



Lei Geral de Proteção de Dados LGPD

Passo a passo para a empresa ficar em dia com a LGPD



Com a LGPD em pleno vigor é necessário que as empresas revisem suas práticas de segurança e transparência para cumprir a Lei e evitar multas. **Treinamentos de capacitação da equipe responsável, reavaliação da forma de coleta e de armazenamento de dados, além de atualização da política de privacidade são algumas das ações recomendadas.**

O checklist abaixo reúne os cinco passos necessários para ajudar as empresas a cumprir a Lei.



1. Mapeamento e classificação dos dados coletados e processados:

Para começar, o primeiro passo é identificar os dados pessoais que estão armazenados para poder categorizá-los por tipos. É importante se questionar sobre o objetivo dessas informações coletadas, como elas são coletadas, com quem elas são compartilhadas e como são guardadas.

Em seguida, é necessário separá-las de acordo com o tipo de dado. A lei exige consentimento específico para os dados pessoais sensíveis.



2. Medidas de segurança e transparência:

Em seguida, medidas de segurança e transparência devem ser introduzidas para minimizar os riscos de vazamentos, perdas e acessos não autorizados. Além de apostar em tecnologia, recomenda-se investir em treinamentos com a finalidade de capacitar e preparar a equipe. Também é importante criar na empresa a cultura da proteção de dados em todos os departamentos, por isso os treinamentos e ações que promovem a conscientização são fundamentais nesse processo.





3. Identificar e nomear os agentes de tratamento:

controlador e o operador. O primeiro tem poder de decisão sobre os dados coletados, geralmente é a própria empresa. Já o segundo é o responsável pelo tratamento de dados sob a ordem do controlador.



- 4. Nomear um encarregado de proteção de dados:** o controlador e o operador indicam o profissional que atua na fiscalização do cumprimento da empresa em relação às normas. Ele também trabalha como ponte de comunicação entre controlador, titulares dos dados e Autoridade Nacional de Proteção de Dados (ANPD).

5. Revisão dos contratos, termos de uso e políticas de privacidade:

Por fim, os termos de uso e política de privacidade precisam ser transparentes com os titulares dos dados. É preciso que detalhes estejam explícitos, como o motivo da coleta de dados, quem está armazenando as informações, quais os direitos do usuário, o objetivo do compartilhamento de dados com terceiros, entre outros. Por isso é fundamental que as empresas revisem seus contratos ou termos de uso de produtos ou serviços e as suas respectivas políticas de privacidade.



Titulares dos dados e seus direitos

A Lei Geral de Proteção de Dados traz um capítulo inteiro dedicado aos direitos dos titulares dos dados pessoais. Segundo a Lei, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, intimidade e privacidade.

Segundo a LGPD, o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:



