AFINAL, O QUE É A LGPD?

A LGPD, Lei nº. 13.709/2018, é a Lei Geral de Proteção de Dados Pessoais brasileira. Através dela, são protegidos os dados de pessoas físicas no meio físico ou digital.

Quando foi publicada?

15 de agosto de 2018.

Quando entrou em vigor?

A LGPD entrou em vigou em 18/09/2020.

As penalidades poderão ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD) a partir do dia 01/08/2021.

Quem ela afeta?

Por ser uma lei geral, afeta todos os setores e ramos de atividades que tratam dados de pessoas físicas, tanto no setor privado como no público.

QUAIS SÃO OS FUNDAMENTOS DA LGPD?

- Respeito à privacidade, protegendo os dados das pessoas.
- Autodeterminação informativa para que as pessoas sejam informadas e possam tomar decisões corretas.
- Liberdade de expressão, de informação, de comunicação e de opinião
- Inviolabilidade da intimidade, da honra e da imagem
- Desenvolvimento econômico, tecnológico e inovação.
- Livre iniciativa, livre concorrência e defesa do consumidor, garantindo que os dados pessoais possam continuar sendo tratados e as empresas possam gerir livremente seus negócios, respeitando os direitos dos consumidores, já previstos no Código de Defesa do Consumidor.
- Direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais.

DESMITIFICANDO A LGPD

Conhecer as novas regras, independente do porte da empresa, pode fazer toda a diferença!

Isso porque você pode utilizar dados pessoais nas mais diversas situações, desde a contratação de empregados, por meio do Contrato de Trabalho, até as análises de crédito de clientes para fechar um negócio.

E você sabia que os dados não precisam estar armazenados em um sistema, em um site ou em nuvem para que seja obrigatório o cumprimento das regras sobre proteção de dados pessoais?

Aqueles arquivos físicos ou aquela gaveta onde estão guardados os currículos de candidatos ou fichas impressas preenchidas por clientes também precisarão ser tratados de acordo com a LGPD!

QUANDO A LGPD SERÁ APLICÁVEL?

A LGPD É APLICÁVEL...

- Para dados de pessoas físicas.
- Para dados tratados no Brasil
- Quando o tratamento dos dados tiver como objetivo a oferta ou fornecimento de bens ou serviços a pessoas localizadas no Brasil.

E QUAIS SÃO AS EXCEÇÕES?

A LGPD NÃO É APLICÁVEL...

- Para fins jornalísticos, artísticos ou acadêmicos.
- Para fins relacionados à segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.
- Em casos de tratamento de dados pessoais provenientes de fora do território nacional, desde que não sejam objeto de comunicação ou uso compartilhado com agentes de tratamento brasileiros ou transferência para outro país que não o de origem.

O QUE É DADO PESSOAL?

Dado pessoal é a informação relacionada a pessoa física (natural) que permite que o indivíduo possa ser imediatamente identificado ou identificável.

Confira alguns exemplos:

- Número do CPF
- Dados Cadastrais
- Data Nascimento
- Profissão
- Dados de Geolocalização
- Interesses e Hábitos de Consumo
- IP

E muitos outros!

MAS SERÁ QUE TUDO É DADO PESSOAL?

Não! Existem dados que são anonimizados, ou seja, relativos à pessoa física que não possa ser identificada, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento.

Esses dados não são considerados dado pessoal e, por consequência, não precisam obedecer às regras previstas na LGPD.

O QUE É DADO PESSOAL SENSÍVEL?

Dado pessoal sensível é uma categoria especial de dados pessoais que merecem ser tratados com mais cautela como:

- 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
- Informação genética ou biométrica

Fique atento se você possui esse tipo de dados e avalie se precisa mesmo deles e/ou se tem justificativa legal para tratá-los. Repense se você precisa mesmo saber qual é, por exemplo, a religião de um candidato participante de um processo seletivo, informações referentes à vida sexual do seu colaborador ou a cor da pele do seu cliente.

E QUEM SÃO OS AGENTES DE TRATAMENTO?

A Lei Geral de Proteção de Dados define os agentes de tratamento de dados pessoais como **Controlador** e **Operador**.

CONTROLADOR

Pessoa física ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento dos dados pessoais.

