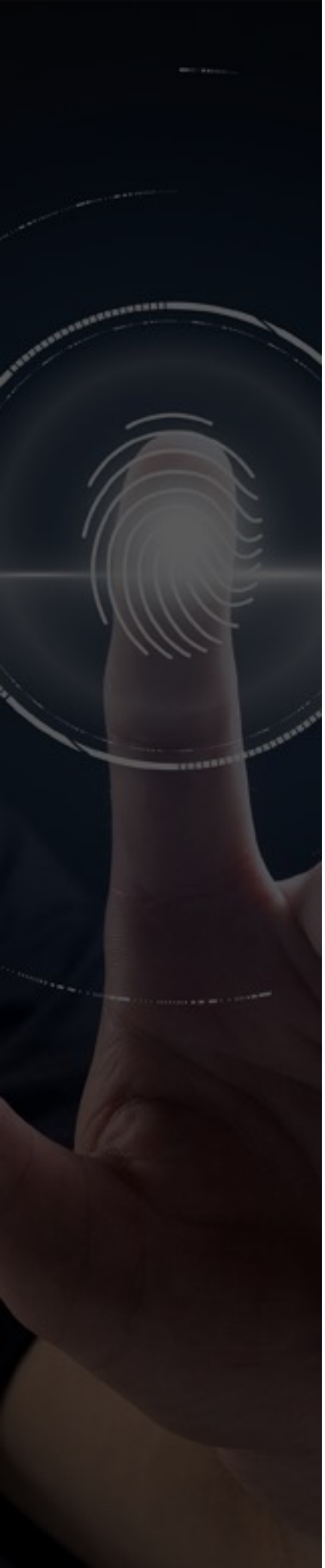
LGPD – Lei geral de proteção de dados

Nesse guia simples e prático, vamos te ajudar a entender o que é a lei, seus princípios fundamentais, e sua aplicabilidade no dia a dia de sua empresa.

25 ANOS



SUMÁRIO

ENTENDENDO A LGPD

A preocupação global com a privacidade e segurança dos dados pessoais se intensificou com o aumento da utilização da internet e das tecnologias digitais. Todas as empresas tratam dados que trazem retornos significativos para o negócio. Assim, os dados pessoais dos consumidores se tornam essenciais e necessários para essa cadeia de produção.

ENTÃO, O QUE É A LGPD?

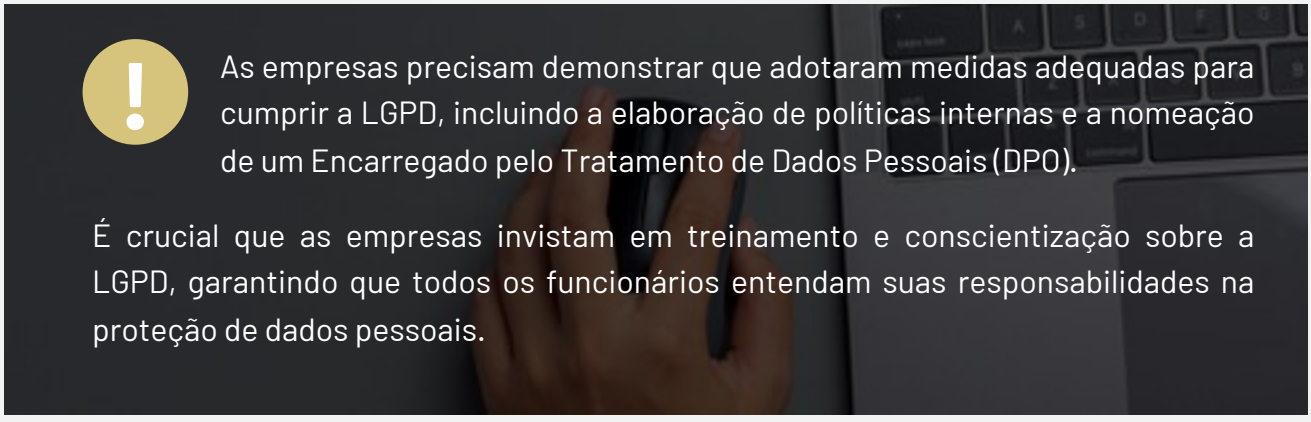
A lei foi criada para garantir a privacidade e proteção de dados pessoais. A **LGPD** visa promover a transparência na relação entre pessoas físicas e jurídicas.

ENTENDENDO A

LGPD

ANDP

Órgão do governo brasileiro criado para garantir que as informações pessoais dos cidadãos sejam protegidas e usadas de forma correta pelas empresas e outras organizações. Ela também orienta essas entidades sobre como cumprir a LGPD e impõe penalidades quando necessário.



As empresas precisam demonstrar que adotaram medidas adequadas para cumprir a LGPD, incluindo a elaboração de políticas internas e a nomeação de um Encarregado pelo Tratamento de Dados Pessoais (DPO).

É crucial que as empresas invistam em treinamento e conscientização sobre a LGPD, garantindo que todos os funcionários entendam suas responsabilidades na proteção de dados pessoais.

CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

É um órgão consultivo da ANPD, composto por membros da sociedade civil e representantes do poder público.

- Propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
- Elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- Sugerir ações a serem realizadas pela ANPD;
- Elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade, e;
- Disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

ENTENDENDO A

LGPD

TITULARES DE DADOS

O titular é a pessoa física a quem se referem os dados pessoais. É o dono da informação que somente a ele diz respeito. Enfim, o titular de dados pessoais somos eu e você!

DADOS PESSOAIS

Informação que representa todo e qualquer dado que possa tornar uma pessoa identificável, seja ela diretamente relacionada ao seu titular (como um nome ou número de documento) indiretamente relacionada, mas com potencial de identificá-lo (a) (como endereço, idade, informações sobre hábitos de compra etc).

- **Nome, sobrenome, data de nascimento, CPF, RG, CNH, carteira de trabalho, passaporte, título de eleitor, matrícula, servidor/colaborador;**
- **Endereço residencial, comercial ou eletrônico;**
- **E-mail corporativo;**
- **Número de telefone;**
- **Placa de automóvel;**
- **Cookie/Log (Endereço de IP + Hora de acesso);**

DADOS SENSÍVEIS

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.

