automatização de controles como férias e controle de ponto.
- Checagem de sobrecarga de trabalho: percepção de que determinadas unidades, órgãos ou núcleos precisam de mais colaboradores em determinados setores.
- Contratações: necessidade de novas contratações, padrões de admissão e desligamento de estagiários, controle responsável das informações de candidatos em processo seletivo.

8

Plano de ação

8.1 Plano de ação – política institucional em LGPD

Um dos grandes desafios trazidos pela LGPD é a necessidade da criação de uma cultura de privacidade e proteção de dados pessoais nas instituições.

O plano de ação destina-se à implementação de um Programa de Governança de médio e longo prazo, com estabelecimento de medidas elementares à adequação regulatória à LGPD. Diante desse desafio, as diretrizes de governança de proteção de dados e privacidade devem integrar a política institucional da organização.

9

Parte prática

9.1 Política de privacidade e avisos de privacidade

A Política de Privacidade e Avisos de Privacidade buscam informar aos titulares acerca dos dados pessoais coletados, das finalidades empregadas e do modo de tratamento dos dados pessoais.

Trata-se de se buscar a construção de uma relação de confiança e transparência com os titulares, sendo um dos pilares do

Programa de Governança. Por essa razão, de maneira a consagrar o princípio da transparência, informações devem ser claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

9.2 Registro de atividades de tratamento de dados (art. 37, da LGPD)

A construção de um registro de atividades de tratamento de dados pessoais busca atender à obrigação legal de que os agentes de tratamento mantenham documentados todas as informações relevantes sobre as operações de tratamento de dados pessoais.

O Registro de Atividade de Processamento de Dados será construído com base na realização do diagnóstico das atividades de tratamento de dados pessoais, com o mapeamento de todos os processos internos da instituição que, de alguma maneira, lidam com dados pessoais.

9.3 Guia de resposta a incidentes: como lidar com um incidente de vazamento de dados pessoais?

O tratamento de dados pessoais, por si só, é uma atividade de risco, que, em certa medida, pode gerar algum dano ou transtorno ao titular.

Por esse motivo, o art. 48, da LGPD, disciplina rigorosamente as medidas que os agentes de tratamento devem tomar assim que tiverem conhecimento da ocorrência de algum incidente de segurança que envolva dados pessoais.

A partir disso, os agentes de tratamento devem estabelecer um guia de medidas eficazes para solucionar qualquer evento que possa apresentar um risco de dano ao titular. Assim, é essencial que a instituição estabeleça uma Política de Segurança da

Informação e um Plano de Resposta a Incidentes, contendo diretrizes de controle de risco e mitigação de danos decorrentes de incidentes de segurança de dados pessoais.

Segundo art. 48, § 1º, da LGPD, o controlador deverá comunicar, em prazo razoável, à ANPD e ao titular a ocorrência de todo incidente que possa acarretar risco ou dano relevante aos titulares.

Até o presente momento, a recomendação apresentada pela ANPD é que a comunicação seja feita dentro do prazo de 2 dias úteis, contados a partir da ciência do evento adverso, desde que tal evento enseje risco relevante à esfera do titular.

Diante disso, é essencial que os agentes de tratamento disponham de um plano de gestão de incidentes de segurança de dados pessoais, a fim de que as medidas sejam tomadas o mais breve possível.

9.4 Como atender às solicitações dos titulares

Segundo o art. 19, II, da LGPD, os agentes de tratamento deverão responder às solicitações dos titulares no prazo de 15 dias.

Desse modo, embora seja interessante que o agente de tratamento disponha de uma interface destinada à apresentação dos requerimentos dos titulares, o que é, de fato, indispensável, é que o agente de tratamento disponha de capacidade técnica mínima para atender os pedidos, acompanhamento todo o processo. Seguem algumas medidas a serem tomadas

- Adoção de medidas técnicas e organizacionais que permitem o exercício de direitos dos titulares e, caso necessário, implementar ferramentas que permitam o exercício de seus direitos de forma facilitada. Desenvolvimento de formulário de consulta padrão dos titulares e modelos de respostas.

- Definir políticas, padrões e procedimentos que estabeleçam a forma pela qual será operacionalizado o atendimento às requisições de titulares de dados pessoais relacionados à execução de seus direitos (canal de comunicação específico, por exemplo). O fluxo de atendimento das requisições de exercício de direitos por parte dos titulares de dados pessoais deve se desenvolver de forma a atender os requisitos de tempo e forma exigidos pela LGPD.

- Avaliar a possibilidade de inclusão, nos canais da instituição, de uma aba específica para exercício de direitos dos titulares, concedendo a possibilidade de acesso, modificação e revogação de preferências e dados pessoais, diretamente pelo titular dos dados, vez que tal atitude facilita o exercício dos direitos pelo titular, retira o ônus de atendimento às solicitações e mantém a integridade dos dados pessoais tratados.

No que diz respeito ao exercício de direitos pelo titular de dados, deve-se assegurar o oferecimento de mecanismos de participação do titular, em razão do princípio da autodeterminação informativa. Neste ponto, é preciso compreender que a participação do titular é um elemento essencial para o estabelecimento de uma relação de confiança.

Papel, funções e responsabilidades do Encarregado de Dados; (vide item 2.6)

10

Principais medidas de segurança

10.1 Principais medidas de segurança

Em razão do progresso tecnológico, a grande parcela dos dados pessoais é tratada em sistemas informáticos.