OPERADOR

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

Os papéis de Controlador e Operador não são imutáveis. Em uma situação, sua empresa poderá ser a Controladora e, em outra, a Operadora dos dados pessoais.

QUEM É O ENCARREGADO?

O Encarregado ou DPO (Data Protection Office) é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), que poderá ser um empregado do Controlador ou prestador de serviço. Atualmente, todo Controlador é obrigado a indicar um Encarregado, seja um grande ou pequeno varejista, por exemplo, uma pizzaria ou um consultório médico.

Quais são suas atribuições?

- Receber reclamações e comunicações.
- Prestar esclarecimentos.
- Adotar providências.
- Orientar empregados e contratados.
- Outras atividades relacionadas ao tratamento de dados pessoais do Controlador e do Operador.

Atenção!

A Autoridade Nacional poderá estabelecer normas complementares sobre a definição e as atribuições do Encarregado, conforme a natureza e o porte da empresa ou o volume de operações de tratamento de dados.

O QUE A LGPD CONSIDERA COMO TRATAMENTO DE DADOS PESSOAIS?

Mesmo sem saber, diariamente, você executa diversas atividades de tratamento de dados pessoais, desde a coleta do dado, seu armazenamento, até seu descarte. Veja!

- Coleta
- Produção
- Recepção
- Classificação
- Utilização
- Acesso
- Reprodução
- Transmissão
- Distribuição
- Proceswsamento
- Arquivamento
- Armazenamento
- Eliminação
- Avaliação ou controle da informação
- Modificação
- Comunicação
- Transferência
- Difusão
- Extração

A LGPD TRAZ HIPÓTESES QUE AUTORIZAM O TRATAMENTO DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

BASES LEGAIS

QUANDO PODE OCORRER O TRATAMENTO DOS DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS?

Dados Pessoais

- Consentimento.
- Cumprimento de obrigação legal ou regulatória.
- Execução de políticas públicas pela Administração Pública.
- Realização de estudos por órgãos de pesquisa.
- Exercício regular de direitos e em processo judicial, administrativo e arbital.
- Proteção da vida ou da incolumidade física do título ou de terceiros.
- Tutela da saúde.
- Interesse legítimo do controlador ou terceiros.
- Proteção do Crédito.
- Para execução de contratos e procedimentos preliminares a eles relacionados.

Dados Pessoais Sensíveis

- Consentimento.
- Cumprimento de obrigação legal ou regulatória.
- Execução de políticas públicas pela Administração Pública.
- Realização de estudos por órgãos de pesquisa.
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbital.
- Proteção da vida ou da incolumidade física do título ou de terceiros.
- Tutela da saúde.
- Garantia da prevenção à fraude e à segurança do titular.

A LGPD ADOTOU O CONCEITO DE CRIANÇA E ADOLESCENTE PREVISTO NO ART. 2º DA LEI Nº. 8.069/90 (ESTATUTO DA CRIANÇA E DO ADOLESCENTE):

"Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade."

Fique atento se você trata dados de crianças e adolescentes, pois para esses casos, a LGPD estabeleceu regras específicas:

- O tratamento deverá ser realizado no melhor interesse da criança e do adolescente.

- É necessário o consentimento específico e destacado de um dos pais ou do responsável legal, salvo exceções previstas na lei.

PRINCÍPIOS

A LGPD TRAZ UM ROL TAXATIVO DE PRINCÍPIOS QUE DEVEM SER CUMPRIDOS PELOS AGENTES DE TRATAMENTO DOS DADOS PESSOAIS, SÃO ELES:

Finalidade

> Propósitos legítimos, específicos, explícitos e informados.

Adequação

> Compatibilidade com os dados tratados e as finalidades informadas.

Necessidade

> Limitação ao mínimo de dados necessários para a finalidade informada.

Livre Acesso

> Consulta facilitada e gratuita.

Qualidade

> Exatidão, clareza, relevância e atualização de dados.

PRINCÍPIOS

Transparência

> Informações claras, precisas e facilmente acessíveis.

Segurança

> Medidas técnicas e administrativas aptas a proteger os dados.

Prevenção

> Medidas para prevenir a ocorrência de danos em virtude do tratamento.