- Convicção Religiosa ou organização de caráter religioso
- Origem Racial ou Étnica
- Opinião política, filiação a sindicato, organização de caráter filosófico ou político
- Dado Genético
- Dado referente à vida sexual
- Dado referente à saúde
- Dado Biométrico

ENTENDENDO A LGPD

AGENTES DE TRATAMENTO DE DADOS PESSOAIS

CONTROLADOR:

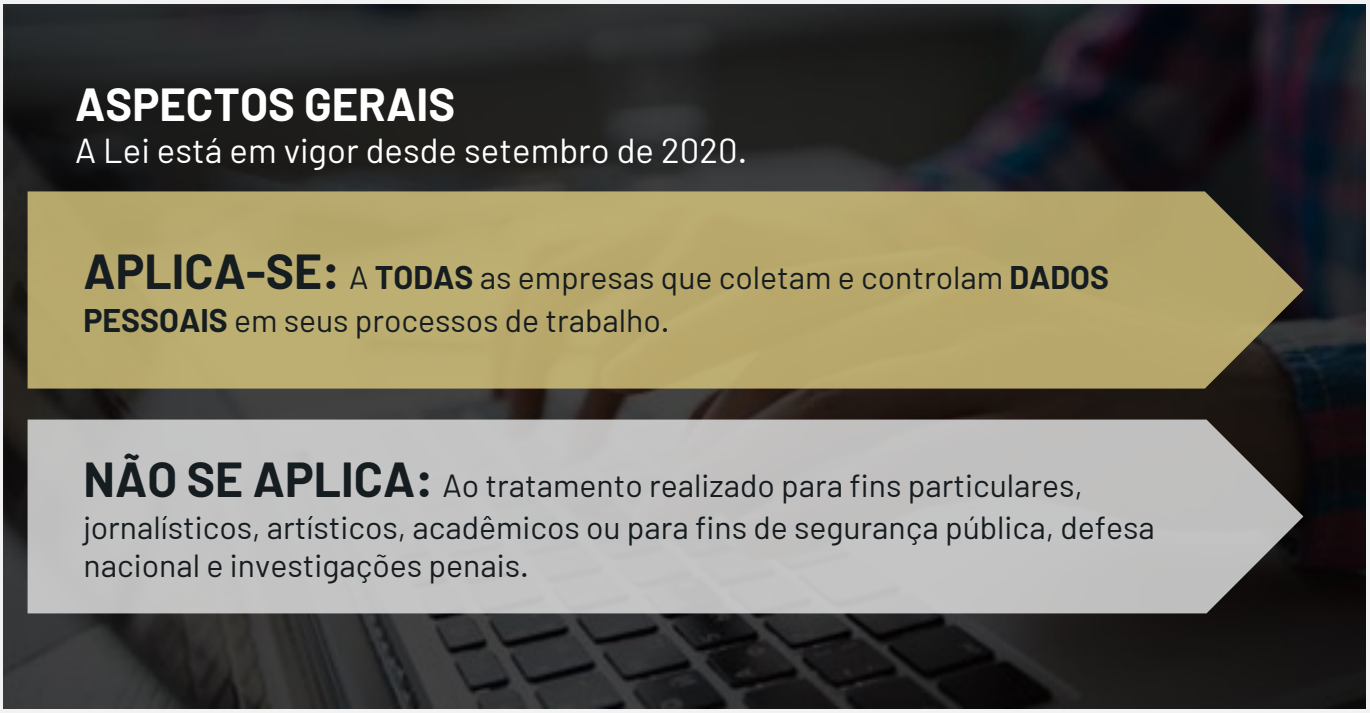
pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

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, os titulares dos dados e a autoridade nacional de proteção de dados;



ASPECTOS GERAIS

A Lei está em vigor desde setembro de 2020.

APLICA-SE: A **TODAS** as empresas que coletam e controlam **DADOS PESSOAIS** em seus processos de trabalho.

NÃO SE APLICA: Ao tratamento realizado para fins particulares, jornalísticos, artísticos, acadêmicos ou para fins de segurança pública, defesa nacional e investigações penais.

PRINCÍPIOS DA

LGPD

PRINCÍPIOS QUE DEVEM REGER O TRATAMENTO DE DADOS PESSOAIS - ART.6

PRINCÍPIO DA FINALIDADE

A realização do tratamento deve acontecer com intenções legítimas, claras, explícitas e comunicadas ao indivíduo, sem a possibilidade de realizar tratamentos subsequentes que não estejam alinhados com essas finalidades.

PRINCÍPIO DA ADEQUAÇÃO

A adequação do tratamento deve acontecer de acordo com os propósitos comunicados ao titular, em consonância com o contexto do procedimento;

PRINCÍPIO DO LIVRE ACESSO

Garantia oferecida aos titulares com acesso irrestrito a informações, de maneira simplificada e sem custos, sobre como e por quanto tempo seus dados pessoais serão processados, abrangendo a totalidade de suas informações pessoais.

PRINCÍPIO DA NECESSIDADE

O tratamento deve restringir-se à realização de suas finalidades, envolvendo apenas os dados relevantes, em quantidade proporcional e sem excessos em relação aos propósitos do tratamento de dados.

PRINCÍPIO DA QUALIDADE DOS DADOS

É a garantia dada aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

PRINCÍPIOS
DA LGPD

PRINCÍPIO DA TRANSPARÊNCIA
É a garantia fornecida aos titulares de que estes receberão informações transparentes, precisas e de fácil acesso acerca da condução do tratamento de dados, bem como dos responsáveis pelo referido processo, respeitando os segredos comerciais e industriais.

PRINCÍPIO DA PREVENÇÃO
Implementação de ações com o objetivo de evitar a manifestação de prejuízos decorrentes do tratamento de informações pessoais.

PRINCÍPIO DA NÃO DISCRIMINAÇÃO
É a garantia de que o tratamento dos dados não será realizado para fins discriminatórios, ilícitos ou abusivos.

PRINCÍPIO DA SEGURANÇA
É o emprego de medidas técnicas e administrativas eficazes para salvaguardar as informações pessoais contra acessos não autorizados, bem como prevenir incidentes acidentais ou ilegais como destruição, perda, alteração, comunicação ou divulgação.

PRINCÍPIO DA BOA-FÉ
Todos os documentos, estratégias de organização, o planejamento para a governança da privacidade devem necessariamente fundamentar-se no princípio da boa-fé.

DIREITOS DOS

TÍTULARES

DIREITO À INFORMAÇÃO

A Lei Geral de Proteção de Dados (LGPD) enfatiza, em diversas instâncias, a importância da transparência. Portanto, é um direito do titular da informação saber com precisão quais entidades, sejam públicas ou privadas, estão compartilhando seus dados. Essas entidades devem ser explicitamente identificadas, evitando referências genéricas.

ACESSO AOS DADOS

Além de verificar se a instituição está cuidando adequadamente de seus dados pessoais, o titular tem o direito de requisitar o acesso a essas informações. Em outras palavras, é viável obter uma cópia dos dados pessoais arquivados pela organização.

Assim como no processo de confirmação do tratamento, a resposta ao pedido de acesso pode ser fornecida de maneira imediata e simplificada, ou por meio de uma declaração completa, dentro do prazo máximo de 15 dias a contar da data da solicitação.

DIREITOS DOS

TÍTULARES

CORREÇÃO DOS DADOS

Um direito adicional conferido ao titular dos dados é a possibilidade de requerer à entidade a retificação de informações pessoais que estejam incompletas, imprecisas ou desatualizadas. Isso engloba situações como a atualização de endereço, número de telefone ou estado civil.

PORTABILIDADE DOS DADOS A OUTRO FORNECEDOR DE SERVIÇO OU PRODUTO

A LGPD estipula que o titular dos dados tem o direito de requisitar a portabilidade de suas informações, ou seja, a transferência de seus dados pessoais para outro provedor de serviço ou produto.

Para efetuar tal solicitação, é necessário apresentar um pedido específico, conforme as diretrizes a serem estabelecidas pela ANPD (Autoridade Nacional de Proteção de Dados), que ainda não está em funcionamento.