Por esse motivo, a segurança da informação é um elemento crucial para estabelecer uma relação de confiança com o titular de dados pessoais. Nesse sentido, o princípio da segurança é um dos alicerces normativos da LGDP, dispondo que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

Assim, é importante que a organização implemente cuidados específicos na gestão e nos sistemas utilizados no cotidiano de suas operações. Seguem abaixo algumas medidas que poderão ser tomadas para elevar a segurança da organização:

Criação uma política de segurança personalizada para as atividades da empresa, contendo métodos seguros de coleta, acesso, compartilhamento e descarte de dados pessoais;

Estabelecimento de controles de acessos para os servidores;

Manutenção dos registros de cada atividade executada;

Treinamento e conscientização da equipe para preservar a segurança da informação;

Bloqueio dos sistemas de saída;

Elaboração dos planos de contingência;

Realização de backups periodicamente.

11

Encerramento

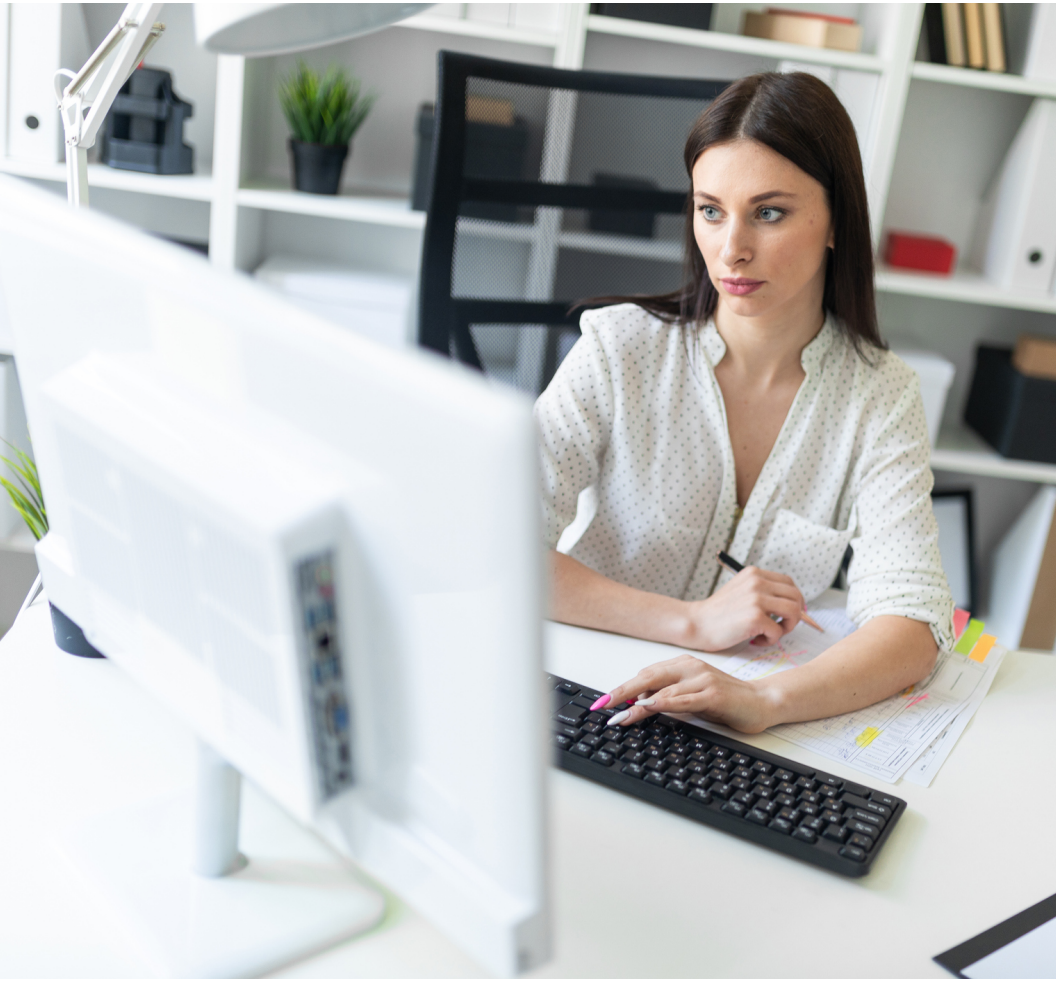
11.1 Encerramento

A adequação à Lei Geral de Proteção de Dados não é uma tarefa fácil, no entanto plenamente possível pelas entidades do sistema de Justiça no Brasil.

A simples implementação de soluções da iniciativa privada é incabível, diante das inúmeras especificidades dos Tribunais brasileiros e sua natureza única de atendimento à população, produção de conhecimento e quantidade de demandas que exigem uma prestação jurisdicional célere e eficiente.

Os Tribunais podem ser líderes de um processo de transformação cultural do sistema de Justiça brasileira. Essa transformação passa pelo reconhecimento de que os dados são das pessoas e que há uma relação de confiança e de obrigações ao realizarmos os tratamentos desses dados. Além disso, há uma questão de responsabilidade e ética pelo tratamento correto desses dados, impedindo utilizações abusivas e indevidas.

A Lei Geral de Proteção de Dados não impede o cenário de inovação e de fluxo dos dados, mas garante que os dados possam ser utilizados de forma legítima, com respeito aos direitos dos titulares e procedimentos para que haja documentação, avaliação de risco e fluxos adequados para a sua utilização conforme finalidades específicas.



SMN ADVOGADOS ASSOCIADOS

Somos um espaço de aprendizado que faz a inovação acontecer no setor público.

wegov.com.br