Não discriminação

> Impossibilidade de tratamento para fins discriminatórios, abusivos ou ilícitos.

Responsabilidade e Prestação de Contas

> Demonstração de adoção de medidas eficazes para o cumprimento da LGPD.

A LGPD AMPLIOU OS DIREITOS DOS TITULARES EM RELAÇÃO A PROTEÇÃO DE SEUS DADOS. MAS, QUAIS SÃO ESSES DIREITOS?

DIREITO DOS TITULARES

Confirmação de existência de tratamento

> Simplificada e ocorre imediatamente; ou em 15 dias por declaração completa

Acesso aos dados

> Armazenamento em formato que favoreça o acesso

Correção

> Dados inexatos, incompletos ou desatualizados

Anonimização, bloqueio ou eliminação

> Dados excessivos ou tratados ilicitamente.

Portabilidade

> Para outro fornecedor mediante requisição expressa – pendente regulação da ANPD

DIREITO DOS TITULARES

Eliminação dos dados tratados com o consentimento

Informação sobre compartilhamento

Informação sobre a possibilidade de não fornecer consentimento

Revogação do consentimento

Revisão de decisões tomadas com base em tratamento automatizado

TÉRMINO DO TRATAMENTO E ELIMINAÇÃO DOS DADOS PESSOAIS

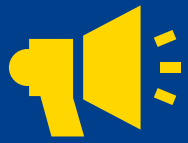
A LGPD PREVÊ A OBRIGATORIEDADE DE ESTABELECER UM CICLO DE VIDA PARA OS DADOS PESSOAIS, QUE DEVE SER OBSERVADO.

NESTE SENTIDO, O TRATAMENTO CHEGARÁ AO FIM E OS DADOS PRECISARÃO SER ELIMINADOS QUANDO:

Atingida a finalidade.

Dados não são mais necessários ou pertinentes à finalidade.

Fim do período de tratamento.



Comunicação do titular, resguardado o interesse público.

Determinação da Autoridade Nacional (ANPD).

SEGURANÇA DA INFORMAÇÃO

Atualmente, é muito importante que toda empresa tenha mecanismos voltados para a segurança da informação.

E a LGPD exige que Controladores e Operadores adotem medidas de segurança, técnicas e administrativas para 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.

O QUE FAZER CASO OCORRA ALGUM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO?

O Controlador deverá comunicar à Autoridade Nacional (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

A comunicação será feita em prazo razoável, ainda a ser definido pela autoridade nacional, e deverá mencionar:

Descrição da natureza dos dados pessoais afetados.

Informações sobre os titulares envolvidos.

Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial.

Riscos relacionados ao incidente.

Motivos da demora, caso a comunicação não tenha sido imediata.

Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Atenção!

Na ocorrência de um incidente, sua empresa precisará estar preparada para seguir todos requisitos previstos na lei.

SANÇÕES ADMINISTRATIVAS

SANÇÕES ADMINISTRATIVAS

Advertência.

Multa de até 2% do faturamento até o limite de R$50.000.000,00

Multa diária.

Publicização da infração.

Bloqueio ou eliminação.

Suspensão parcial, por até 6 meses, do banco de dados envolvido.

Proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados

RESPONSABILIDADES

Operador e Controlador:

- O Controlador ou o Operador que, em razão do exercício da atividade de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, fica obrigado a repará-lo.
- O Operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas do controlador.
- Os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente.

Agentes de tratamento:

Os agentes de tratamento só não serão responsabilizados quando provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído, ou que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados, ou ainda que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

O Decreto nº. 10.474, de 27 de agosto de 2020, estabelece a Estrutura Regimental e Organizacional da ANPD.

Quem compõe a ANPD?

- Conselho Diretor, órgão máximo de direção.
- Conselho Nacional de Proteção de Dados Pessoais e da Privacidade.
- Corregedoria.
- Ouvidoria.
- Órgão de assessoramento jurídico próprio.
- Unidades administrativas e especializadas necessárias à aplicação do disposto na Lei.

Quais são suas principais atribuições?

- Zelar pela proteção dos dados pessoais.
- Editar normas e procedimentos.
- Decidir sobre a interpretação da LGPD, inclusive sobre casos omissos.
- Requisitar informações às empresas que realizam tratamento de dados.
- Implementar mecanismos para o registro de reclamações.
- Fiscalizar e aplicar sanções.