Além disso, é importante observar que a portabilidade não abrange dados que tenham sido previamente anonimizados pelo responsável pelo tratamento, os quais, aliás, não estão contemplados no âmbito da LGPD.

ANONIMIZAÇÃO DOS SEUS DADOS

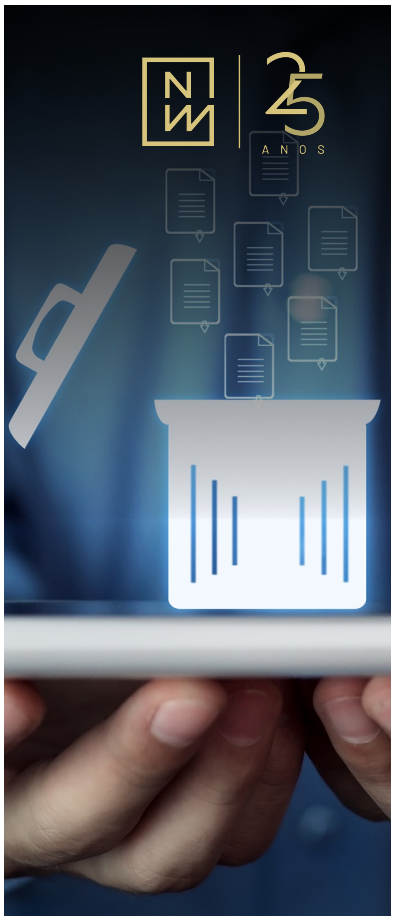
O detentor dos dados também possui o direito de requerer a anonimização, um procedimento que torna um dado impossível de ser associado a um indivíduo, bloqueio ou exclusão de dados quando estes se revelarem desnecessários, excessivos ou processados em desacordo com a legislação.

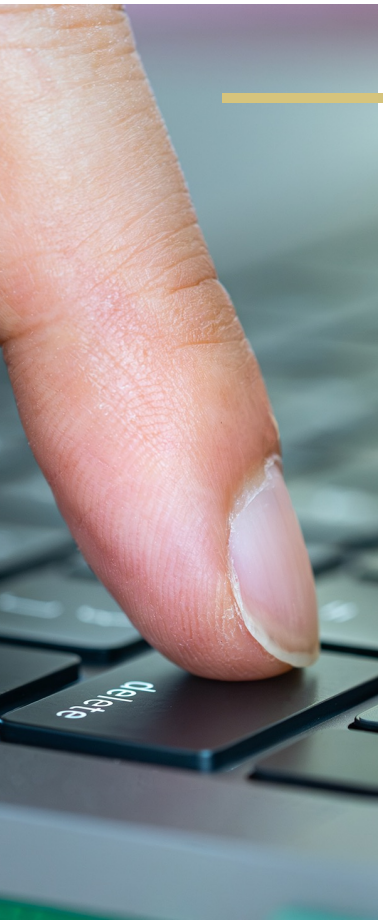
Isso inclui situações em que a organização manipula dados que não são indispensáveis para atingir a finalidade do tratamento ou quando o tratamento não se adequa a nenhuma das bases legais estipuladas pela lei.

ELIMINAÇÃO DOS DADOS TRATADOS

Caso o titular a quem os dados se referem inicialmente tenha concordado com o tratamento, mas posteriormente altere sua decisão e não deseje mais que a entidade manipule suas informações pessoais, ela tem o direito de requisitar a exclusão desses dados.

No entanto, existem circunstâncias em que essa prerrogativa não pode ser aplicada, como nos casos em que a organização necessita manter os dados para atender a obrigações legais ou regulatórias.





REVOGAÇÃO DO CONSENTIMENTO

O consentimento concedido para o processamento de dados pessoais é passível de revogação, constituindo um direito do titular dos dados, que pode formalizar tal solicitação para retirar o consentimento previamente concedido.

A fim de efetivamente eliminar os dados já processados até o momento, é necessário apresentar uma requisição específica.

Tanto o controlador quanto o operador que, no curso da realização de atividades de tratamento de dados pessoais, ocasionarem prejuízos patrimoniais, morais, individuais ou coletivos a terceiros, em desacordo com as disposições da legislação de proteção de dados pessoais, têm a obrigação de realizar a devida reparação.

RESPONSABILIDADES DAS

EMPRESAS

O QUE AS EMPRESAS NÃO PODEM FAZER?

- Utilizar dados pessoais para finalidades diferentes das que foram informadas ao titular no momento da coleta;
- Compartilhar dados pessoais com terceiros sem autorização expressa do titular ou sem base legal específica para fazê-lo;
- Armazenar dados pessoais por tempo superior ao necessário para as finalidades para as quais foram coletadas;
- Utilizar dados pessoais para a prática de discriminação ilícita ou abusiva;
- Coletar dados pessoais sem consentimento explícito do titular, a pessoa a quem os dados se referem, ou sem uma base legal específica para fazê-lo.

RESPONSABILIDADE DAS

EMPRESAS

SOLIDÁRIA

O operador é solidariamente responsável pelos prejuízos resultantes do tratamento, caso não cumpra as obrigações estabelecidas pela legislação de proteção de dados ou não siga as instruções legítimas do controlador.

Os controladores que participaram diretamente do tratamento, resultando em danos ao titular dos dados, também respondem solidariamente.

Independentemente de quem tenha sido o responsável direto pelo vazamento, ambas as partes podem ser responsabilizadas pela compensação dos danos, preservando o direito de reembolso para aquele que reparar o dano ao titular. Isso ocorrerá em relação aos demais responsáveis, proporcionalmente à sua participação no evento causador dos danos.

Todos os membros da cadeia de fornecimento devem responder solidariamente perante o consumidor

RESPONSABILIDADE DAS EMPRESAS

O QUE ACONTECE SE A EMPRESA NÃO CUMPRIR A LEI ?

As empresas que não cumprirem a LGPD estão sujeitas a penalidades que podem incluir multas, advertências, e até mesmo a suspensão do processamento de dados

Advertência - Com a adoção de medidas corretivas.

Multa - De até 2% do faturamento, com limite de até R$ 50 milhões.

Comunicação da infração - Comunicação pública da infração após a devida apuração e confirmação de sua ocorrência.

Bloqueio - Ou a eliminação dos dados pessoais relacionados à irregularidade até a sua regularização.

Suspensão parcial do funcionamento - Do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador.

Suspensão do exercício - da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período.

Proibição - Parcial ou total da atividade de tratamento de dados.

RESPONSABILIDADE DAS EMPRESAS

PENALIDADES

As empresas que não cumprirem a LGPD estão sujeitas a penalidades, que podem incluir multas, advertências, e até mesmo a suspensão do processamento de dados

DESCREBIDILIDADE COM O CLIENTE

Uma organização que negligencia o cumprimento da legislação pode prejudicar sua imagem no mercado e enfrentar conflitos com os clientes. Isso ocorre devido à crescente exigência do consumidor final, que busca informações não apenas sobre produtos e serviços, mas também sobre as práticas internas da empresa. A reputação da empresa pode ser gravemente afetada, gerando desconfiança por parte dos clientes e investidores. Isso pode resultar em perdas financeiras significativas e dificuldades na reconstrução da confiança do público.

