

Política de Proteção de Dados dos Consumidores

1. Objetivo

A presente política tem o objetivo de Estabelecer diretrizes claras para a coleta, armazenamento, processamento e compartilhamento de dados pessoais dos consumidores, assegurando a proteção desses dados em conformidade com o Código de Defesa do Consumidor, com a Lei Geral de Proteção de Dados e outras legislações aplicáveis.

2. Âmbito de Aplicação

Esta política é aplicável a todas as operações da empresa que envolvam dados pessoais de consumidores, em todos os setores e por todos os colaboradores.

Referências Legais

Artigo 43 do Código de Defesa do Consumidor: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

Artigo 7º da Lei Geral de Proteção de Dados: tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

(...)

Artigo 9º da Lei Geral de Proteção de Dados: O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;

II - forma e duração do tratamento, observados os segredos comercial e industrial;

III - identificação do controlador;

IV - informações de contato do controlador;

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Artigo 18 da Lei Geral de Proteção de Dados: 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:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

V - 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; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

3. Governança de Dados

Comitê de Proteção de Dados: A empresa deve criar um Comitê de Proteção de Dados, que será responsável por supervisionar todas as atividades de tratamento de dados pessoais, assegurando a conformidade com a Lei Geral de Proteção de Dados. Este comitê deve ser

presidido por um Encarregado de Dados (Data Protection Officer - DPO), que atuará como ponto de contato entre a empresa e a Autoridade Nacional de Proteção de Dados (ANPD).

Registros de Atividades de Tratamento: Conforme o Artigo 37 da Lei Geral de Proteção de Dados, a empresa deve manter registros detalhados de todas as atividades de tratamento de dados pessoais, incluindo o propósito do tratamento, as categorias de dados tratados e os destinatários a quem os dados foram ou serão divulgados.

4. Coleta de Dados

Consentimento do Titular: Antes de iniciar a coleta de dados pessoais, é essencial obter o consentimento claro e inequívoco do titular, conforme estipulado no Artigo 7º da Lei Geral de Proteção de Dados. O consentimento deve ser específico para cada finalidade de tratamento e deve ser documentado de forma que possa ser facilmente acessado e verificado.

Finalidades Legítimas e Específicas: A coleta de dados deve estar atrelada a finalidades legítimas, específicas e explícitas, que devem ser informadas ao titular no momento da coleta. Qualquer uso dos dados que não esteja alinhado com estas finalidades deve ser evitado e considerado ilegal.

5. Armazenamento e Segurança

Medidas de Segurança: Implementar medidas de segurança robustas, tais como criptografia, firewalls, e controles de acesso, para proteger os dados pessoais contra acessos não autorizados, perda ou destruição acidental. A segurança deve ser uma preocupação contínua, com atualizações e testes regulares dos sistemas de segurança.

Política de Retenção: Definir uma política clara de retenção de dados, especificando quanto tempo os dados pessoais serão armazenados. Essa política deve estar em conformidade com os requisitos legais e apenas manter os dados pelo tempo necessário para cumprir as finalidades para as quais foram coletados.

6. Transparência e Comunicação

Política de Privacidade: Manter uma política de privacidade clara e acessível, que deve ser atualizada regularmente. Esta política deve detalhar todas as práticas de tratamento de

dados da empresa, incluindo como os dados são coletados, usados, compartilhados e protegidos, além de como os titulares podem exercer seus direitos.

Comunicação Ativa: Sempre que houver uma mudança significativa na forma como os dados pessoais são tratados, os titulares devem ser informados ativamente, garantindo que estão sempre cientes de como suas informações estão sendo manuseadas.

7. Direitos dos Titulares

Facilitação dos Direitos: Garantir que os titulares de dados possam facilmente exercer seus direitos previstos no Artigo 18 da Lei Geral de Proteção de Dados, incluindo o direito de acessar seus dados, solicitar correções, e requerer a eliminação ou bloqueio de seus dados quando necessário.

Procedimentos para Exercício de Direitos: Estabelecer procedimentos internos claros para responder às solicitações dos titulares de dados. Estes procedimentos devem ser eficientes e projetados para garantir que as solicitações sejam atendidas dentro dos prazos legais.

8. Avaliação de Impacto à Proteção de Dados (DPIA)

Realização de DPIAs: Antes de iniciar qualquer novo projeto de tratamento de dados que possa resultar em alto risco para a privacidade dos titulares, realizar uma Avaliação de Impacto à Proteção de Dados. Esta avaliação deve identificar e mitigar riscos potenciais associados ao tratamento de dados pessoais.

9. Treinamento e Conscientização

Programas de Capacitação: Desenvolver e implementar programas de treinamento regular para todos os colaboradores envolvidos no tratamento de dados pessoais, focando nas práticas seguras de tratamento e na importância de proteger a privacidade dos titulares.

10. Incidentes de Segurança

Plano de Resposta a Incidentes: Criar e manter um plano de resposta a incidentes de segurança de dados, que inclua procedimentos claros para a notificação imediata das partes afetadas e das autoridades regulatórias, conforme necessário.



11. Auditoria e Compliance

Auditorias Regulares: Realizar auditorias internas e externas regulares para verificar a conformidade com esta política e com a legislação vigente, garantindo que quaisquer deficiências sejam prontamente corrigidas.

12. Conclusão

Adotando e implementando esta política aprimorada, a empresa demonstra seu compromisso com a proteção da privacidade e dos dados pessoais de seus consumidores, fortalecendo a confiança e a segurança em todas as suas operações.