Atenção!

O descumprimento das regras referentes à proteção de dados pessoais será fiscalizado pela ANPD. Apesar das sanções administrativas só poderem ser aplicadas a partir do dia 01/08/20, com a entrada em vigor da lei, você já pode ser fiscalizado pelos órgãos de defesa do consumidor, Ministério Público e ser acionado perante o Poder Judiciário.

GLOSSÁRIO

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.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

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;

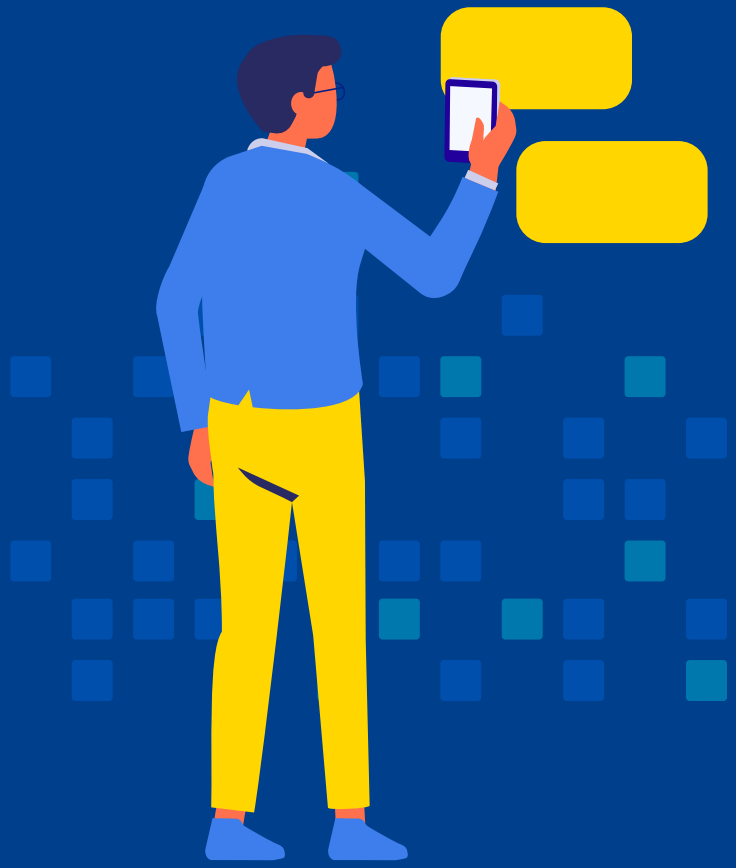
Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses 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.

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

MEDIDAS DE ADEQUAÇÃO À LGPD



Agora que você conhece a LGPD, seus conceitos, as bases legais, os princípios e os direitos dos titulares, já é possível executar seu projeto de adequação.

Para isso, preparamos um material ilustrativo que poderá auxiliá-lo. Confira a seguir!

PARA REALIZAR A ADEQUAÇÃO À LGPD, ALGUMAS MEDIDAS DEVEM SER TOMADAS. CONFIRA!

1 - Definir equipe interna: Ainda que você contrate uma consultoria, precisará de, no mínimo, uma pessoa do seu quadro de colaboradores para acompanhar, validar entregas e cuidar do seu projeto de adequação. O ideal é ter uma equipe multidisciplinar, pois as questões que envolvem dados exigem habilidades distintas.

2 - Promover a conscientização

É muito importante que não apenas o time do projeto saiba sobre a LGPD e a proteção de dados, mas toda a organização. Para isso, recomenda-se que sejam desenvolvidos treinamentos, divulgação de materiais, curiosidades, etc.

3 - Realizar o mapeamento

Todos os processos de todas as áreas que envolvam dados pessoais devem ser mapeados a fim de identificar o tipo de dado, uso, finalidade, acessos e compartilhamentos em cada processo. Assim, poderão ser descobertas falhas, lacunas e os ajustes necessários para a adequação à LGPD.

Algumas empresas optam também por fazer uma espécie de varredura automatizada (Data Discovery) em todos os seus sistemas e máquinas, em razão do grande volume de dados. Verifique se este é o seu caso!