INSEGURANÇA JURÍDICA

A insegurança jurídica resultante do vazamento pode prejudicar a competitividade da empresa no mercado financeiro. Clientes em potencial podem escolher instituições mais confiáveis, e investidores podem hesitar em apoiar uma empresa com histórico de falhas na segurança de dados.

CONSENTIMENTO E LEGITÍMIDADE

CONSENTIMENTO

O consentimento é definido no art. 5°, XII, da LGPD como **"manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".** A lei também estabelece outras "condições" para o consentimento, com disposições específicas sobre:

- Manutenção de registros para demonstrar consentimento;
- Nulidade em caso de fornecimento de informações de conteúdo enganoso, abusivo ou pouco transparente;
- Clareza das solicitações de consentimento;
- Direito de revogar o consentimento facilmente e a qualquer momento;
- Consentimento dado livremente se um contrato estiver condicionado a consentimento (vedação do tratamento mediante vício de consentimento).

Basear o processamento de dados pessoais no consentimento em conformidade com a LGPD significa dar aos indivíduos uma escolha genuína e controle contínuo sobre como a organização usa seus dados, bem como significa garantir transparência e responsabilidade.
Uma vez coletado o consentimento, este deverá ser registrado e arquivado.

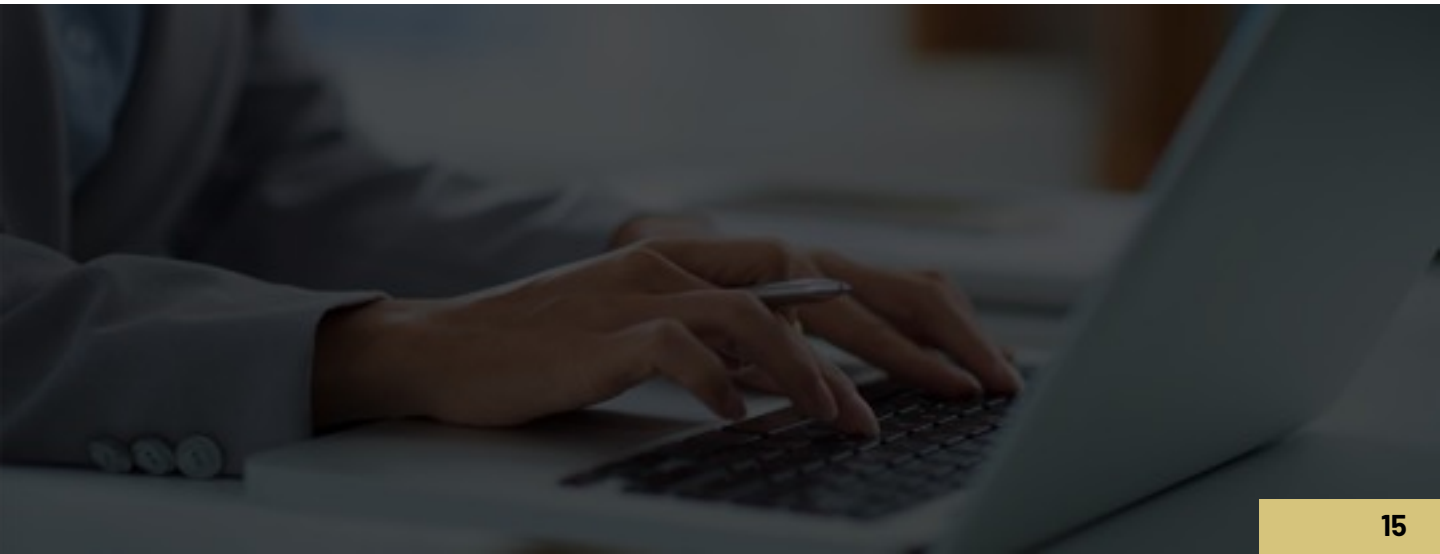
CONSENTIMENTO E
LEGITIMIDADE

O consentimento específico e destacado é uma forma de legitimar o processamento de dados pessoais sensíveis, mas não a única. Os artigos 7 e 11 enumeram outras condições alternativas para o processamento de dados, inclusive de categorias sensíveis, devendo-se ponderar qual a mais adequada ao processamento em questão.

Se a organização deseja processar dados sensíveis, pode obter do indivíduo o "consentimento específico e destacado". No entanto, isso não significa que esta base legal seja a melhor ou a mais adequada, devendo sempre considerar se alguma das outras condições se ajusta melhor à situação específica.

ATENÇÃO

O consentimento não deve ser empregado como a base legal para qualquer tipo de tratamento de dados pessoais, sendo necessário que, caso a caso, exista uma reflexão sobre todas as demais bases legais do artigo 7º antes de se optar pelo consentimento.



CONSENTIMENTO E LEGITIMIDADE

AVALIAÇÃO DO CONSENTIMENTO

a) A organização ainda poderia continuar processando os dados sob uma base legal diferente caso o consentimento fosse revogado?

Buscar o consentimento do indivíduo nesses casos é enganoso e inerentemente injusto, pois apresenta ao indivíduo uma falsa escolha e apenas a ilusão de controle. A base legal mais apropriada deve ser indicada desde o início.

b) A organização pede "consentimento" como uma pré-condição para permitir o acesso aos serviços.

Se a organização exigir que alguém concorde com o tratamento como condição do serviço, é improvável que o consentimento seja a base legal mais apropriada. Em algumas circunstâncias, não será sequer considerado um consentimento válido. Se o processamento é necessário para a execução do serviço, a base legal mais apropriada provavelmente será aquela “para a execução de um contrato" (artigo 7°, V). Provavelmente, só será necessário contar com o consentimento se for obrigado a fazê-lo por meio de outra cláusula, como no caso de marketing eletrônico. O consentimento não é apenas impróprio como uma base legal, mas considerado inválido, pois não é dado livremente.

AVALIAÇÃO DO CONSENTIMENTO

c) A organização está em uma posição de poder sobre o indivíduo

O consentimento geralmente não será apropriado se houver um claro desequilíbrio de poder entre a organização e o indivíduo. Isso ocorre porque dependem de seus serviços ou temem consequências adversas, podendo levar à percepção de que não têm escolha a não ser concordar – e, nestes casos, considera-se que o consentimento não foi dado livremente. Este é particularmente um problema para empregadores e as autoridades públicas.

Se a organização está processando dados de funcionários, ou está em qualquer outra posição de poder sobre um indivíduo, deve buscar outra base para o processamento.

No entanto, os empregadores não estão proibidos de usar o consentimento como base legal. Mesmo estando em uma posição de poder, pode haver situações em que ainda é possível demonstrar que o consentimento foi dado livremente.

No entanto, é necessário examinar cuidadosamente as circunstâncias específicas e estar confiante de que se pode demonstrar a existência da liberdade de escolha entre dar ou recusar o consentimento. É fundamental tomar medidas para garantir que o indivíduo não sinta qualquer pressão para consentir, dissipando possíveis preocupações sobre as consequências da recusa do consentimento.