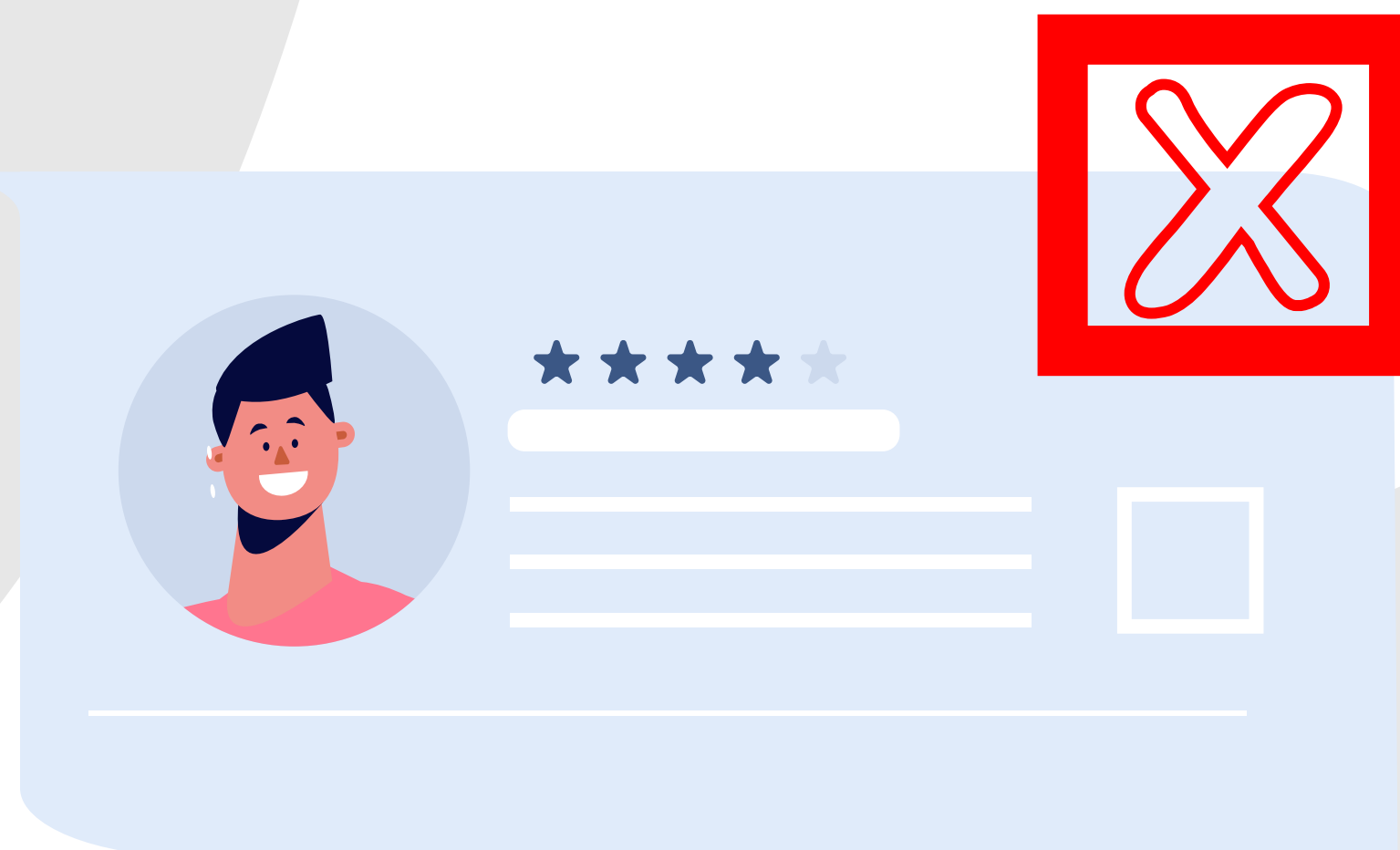
- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;



- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;



- Revogação do consentimento:
o titular dos dados pessoais tem
o direito de revogar seu consentimento
a qualquer tempo, através
de requerimento e sem custos.
As empresas devem facilitar
o procedimento interno para que isso
ocorra. O período em que as empresas
efetuaram o tratamento dos dados
sob o consentimento do titular fica
expressamente resguardado pela lei,
ou seja, as empresas não poderão ser
penalizadas por esse período.



- A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: em formato simplificado, imediatamente; ou 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, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular. Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.






- As informações e os dados poderão ser fornecidos: por meio eletrônico, seguro e idôneo para esse fim; ou sob forma impressa.
- Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.



- A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.
- O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
- O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

- 
- Em caso de não oferecimento de informações, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.
 - Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.
 - A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente.

Sigilo dos Dados e Boas Práticas

Cabe aos agentes de tratamento adotar 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.

Já o controlador é o responsável por comunicar à autoridade nacional 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, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos;
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata;
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