COMO REALIZAR O MAPEAMENTO DOS DADOS PARA DEFINIR AS BASES LEGAIS?

Durante ou após o mapeamento dos dados, será possível identificar as bases legais que justificam a realização do tratamento.

- O mapeamento poderá ser realizado através de entrevistas presenciais ou não.
- Caso você não possua uma ferramenta que lhe auxilie no mapeamento poderá realizá-lo por meio de planilhas em Excel. Neste caso, o importante é que cada processo seja descrito em uma linha separada, que as áreas sejam identificadas em planilhas diferentes e que, a medida que ocorram alterações nos processos, as planilhas sejam atualizadas.
- O importante é que a área responda as perguntas da forma mais clara possível.

Veja algumas informações que podem ajudar você a conhecer processos e identificar a base legal, nos termos da LGPD:

- Nome da área
- Nome e descrição do processo
- Quais são os dados pessoais coletados neste processo? São coletados dados de crianças e adolescentes?
- São coletados dados sensíveis neste processo?
- Quem são os titulares dos dados envolvidos no processo?
- Qual é a origem dos dados?
- Qual é o tratamento realizado neste processo?
- Qual é a finalidade do tratamento dos dados?

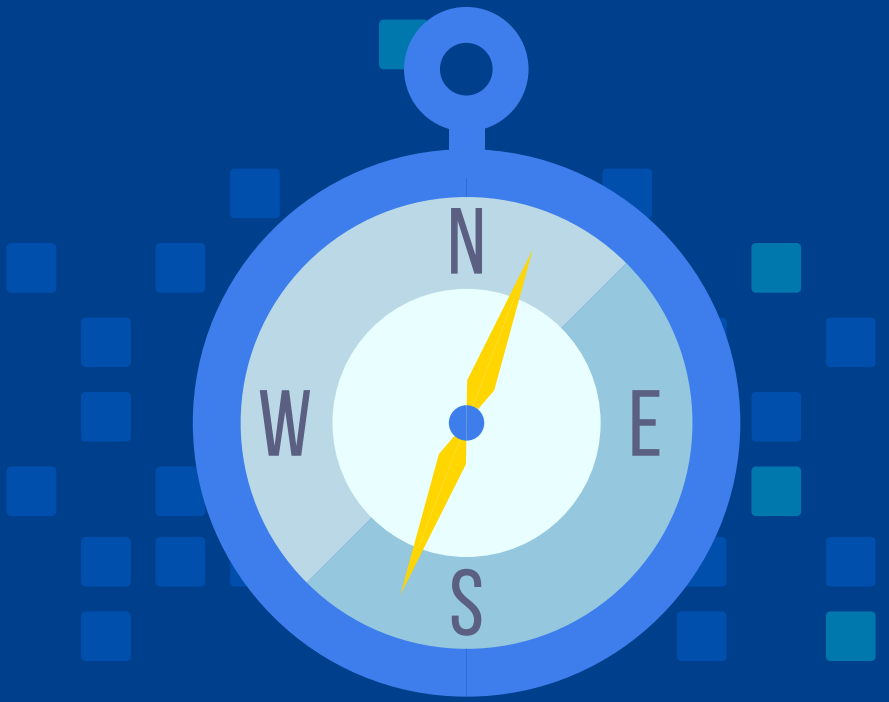
O QUE FAZER DEPOIS DO MAPEAMENTO?

4 - Gap Analysis

Após realizar o mapeamento, você precisará compreender as respostas informadas e identificar falhas/lacunas que precisem de ajustes. Nesta etapa, você poderá notar que precisa atualizar contratos com fornecedores, criar políticas de privacidade para sites, colaboradores, terceiros/fornecedores, revisar acessos de colaboradores aos sistemas, etc.

5 - Plano de Ação

Neste momento, trace seu plano de ação, ou seja, quais ações precisará realizar para estar em conformidade com a lei, quanto tempo precisará para cumprir cada tarefa e quem serão os responsáveis.



6 - Atendimento aos Titulares

Com a vigência da LGPD os titulares dos dados podem exercer vários direitos relacionados aos seus dados pessoais e a qualquer tempo.