CONSENTIMENTO E LEGITIMIDADE

REQUISITOS DE VALIDADE

O consentimento deve ser informado. Isso significa que deve abranger as seguintes informações:

- A identidade do responsável pelo tratamento;
- Os objetivos do tratamento;
- As atividades de tratamento;
- O direito de revogar o consentimento a qualquer momento.

Deve ser explicado claramente com o que os indivíduos estão consentindo de uma forma que possam compreender facilmente. A solicitação de consentimento deve ser relevante, concisa, separada de outros termos e condições e em linguagem simples.

Se o pedido de consentimento for vago, abrangente ou difícil de compreender, será inválido. Em particular, a linguagem que pode confundir - por exemplo, o uso de negativas duplas ou linguagem inconsistente - invalidará o consentimento.

O consentimento dado livremente também será mais difícil de obter no contexto de uma relação em que há um desequilíbrio de poder -especialmente para autoridades públicas e empregadores.

CONSENTIMENTO E LEGITIMIDADE

REQUISITOS DE VALIDADE

Os consentimentos devem ser mantidos sob revisão e atualizados se os objetivos ou atividades evoluírem além do que foi especificado originalmente.

Mesmo que a nova finalidade seja considerada "compatível" com a finalidade original, isso não substitui a necessidade de consentimento para ser específico. Se estava contando com o consentimento, será necessário obter um novo consentimento específico ou então identificar uma nova base legal para o novo propósito.

No caso de dados sensíveis, o consentimento deverá ser dado de forma “específica e destacada”. Todo consentimento deve envolver uma indicação específica, informada e inequívoca dos desejos do indivíduo, afirmado em uma declaração clara (seja oral ou escrita).

O consentimento pode ser obtido oralmente, desde que seja mantido um registro do script.

A LGPD não define um limite de tempo específico para consentimento. O consentimento provavelmente se degradará com o tempo, mas a duração dependerá do contexto, considerando o escopo do consentimento original e as expectativas do indivíduo.

Se as operações ou objetivos do tratamento forem alterados, os consentimentos originais podem não ser mais específicos ou informados o suficiente.

Se isso acontecer, a organização precisará buscar um novo consentimento ou identificar outra base legal.

ELABORANDO PEDIDO DE CONSENTIMENTO

As solicitações de consentimento precisam ser concisas, fáceis de entender e separadas de quaisquer outras informações (como termos e condições gerais).

A ORGANIZAÇÃO DEVE:

- ✓ Manter sua solicitação de consentimento separada de seus termos e condições gerais e direcionar claramente a atenção das pessoas a ela;
- ✓ Usar uma linguagem clara e direta;
- ✓ Adotar um estilo simples que o público-alvo considere fácil de entender – isso é particularmente importante se há um pedido de consentimento dirigido a menores de idade; nesse caso, poderá ser solicitada a autorização dos pais (também devem ser consideradas questões de verificação de idade e autorização dos pais);
- ✓ Evitar jargões técnicos ou jurídicos e terminologia confusa;
- ✓ Utilizar linguagem e métodos consistentes em várias opções de consentimento;
- ✓ Manter as solicitações de consentimento concisas e específicas, evitando redações vagas ou abrangentes.

INFORMAÇÕES QUE O PEDIDO DE CONSENTIMENTO DEVE CONTER

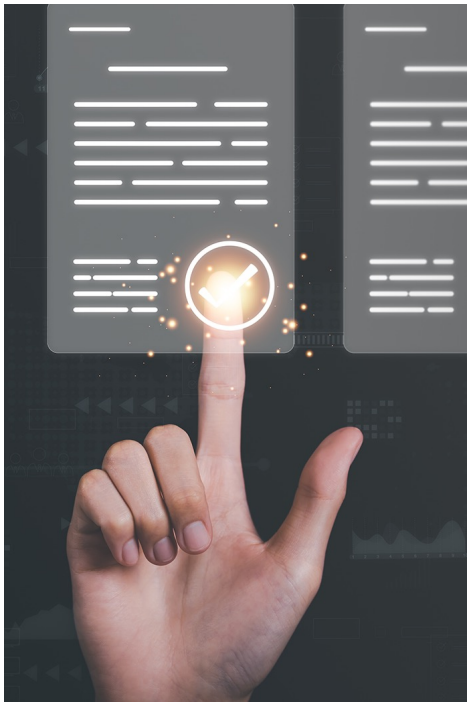
O consentimento deve ser específico e informado. Devem ser incluídos, no mínimo:

A ORGANIZAÇÃO DEVE:

- ✓ Nome da organização e os nomes de quaisquer outros controladores que contarão com o consentimento (o consentimento para categorias de controladores e terceiros não será específico o suficiente);• Usar uma linguagem clara e direta;
- ✓ Por que a organização deseja os dados (os objetivos do processamento);
- ✓ O que a organização fará com os dados (as atividades de processamento);
- ✓ Que as pessoas podem retirar seu consentimento a qualquer momento. É uma boa prática dizer-lhes como fazer isso.

Se for necessário incluir muitas informações, a organização deverá se certificar de que ainda sejam visíveis e fáceis de ler.

A organização deve considerar se há outra base legal para qualquer um dos processos, para que possa concentrar a solicitação de consentimento. Em utilizando outra base, ainda precisará fornecer informações de privacidade claras e abrangentes, mas, conforme observado acima, isso é diferente de uma solicitação de consentimento e pode ser objeto de uma abordagem em camadas.



MÉTODOS PARA OBTENÇÃO DO CONSENTIMENTO

As pessoas não devem ser forçadas a concordar numa base do "tudo ou nada" – elas podem querer consentir com algumas coisas, mas não com outras

A ORGANIZAÇÃO DEVE:

- ✓ Assinar uma declaração de consentimento em um formulário de papel;
- ✓ Marcar uma caixa de opt-in em papel ou eletronicamente;
- ✓ Clicar em um botão de aceitação ou link online; selecionar opções "Sim/Não" (apresentadas com a mesma ênfase);
- ✓ Escolher configurações técnicas ou configurações de painel de preferências (dashboard);
- ✓ Responder a um e-mail solicitando consentimento;
- ✓ Responder "Sim" a um pedido de consentimento verbal claro;
- ✓ Fornece informações opcionais voluntárias para uma finalidade específica - por exemplo, preencher campos opcionais em um formulário (combinado com avisos just-in-time) ou colocar um cartão de visita em uma caixa.

Se for necessário consentimento explícito, o opt-in deve envolver uma declaração expressa confirmando o consentimento

O silêncio, a inatividade, caixas pré-marcadas, caixas de opt-out, configurações padrão ou uma aceitação geral de seus termos e condições não são consideradas opções válidas para obtenção do consentimento.