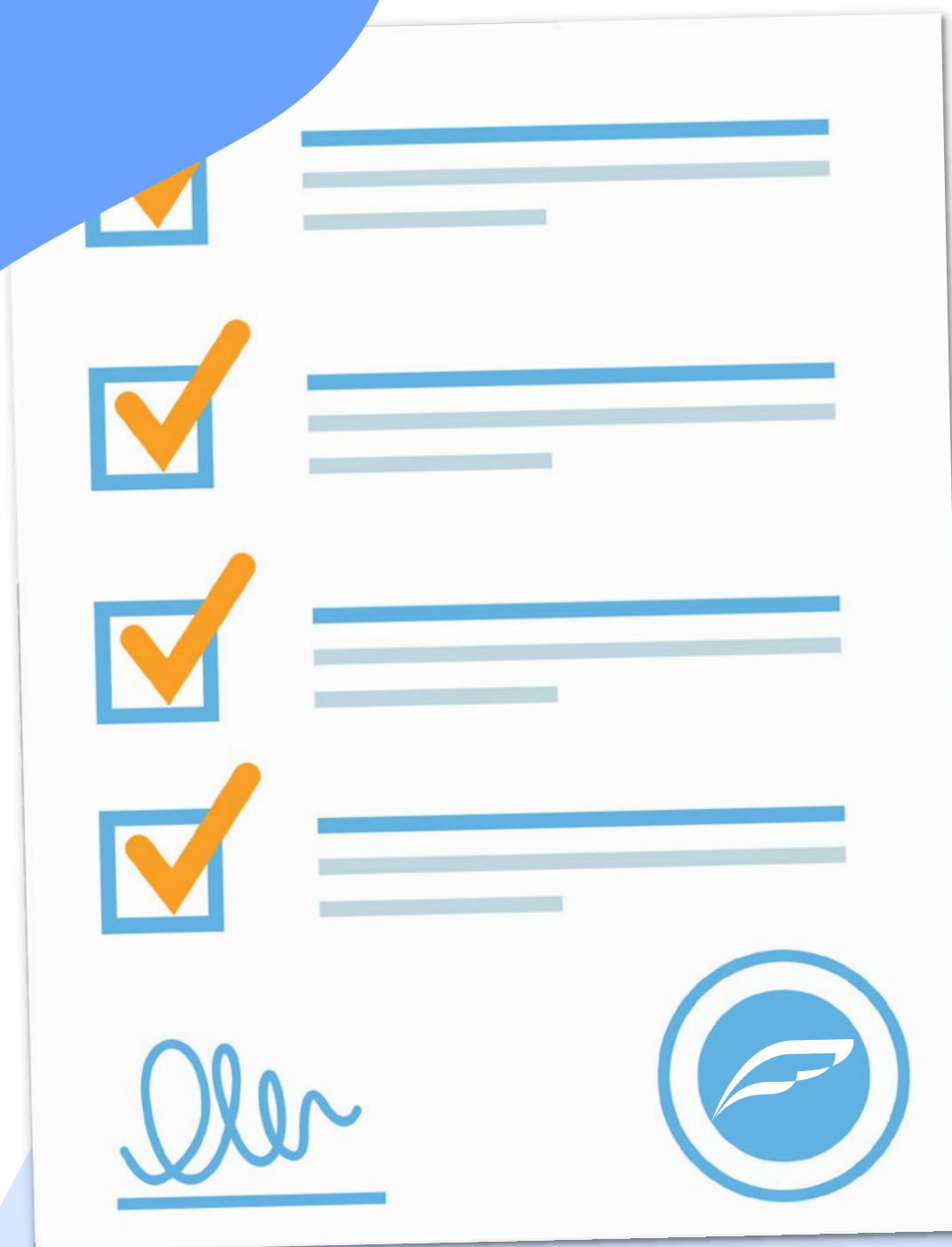


A autoridade nacional vai verificar a gravidade do incidente e poderá, caso necessário, determinar ao controlador a adoção de providências, tais como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou diminuir os efeitos do incidente.

Para evitar esses incidentes, é essencial a adoção de medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados acessá-los. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança.



É primordial que as empresas, através dos controladores e operadores, formulem regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, além das ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.



O programa de compliance e governança de dados tem o objetivo de estabelecer regras e políticas claras de boas práticas relacionadas ao tratamento de dados, além da elaboração periódica de relatórios de impacto com a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e as medidas para garantir a segurança das informações e a privacidade dos seus clientes, bem como as medidas adotadas para minimizar os riscos.



Considerações Finais

A série de três e-books buscou esmiuçar de maneira mais clara os principais pontos da Lei Geral de Proteção de Dados com o objetivo de ajudar os empresários a adequar seus negócios a essa realidade que veio para ficar.



A LGPD veio para fortalecer a segurança das relações jurídicas e a confiança dos clientes no tratamento de dados pessoais, garantindo a livre iniciativa, a livre concorrência e a defesa das relações comerciais e de consumo. A Lei favorece a concorrência e a livre atividade econômica, inclusive com portabilidade de dados.

A LGPD exige dos empresários uma adaptação, mas é primordial para o fortalecimento dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade dos indivíduos, além de garantir mais segurança jurídica a todos.