Você precisará disponibilizar um meio de atendimento, que poderá ser físico ou digital. Esse atendimento deverá ser gratuito e de forma facilitada.

Fique atento para confirmar a identidade do titular. Confirme que quem está requisitando o atendimento é o próprio titular ou seu representante legal. O acesso indevido poderá ser uma infração à lei.

7 - Governança

Depois de executar seu plano de ação, será necessário ter governança dos dados. Nos termos da LGPD, o responsável pela governança é o Encarregado (DPO). Ele deve ser o canal de comunicação entre a empresa, a ANPD e os titulares, bem como fazer a gestão de todos os processos que envolvam dados pessoais.

Encarregado

Atualmente, todos os Controladores são obrigados a indicar um Encarregado, que pode ser um colaborador interno ou terceirizado; o importante é que ele tenha conhecimentos sólidos sobre privacidade e proteção de dados, e possa atuar com autonomia em suas atribuições.

O Encarregado poderá ser indicado logo no início do projeto ou no momento que for mais oportuno, até a entrada em vigor da lei.

A LGPD prevê que a ANPD poderá regulamentar este ponto fazendo algumas isenções.

Comprometimento
Plano de resposta a incidentes
Organização
Atualização constante
Mecanismos de supervisão e mitigação de risco
Ações importantes que devem constar no **Programa efetivo de governança em privacidade**
Procedimentos
Ações educativas
Normas da segurança
Avaliação sistemática de impacto e riscos
Obrigações e responsabilidades
Padrões técnicos
Transparência e confiança

FAQ LGPD

Dados pessoais sensíveis são apenas aqueles informados pela LGPD ou existem outros que também podem ser considerados sensíveis?

A LGPD trouxe um rol taxativo não cabendo uma interpretação extensiva, assim são considerados dados sensíveis apenas os dados 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.

O que é dado pseudonimizado?

É o dado pessoal que, em razão de um tratamento, perde a possibilidade de associação, direta ou indireta, ao titular, senão pelo uso de informação adicional mantida separadamente pelo Controlador em ambiente controlado e seguro.

Podemos exemplificar o dado pseudonomizado com a seguinte situação:

Em uma planilha, o titular é identificado por um código alfanumérico, sendo possível apenas para a empresa que criou a planilha identificar quem seria aquele titular.

Podemos considerar que os dados constantes na planilha estão pseudonimizados, uma vez que a empresa que criou a planilha tem condições de identificar o titular, mas todas as outras empresas que tiverem acesso à planilha não têm a mesma condição.

Não se pode confundir o dado pseudonimizado com o dado anonimizado, uma vez que este último perde a capacidade de associação ao titular e, portanto, deixa de ser dado pessoal.

É preciso cumprir todos os princípios previstos na LGPD ou apenas um deles já é suficiente?

Além da obrigatoriedade do tratamento dos dados se basear na boa-fé, os agentes de tratamento são obrigados a cumprir todos os princípios previstos na LGPD. O descumprimento de apenas um deles já é causa de infração à lei.

O que é o princípio do Privacy By Design?

É um princípio que busca garantir que os cuidados com a privacidade e proteção dos dados pessoais devam estar presentes desde a criação do produto ou serviço, antes

mesmo de ser disponibilizado para o titular. Por exemplo, quando uma plataforma é oferecida ao mercado deverá já prever todas as aplicações necessárias para garantir que a privacidade e os dados dos usuários estejam protegidos e sejam respeitados.

As empresas também precisarão adotar a privacidade como padrão, conforme determina o princípio do Privacy By Default.

Em relação às bases legais que justificam o tratamento dos dados pessoais, existe alguma que seja mais importante que outra?

Não existe hierarquia entre as bases legais. O importante é que o tratamento seja justificado em, pelo menos, uma delas e que seja escolhida a mais apropriada para justificar o tratamento do dado pessoal.

Dentre as 10 bases legais previstas para o tratamento de dados pessoais, o consentimento pode ser considerado o mais simples?

Pelo contrário, a utilização do consentimento como base legal é algo que, em um primeiro momento, parece ser o caminho mais simples, contudo a lei trouxe vários requisitos que devem ser cumpridos e que tornam esta base legal bem complexa de ser utilizada. Portanto, avalie bem se você precisa mesmo do consentimento do titular para realizar o tratamento e, se precisar, não deixe de cumprir todos os requisitos da lei.