REGISTRO DO CONSENTIMENTO

Conforme a LGPD, a organização deverá fornecer Registro de Consentimento por **escrito** ou por outro meio que **demonstre a manifestação de vontade do titular.**

A organização deve ter uma **trilha de auditoria eficaz** que permita verificar como e quando o consentimento foi dado, para que possa fornecer evidências em caso de contestação. Esta evidência deverá ser mantida enquanto o tratamento com base no consentimento estiver ocorrendo, a fim de demonstrar sua

- **Quem consentiu:** o nome do indivíduo ou outro identificador (por exemplo, nome de usuário online, ID da sessão).
- **Quando o consentimento foi obtido:** uma cópia de um documento datado ou registros online que incluem um carimbo de data/hora; ou, para consentimento verbal, um protocolo contendo a hora e data da conversa.
- **O que foi informado na época da obtenção do consentimento:** uma cópia original do documento ou formulário de captura de dados contendo a declaração de consentimento em uso naquele momento, junto com qualquer política de privacidade separada ou outras informações de privacidade, incluindo números de versão e datas correspondentes à data em que o consentimento foi dado. Se o consentimento foi dado oralmente, os registros devem incluir uma cópia do script usado naquele momento.
- **Como o consentimento foi obtido:** para consentimento por escrito, uma cópia do documento relevante ou formulário de captura de dados. Se o consentimento foi fornecido online, os registros devem incluir os dados enviados, bem como um carimbo de data/hora para vinculá-los à versão relevante do formulário de captura de dados. Se o consentimento foi dado oralmente, deve-se manter o protocolo fornecido no momento da conversa – não precisa ser um registro completo da conversa.
- Se o consentimento foi revogado e, em caso afirmativo, quando.

GERENCIANDO O CONSENTIMENTO

As obrigações da organização não terminam quando está obtém consentimento.

É uma boa prática fornecer ferramentas de gerenciamento de preferências, como **painéis de privacidade** (dashboards), para permitir que as pessoas acessem e atualizem facilmente suas configurações de consentimento.

Se a organização não conta com um painel de privacidade, é necessário fornecer outras maneiras fáceis para que as pessoas possam retirar o consentimento a qualquer momento que desejarem.

A organização deve manter seus consentimentos sob constante monitoramento e revisão. Pode ser necessário atualizá-los se as condições mudarem.

A organização também deve considerar se deseja atualizar automaticamente o consentimento em intervalos apropriados. A frequência com que é apropriado fazer isso dependerá do contexto específico, incluindo as expectativas das pessoas, se há um contato regular e como os pedidos de consentimento repetidos prejudicariam o indivíduo. Em caso de dúvida, recomenda-se a renovação do consentimento a cada dois anos, mas é possível oferecer justificativas que prevejam um período mais longo ou se é necessária uma atualização mais regular para garantir bons níveis de confiança e envolvimento.

REVOGANDO O CONSENTIMENTO

A LGPD garante aos titulares o direito específico de revogar o consentimento. A organização precisa se certificar de que implementou procedimentos adequados para garantia desse direito.

Como o direito de revogação é "a qualquer momento", não é suficiente fornecer um opt-out apenas por resposta. O indivíduo deve ser capaz de cancelar a qualquer momento que desejar, por sua própria iniciativa.

Também deve ser tão fácil retirar o consentimento como foi para dá-lo. Isso significa que o processo de retirada do consentimento deve ser um processo de uma etapa, facilmente acessível. Se possível, os indivíduos devem poder retirar seu consentimento usando o mesmo método de quando o deram.

É uma boa prática divulgar as ferramentas de gerenciamento de preferências online e outras formas de exclusão, como números de telefone de atendimento ao cliente. Deve-se ter em mente que nem todos se sentem confiantes com a tecnologia ou têm fácil acesso à internet. Se alguém originalmente deu consentimento em papel ou pessoalmente, pode não ser suficiente oferecer apenas um opt-out online.

Também é uma boa prática fornece mecanismos de desativação a qualquer momento, como painéis de privacidade, e desativação por meio de resposta a cada contato. Isso pode incluir um link de cancelamento de inscrição em um e-mail, ou um número de telefone, endereço ou link de cancelamento impresso em uma carta.

Devido à natureza das operações dos Controladores, pode ser necessário processar dados pessoais em conjunto com funcionários, departamentos, órgãos e instituições de outros países. Isso inclui operadoras de serviços terceirizados contratadas fora da jurisdição doméstica, bem como o compartilhamento de dados com instituições estrangeiras por meio de convênios e parcerias estabelecidas e até mesmo a contratação de uma nuvem no exterior.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

A LGPD restringe as transferências de dados pessoais para países ou organizações situadas fora do território brasileiro. As restrições aplicam-se a todos os casos em que ocorre a transferência de dados pessoais e que permite o tratamento por agentes internacionais, não importando a frequência ou a quantidade de dados pessoais a ser transferida. O objetivo de tais restrições é garantir ao titular de dados, que possui dados tratados no âmbito da LGPD, a mesma proteção e zelo que lhes são garantidos pela legislação brasileira.

PERMISSÃO CONFORME LGPD

Os países ou organismos internacionais devem oferecer um nível adequado de proteção de dados pessoais conforme estabelecido na LGPD.

O nível de proteção do país estrangeiro será avaliado pela ANPD

Cabe ao Controlador assegurar a segurança dos dados, bem como a proteção dos direitos e garantias dos titulares das informações.

O Controlador deve fornecer e comprovar garantias de conformidade com os princípios, os direitos do titular e o regime de proteção de dados estabelecido pela LGPD.

A TRANSFERÊNCIA SERÁ AUTORIZADA PELA AUTORIDADE NACIONAL.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

PERMISSÃO CONFORME LGPD

A transferência é indispensável para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, conforme estipulado pelos instrumentos do direito internacional.

A transferência é imprescindível para salvaguardar a vida ou a integridade física do titular ou de terceiros.

A transferência acarretará no compromisso estabelecido em um acordo de cooperação internacional.

A transferência pode ser efetuada por meio de um acordo bilateral entre os Ministérios de países distintos.

Com prévia informação sobre a natureza internacional da operação e uma clara distinção entre esta e outras finalidades.

Se o titular tiver expressamente concedido seu consentimento, destacando de maneira específica a transferência

A transferência se faz necessária para a execução de política pública ou no cumprimento de atribuição legal do serviço público.

É indispensável para atender às situações previamente estipuladas nos incisos II, V e VI do art 7° da LGPD.

- Cumprimento de obrigação legal ou regulatória pelo controlador.;
- Execução de Contrato ou procedimentos preliminares;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

PERMISSÃO CONFORME LGPD

Desta maneira, a lei brasileira, prevê os seguintes mecanismos de transferência que permitem o compartilhamento internacional de dados:

I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

a) cláusulas contratuais específicas para determinada transferência;
b) cláusulas-padrão contratuais;
c) normas corporativas globais;
d) selos, certificados e códigos de conduta regularmente emitidos;

III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros;
V - quando a autoridade nacional autorizar a transferência;
VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente está de outras finalidades; ou
IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei."

TRANSFERÊNCIA INTERNACIONAL DE DADOS

COM NÍVEL DE PROTEÇÃO DIFERENTE DO BRASIL

A LGPD estabelece uma gama de garantias e mecanismos de proteção para os direitos dos titulares de dados pessoais. Portanto, se o país ou a entidade para os quais os dados serão transferidos não apresentarem um alinhamento adequado com essas salvaguardas, os direitos e as liberdades fundamentais dos titulares estarão em perigo.

O nível de proteção de dados do País estrangeiro que irá receber a transferência será avaliado pela ANPD, com fundamentação nos critérios a seguir:

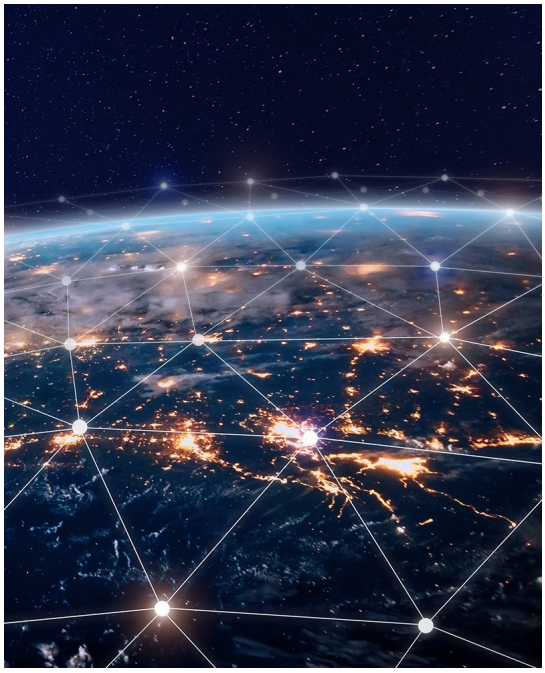
- As disposições normativas gerais e setoriais presentes na legislação vigente no país de destino ou no organismo internacional;
- A natureza dos dados em questão;
- A conformidade com os princípios fundamentais de proteção de dados pessoais e os direitos dos titulares conforme estabelecidos pela LGPD;
- A implementação de medidas de segurança estipuladas em regulamentações pertinentes;
- A existência de salvaguardas judiciais e institucionais que assegurem o respeito aos direitos de proteção de dados pessoais;
- Outras circunstâncias específicas relacionadas à transferência.

MEDIDAS DE GARANTIA APROPRIADAS

Dentre as hipóteses dispostas pela lei que dependem de prévia análise e autorização pela ANPD, as chamadas **medidas de garantia apropriadas,** encontram-se as cláusulas contratuais padrão, cláusulas contratuais específicas para determinada transferência, normas corporativas globais e selos, certificados e códigos de conduta.

Cláusulas contratuais padrão são um conjunto rígido de termos e condições contratuais pré-aprovados pela ANPD que podem ser empregados em contratos em que ocorra a transferência internacional de dados pessoais, condições pelas quais o remetente e o destinatário dos dados pessoais transfronteiriços se submetem a obrigações contratuais específicas no que tange à proteção dos dados pessoais. Uma vez aprovado pela ANPD, o conjunto de cláusulas contratuais padrão poderá ser incluído em contratos entre diferentes empresas e legitimará o fluxo internacional dos dados pessoais entre as partes sem a necessidade de avaliação pela Autoridade competente.

As cláusulas contratuais específicas, que não devem ser confundidas com as cláusulas contratuais padrão, podem ser elaboradas pelas partes e devem ser submetidas à avaliação e aprovação individual da Autoridade Nacional, tendo efeito vinculante única e exclusivamente em relação a transferências de dados pessoais especificadas entre as partes envolvidas. Após sua aprovação específica, o fluxo de dados transnacional passa a ser autorizado.



MEDIDAS DE GARANTIA APROPRIADAS

As **Normas corporativas globais** são medidas utilizadas a fim de permitir que empresas multinacionais e grupos econômicos realizem transferências intraorganizacionais de dados pessoais, ainda que as estejam situadas em diferentes países e sujeitas a diferentes legislações. No caso em que a empresa faça parte de um grupo econômico, e que este grupo já possua em prática normas corporativas globais aprovadas por autoridades competentes de proteção de dados pessoais no país de sua matriz (sede), as transferências internacionais poderão ocorrer entre os participantes do grupo de empresas. Entretanto, recomendamos que tão logo a ANPD entre em funcionamento, as normas corporativas globais já em uso sejam imediatamente submetidas para homologação pela ANPD.

Selos, certificados, códigos de conduta têm o potencial de demonstrar aos titulares de dados que determinadas empresas estão em conformidade com as leis de proteção de dados e assumem as responsabilidades e compromissos inerentes ao tratamento. Contudo, todos eles necessitam de avaliação pela Autoridade Nacional antes que sejam colocados em prática.

CELEBRAÇÃO DE ACORDOS E PARCERIAS COM INSTITUIÇÕES FINANCEIRAS

A celebração de acordos e parcerias com instituições estrangeiras que impliquem na transferência internacional de dados deve levar em conta, de maneira consistente, a finalidade da operação, sua conexão com o objeto contratual.

ATENÇÃO

A sua responsabilidade na cadeia de proteção de dados estará relacionada à legalidade da ordem emitida pelo Controlador. No papel de Controladora, suas responsabilidades serão mais abrangentes, uma vez que tomará as decisões referentes à condução do tratamento de dados.

Destaca-se que as responsabilidades relacionadas à proteção de dados pessoais permanecerão vigentes enquanto os dados estiverem acessíveis às partes envolvidas, mantendo-se válidas mesmo após o encerramento da vigência de convênios e parcerias.

Uma legislação robusta e sólida quanto à LGPD, não apenas serve como um guia para os brasileiros, permitindo-lhes ter mais controle sobre o uso de seus dados pessoais, mas também implica na criação de um ambiente de segurança jurídica. Isso envolve o estabelecimento de normas e procedimentos padronizados, proporcionando ao setor empresarial condições equitativas para competir.

Impacto da LGPD nas

EMPRESAS

REQUISITOS PARA TRATAMENTO DE DADOS PESSOAIS

Todas as organizações que processam dados pessoais devem cumprir as diretrizes estabelecidas pela lei, garantindo transparência, finalidade específica, consentimento adequado, quando necessário, e segurança no processamento desses dados.

IMPACTO NAS EMPRESAS DE GRANDE PORTE

Empresas de grande porte geralmente possuem volumes significativos de dados pessoais. Elas precisam investir em políticas de privacidade robustas, realizar avaliações de impacto à privacidade, implementar medidas de segurança avançadas e nomear um Encarregado de Proteção de Dados (DPO) para garantir conformidade total com a LGPD.

IMPACTO NAS EMPRESAS DE MÉDIO PORTE

Empresas de médio porte podem enfrentar desafios adicionais, pois podem ter recursos limitados em comparação com grandes corporações. No entanto, a conformidade é igualmente vital para elas. Investir em treinamento para funcionários, adoção de práticas de segurança da informação e implementação de processos eficientes é crucial para garantir a conformidade.

IMPACTO NOS SETORES SENSÍVEIS

Setores que lidam com dados sensíveis, como saúde e recursos humanos, estão sujeitos a regulamentações específicas. A LGPD impõe requisitos adicionais para o tratamento desses tipos de dados, incluindo medidas de segurança mais rigorosas e, em algumas vezes, a necessidade de consentimento explícito dos titulares dos dados.