Quais são os requisitos que uma empresa que elege o consentimento para tratar dados pessoais deve cumprir?

A LGPD trouxe uma série de requisitos que devem ser cumpridos quando o tratamento se justificar pelo consentimento.

Nesta situação, o consentimento deverá:

a) ser livre, inequívoco e informado, ou seja, o titular não pode ser obrigado a consentir, não pode ter dúvidas quanto ao conteúdo e deve expressar a sua vontade.

b) ser específico, sendo consideradas nulas as autorizações genéricas por parte do titular. Não serão mais aceitas autorizações genéricas, do tipo: coletamos os seus dados para melhorar a sua experiência ou para melhorar os nossos produtos e serviços.

c) ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

As empresas deverão garantir que o titular possa revogar seu consentimento a qualquer momento mediante manifestação expressa, por procedimento gratuito e facilitado. Assim, será necessário que seja realizada uma gestão do consentimento, uma vez que revogado e eliminado, o dado não poderá mais ser usado pela empresa para a finalidade que foi consentida pelo titular.

O consentimento poderá ser considerado nulo, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo, ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. Caberá às empresas provarem que o consentimento foi obtido em conformidade com a lei, sendo vedado o tratamento de dados pessoais mediante vício de consentimento.

É importante ressaltar que mesmo com a revogação e/ou eliminação do consentimento, é provável que o dado do titular ainda precise ser tratado pela empresa, seja para cumprir uma obrigação legal ou regulatória, seja para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Já em relação aos dados sensíveis, o consentimento ganha um papel de destaque, pois a lei prevê que o tratamento somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável previstas na lei (Art.11, II, a, b, c, d, e, f,g da Lei nº. 13.709/2018).

Em relação ao legítimo interesse, a LGPD traz algumas situações que justificam o tratamento por esta base legal. Estas situações são exemplificativas ou taxativas?

A LGPD traz um rol exemplificativo de situações que possam ser justificadas como Legítimo Interesse.

De acordo com a lei, o controlador somente poderá justificar o tratamento de dados pessoais fundamentado no legítimo interesse para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

a) apoio e promoção de atividades do controlador.

b) 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 as liberdades fundamentais, nos termos desta Lei.

O legítimo interesse é uma base legal considerada subjetiva, portanto deve ser utilizada com cautela, e somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.O controlador deverá adotar medidas para garantir a transparência do tratamento de dados.

Esta base legal será usualmente eleita para justificar o tratamento nas ações de marketing. Portanto, se você utilizar o legítimo interesse, precisará estar apto para atender as expectativas dos titulares quando estes apresentarem o opt-out, demonstrando que a sua expectativa é não fazer parte do mailing de clientes.

As empresas poderão justificar o tratamento de dados pessoais sensíveis pelo seu legítimo interesse?

Não. A base legal do legítimo interesse não é válida para justificar o tratamento de dados sensíveis.

Se a sua empresa trata dados pessoais sensíveis, precisará eleger outra base legal para justificar o tratamento desses dados.

O que é o relatório de impacto? Quando as empresas precisarão elaborá-lo?

O relatório de impacto à proteção de dados pessoais é um documento elaborado pelo controlador. Nele, deve conter a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como quais serão as medidas, salvaguardas e mecanismos de mitigação de risco que a empresa irá adotar.

A Autoridade Nacional de Proteção de Dados (ANPD) poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Deste modo, a recomendação é que as empresas já elaborem proativamente os relatórios de impacto para não serem surpreendidas na eventualidade de serem solicitadas pela ANPD.

Em relação aos direitos dos titulares, quais são os prazos que devem ser cumpridos pelas empresas? E como estas informações e os dados devem ser disponibilizadas para o titular?

No atual momento, temos apenas dois prazos definidos pela LGPD e estes estão relacionados ao direito de confirmação e acesso aos dados pessoais por parte dos titulares. São eles:

a) **imediatamente** e em formato simplificado, de modo que facilite a compreensão do titular.

b) **em 15 dias**, contados da data do requerimento do titular, por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento.