REQUISITOS PARA TRATAMENTO DE DADOS PESSOAIS

EMPRESAS DE PEQUENO PORTE E MICROEMPRESAS

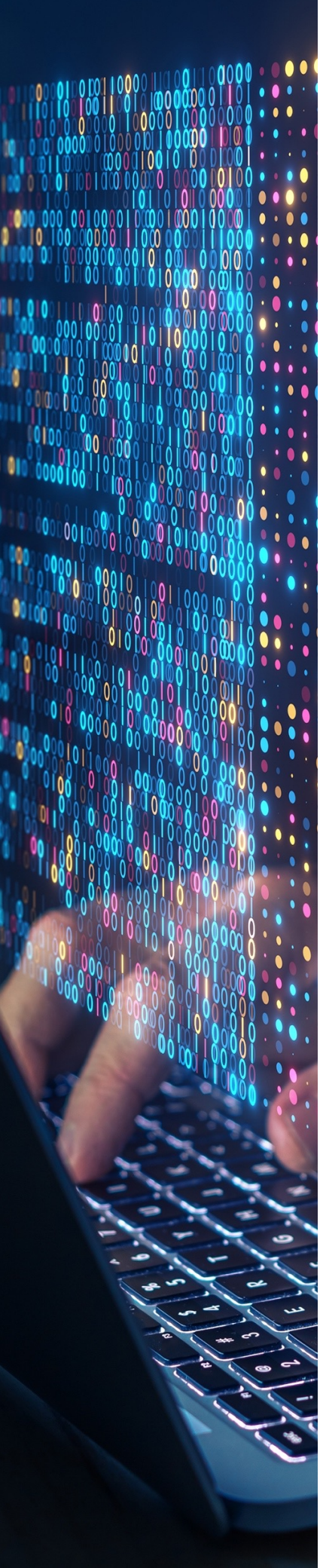
Mesmo pequenas e microempresas não estão isentas da LGPD. Elas também devem cumprir os princípios da lei, adaptando suas práticas de coleta, armazenamento e processamento de dados. Isso pode exigir a implementação de políticas internas, a revisão de contratos com terceiros e a garantia de que os titulares dos dados estejam plenamente cientes de como suas informações serão tratadas.

CONSEQUÊNCIAS POR NÃO CONFORMIDADE

Todas as empresas, independentemente do porte ou setor, estão sujeitas a penalidades significativas em caso de não conformidade com a LGPD. As multas podem variar de acordo com a gravidade da infração, chegando a valores substanciais. Além disso, a reputação da empresa pode ser afetada negativamente em casos de violações de dados.

Em resumo, a LGPD impacta empresas de todos os tamanhos e setores, exigindo uma abordagem proativa para garantir a conformidade e proteger efetivamente os dados pessoais dos cidadãos brasileiros. A colaboração com profissionais especializados, a implementação de medidas de segurança e a educação contínua são essenciais para enfrentar os desafios apresentados por essa legislação.

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD) representa um marco significativo no cenário jurídico e empresarial, impondo novos desafios e responsabilidades às organizações que lidam com dados pessoais. A adequação eficaz a essa legislação torna-se crucial para mitigar riscos legais e preservar a confiança do público



PRÁTICAS RECOMENDADAS PARA
AS EMPRESAS SE ADEQUAREM À

LGPD

Mapeamento de Dados: É importante realizar um detalhado mapeamento de dados pessoais que a empresa coleta, processa e armazena. Compreender a natureza e a finalidade dos dados é essencial para a implementação de medidas adequadas de proteção.

Avaliação de Riscos: É crucial que a Empresa conduza uma análise abrangente de riscos, identificando potenciais vulnerabilidades no tratamento de dados. Isso permitirá a implementação de medidas proporcionais para mitigar riscos e garantir a segurança dos dados.

Consentimento Informado: A empresa deverá utilizar as práticas de obtenção de consentimento, quando necessário, certificando-se de que os titulares dos dados estejam plenamente informados sobre como suas informações serão utilizadas, garantindo a transparência no processo.

Políticas de Privacidade e Governança: A empresa deverá elaborar e/ou ajustar políticas de privacidade robustas que estejam em conformidade com os requisitos da LGPD. Além disso, deverá instituir medidas de governança que garantam a segurança e o correto tratamento dos dados ao longo do ciclo de vida.

PRÁTICAS RECOMENDADAS PARA AS EMPRESAS SE ADEQUAREM À

LGPD

Treinamento e Conscientização: É importante que a Empresa possa Promover a educação e conscientização sobre a LGPD entre os colaboradores. O engajamento de toda a equipe é vital para assegurar uma cultura organizacional comprometida com a proteção dos dados pessoais.

Respostas a Incidentes: A empresa deverá desenvolver um plano de resposta a incidentes para lidar prontamente com possíveis violações de dados. Estabelecer procedimentos claros para notificação às autoridades competentes e aos titulares afetados, conforme exigido pela legislação.

Avaliação de Impacto à Proteção de Dados: Quando for aplicável, a Empresa deverá conduzir avaliações de impacto à proteção de dados para identificar e mitigar riscos significativos relacionados ao tratamento de dados pessoais.

Encarregado de Proteção de Dados: A nomeação de um Encarregado de Proteção de Dados é essencial para supervisionar a conformidade e servir como ponto de contato com autoridades e titulares dos dados.

O contexto atual aponta para uma crescente conscientização acerca da importância da privacidade e do tratamento adequado das informações pessoais. Nesse sentido, o futuro da LGPD no Brasil traz consigo desafios e oportunidades para aqueles que buscam adequar suas práticas e processos às exigências da legislação.

Essas práticas recomendadas, quando implementadas de forma integrada, contribuirão para a conformidade contínua com a LGPD, fortalecendo a posição legal e reputacional da empresa no tratamento responsável de dados pessoais.

Futuro da LGPD no

BRASIL

CONFORMIDADE COM AS LEIS

Destaca-se a necessidade de as organizações estarem plenamente conscientes das obrigações impostas pela LGPD. A conformidade efetiva exige uma revisão abrangente das políticas internas de tratamento de dados, bem como a implementação de mecanismos sólidos de segurança da informação.

A figura do Encarregado de Proteção de Dados (DPO) ganha relevância, sendo fundamental para garantir a conformidade contínua com a LGPD.
O DPO desempenha um papel crucial na supervisão e aconselhamento sobre as práticas de tratamento de dados, servindo como elo entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

OPORTUNIDADES

O futuro da LGPD também traz oportunidades para aqueles que investem proativamente em políticas de privacidade robustas. Empresas que adotam uma abordagem transparente e responsável em relação aos dados pessoais podem não apenas atender às exigências legais, mas também construir a confiança dos consumidores, o que se traduz em uma vantagem competitiva no mercado.
A evolução constante da LGPD também sugere a importância de uma vigilância constante das mudanças regulatórias e adaptação ágil às novas exigências. Isso implica não apenas na conformidade inicial, mas na implementação de uma cultura organizacional voltada para a proteção de dados, refletindo uma abordagem proativa diante das dinâmicas do ambiente legal.

E-book elaborado pelo Núcleo de LGPD da NWADV.

Lei Geral de Proteção de Dados (LGPD)

Márcia Ferreira

Head de Privacidade e Proteção de dados

marcia.ferreira@nwadv.com.br

NELSON WILIANS ADVOGADOS

25 ANOS