Para todos os demais direitos que podem ser exercidos pelos titulares dos dados, a lei não estabeleceu prazos, mas a recomendação é que sejam analisados no menor tempo possível.

As informações e os dados poderão ser fornecidos a critério do titular:

a) por meio eletrônico, seguro e idôneo para esse fim; ou

b) de forma impressa.

As empresas sempre precisarão atender aos pedidos dos titulares?

Não. Os direitos dos titulares não são absolutos. Caberá à empresa avaliar se o pedido apresentado tem fundamento, com base na lei, para ser atendido. Contudo, sempre precisarão apresentar uma resposta ao titular, ainda que seja para informá-lo que não trata os seus dados e, sempre que possível, indicar quem o faz ou as razões de fato ou de direito que impedem a adoção imediata da providência.

É direito do titular peticionar contra a empresa que está tratando seus dados para a Autoridade Nacional de Proteção de Dados (ANPD)?

Sim, o titular dos dados pessoais tem o direito de peticionar em relação a seus dados contra a empresa que está tratando perante a ANPD.

Os dados tornados manifestamente públicos pelo titular podem ser tratados pelas empresas? Precisam do consentimento dos titulares?

A Lei dispensa o consentimento para os dados tornados manifestamente públicos pelo titular, e as empresas poderão tratá-los.

Exemplos corriqueiros de dados tornados manifestamente públicos pelos titulares se referem aos perfis abertos em redes sociais.

No entanto, não é porque o dado foi tornado manifestamente público pelo titular ou é de uma fonte pública que não mereça a proteção da LGPD, pois ele ainda é considerado dado pessoal.

A empresa é obrigada a inserir em seu site, por exemplo, as informações de contato do Encarregado?

De acordo com a LGPD, a identidade e as informações de contato do Encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

As regras da LGPD conflitam ou invalidam as do Cadastro Positivo?

Não. A LGPD (Lei nº. 13.709/2018) é uma lei geral que afeta todos os ramos e atividades da economia que tratam dados pessoais e busca proteger apenas dados de pessoas físicas.

Já a Lei do Cadastro Positivo (Lei nº. 12.414/2011) é uma lei específica e que se limita a estabelecer regras referentes aos dados relacionados ao histórico de pagamento, tanto de pessoas físicas quanto de pessoas jurídicas.

Em razão da LGPD, o SPC Brasil estará impedido de tratar os dados das pessoas físicas? Precisará, por exemplo, do consentimento delas para viabilizar uma consulta para análise de crédito ou processar um registro de inadimplência?

Não. O SPC Brasil não estará impedido de tratar os dados das pessoas físicas e, para essas finalidades, não precisará do consentimento, uma vez que a LGPD em seu art.7º, VII estabeleceu a bases legais de "Proteção ao Crédito", "Legítimo Interesse", entre outras bases que dispensam o consentimento do titular para realização do tratamento dos dados pessoais.

O SPC Brasil disponibiliza algum contato ou canal para que o titular possa exercer os direitos previstos na LGPD?

Sim! O SPC Brasil mantém um canal aberto de comunicação, onde os titulares podem exercer os direitos previstos na LGPD, através da página LGPD, no Portal do Consumidor do SPC Brasil. Cabe ressaltar, que os direitos dos titulares não são absolutos e caberá ao SPC Brasil avaliar se o pedido apresentado tem fundamento, com base na lei, para ser atendido.

O SPC Brasil utiliza dados pessoais para alguma decisão automatizada?

Decisão automatizada é o procedimento de classificação, atribuição de nota, aprovação ou rejeição atribuído pelo tratamento de informações pessoais. O SPC Brasil utiliza dados pessoais para a configuração automatizada do Score.

Nosso Score é composto com outras informações além do seu CPF, tais como: informações cadastrais, informações do cadastro positivo (adimplência), informações de consulta e informações de débito (inclusão de débitos por terceiros em nossas bases). Com base em nossa análise matemática, nós determinamos o perfil de consumo de cada um e a pontuação do Score.

Esperamos que esse material tenha ajudado você a entender e se preparar para a LGPD.

Compliance
SPC Brasil

Responsáveis pelo conteúdo:

Encarregado (DPO)

Compliance

Marketing SPC Brasil