

Lei Geral da Proteção de Dados - LGPD

APRESENTAÇÃO

O presente manual tem o objetivo de orientar os colaboradores quanto aos procedimentos para a implementação da LGPD no âmbito dos seus clientes, fornecedores, órgãos públicos etc.

Tais orientações são fundamentais não só para garantir a correta aplicabilidade da lei, mas também para evitar a violação dos direitos do titular de dados em relação ao tratamento de dados pessoais efetuado pela empresa.

As recomendações para a implementação da LGPD estão baseadas no conjunto de normas legais relacionadas ao tema.



CULTURA ORGANIZACIONAL EM RELAÇÃO À LGPD

A adequação da empresa em relação à Lei Geral de Proteção de Dados está diretamente relacionada a uma transformação cultural das instituições, de modo que sejam atingidos todos os níveis, desde o estratégico até o operacional.



Essa mudança cultural envolve:

(i) refletir sobre a privacidade dos dados pessoais de todos, em todas as fases que envolvem o tratamento;

e

(ii) desenvolver ações de conscientização dos colaboradores, no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades empresariais cotidianas.

Nesse contexto, o diagnóstico da cultura organizacional tem como principal objetivo, identificar o nível de percepção dos servidores em relação à LGPD, orientar o encarregado de dados e aos demais, conforme as suas necessidades específicas, e promover melhoramentos em relação ao tratamento de dados.

É relevante que essa pesquisa seja feita de forma ampla, de modo a atingir um número expressivo de colaboradores, para que a partir da análise sobre a percepção e o conhecimento dessas pessoas sobre a proteção de dados pessoais, seja possível identificar a necessidade de ampliação da conscientização de toda a empresa em relação ao assunto. A avaliação em questão poderá ser realizada por meio do questionário sugerido no Anexo deste Manual.

DA GOVERNANÇA DE DADOS

1 Tão importante quanto a conscientização da empresa em relação à proteção de dados, é a governança desses, realizada mediante a análise do planejamento, gestão e controle do uso dos mesmos.

2 **A avaliação desses aspectos pode ser efetuada por meio do preenchimento de gestores da pasta, com o objetivo de mensurar quais são as práticas atuais, determinando em qual estágio a empresa se encontra, antes de avançar nas mudanças necessárias para adequação à LGPD, por intermédio de estratégias futuras.**

Ressalta-se a importância da realização periódica dessa avaliação, com a finalidade de acompanhar a evolução e a necessidade de eventuais melhorias, fundamentais à governança do tratamento.

3 ANÁLISE DOS DIAGNÓSTICOS

Baseado nos resultados dos diagnósticos realizados é possível iniciar uma estratégia de implementação à LGPD, dividida nos seguintes tópicos:

1. Mapear o tratamento dos dados pessoais;
2. Levantar os riscos do tratamento;
3. Elaborar o Relatório de Impacto à Proteção de Dados (RIPD);
4. Criar políticas de privacidade de dados e tratamento de incidentes, e adaptar os documentos internos e externos;
5. Canais de Comunicação;
6. Designar o Encarregado de Dados;
7. Treinar as equipes que tratam dados pessoais;
8. Associar o compliance à LGPD.

4 EXECUÇÃO DE MAPEAMENTO DE DADOS

Mapeamento de dados é uma atividade de catalogação de todo o fluxo de dados pessoais, que são objeto das operações de tratamento. Recomenda-se que as informações obtidas sejam mantidas em sistemas eletrônicos, facilitando a tomada de decisões e a manutenção de registros.

Esse levantamento pode ser realizado mediante o preenchimento de planilhas. Em paralelo ao mapeamento, é importante manter o inventário de dados pessoais, que visa entender, de forma detalhada, a variedade dos dados tratados na empresa e categorizá-los, mensurando os riscos existentes e seus impactos, servindo como base para elaboração de planos de ação mais direcionados e efetivos.

5 LEVANTAMENTO DE RISCOS

O levantamento de riscos tem como objetivo mitigá-los, por meio do controle e da redução desses, até que, em algum momento, eles sejam extintos. Trata-se de um procedimento que ajuda a planejar as ações preventivas tomadas por parte dos órgãos ou entidades estaduais.

Para que essa análise ocorra de forma satisfatória, todos os envolvidos no processo de tratamento de dados devem participar desse levantamento.

Considerando que o resultado é utilizado como um indicador que informa o nível dos riscos, a fim de obter um diagnóstico da situação, deve ser periodicamente revisitado e atualizado.

6 ELABORAÇÃO DE RELATÓRIO DE IMPACTO DE PROTEÇÃO À DADOS - RIPD

De acordo com o art. 5º, XVII da LGPD, relatório de impacto à proteção de dados pessoais é uma 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 riscos.

O conteúdo mínimo do RIPD está previsto no parágrafo único, do art. 38 da LGPD, devendo conter a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O Relatório de Impacto de Proteção de Dados (RIPD) deve ser elaborado, tanto na fase inicial do programa que inclui o tratamento de dados, quanto nas operações de tratamento que estão em andamento.

7 A ELABORAÇÃO DO RIPD DEVE CONTEMPLAR AS SEQUENTES ETAPAS:

A. Identificar os agentes de tratamento de dados: controlador, operador, encarregado;

B. Reconhecer a necessidade de elaborar o relatório:

- Para tratamento de dados pessoais realizados para fins de segurança da empresa e atividades de investigação e repressão de infrações penais.
- Quando houver infração da LGPD em decorrência do tratamento de dados pessoais,
- A qualquer momento sob determinação da ANPD (art. 38).

C. Descrever o tratamento: especificação da natureza, escopo, contexto e finalidade do tratamento que podem gerar riscos às liberdades civis e aos direitos fundamentais.

É importante que o RIPD seja revisado e atualizado anualmente ou quando houver mudança que atinja o tratamento dos dados pessoais realizados pela instituição.

8 Relatório de Impacto de Proteção de Dados (RIPD)

1. Descrição do tratamento de dados

Este relatório abrange o tratamento de dados de clientes da empresa realizado para fins de fornecimento de produtos e serviços, incluindo coleta, armazenamento, uso, compartilhamento e eliminação de dados.

2. Necessidade e proporcionalidade

O tratamento de dados pessoais é essencial para viabilizar o fornecimento dos produtos e serviços aos clientes, cumprindo obrigações legais e contratuais vinculadas à nossa atividade empresarial. Buscamos coletar e reter apenas os dados necessários para essas finalidades.

3. Mapeamento dos fluxos dos dados

- Coleta em formulários de cadastro e contratos.
- Armazenamento em bases de dados e sistemas internos.
- Uso para comunicações, suporte ao cliente e demais fins contratuais.
- Compartilhamento com parceiros quando necessário para prestação de serviço.
- Eliminação mediante solicitação ou após período de retenção.

4. Análise de riscos e medidas de segurança

Riscos identificados: acesso não autorizado, vazamento, modificação ou destruição acidental.

Medidas adotadas: criptografia, controle de acesso, firewall, treinamento, política de segurança, monitoramento, backup.

5. Consultas a stakeholders

Foram realizadas consultas a clientes, funcionários e parceiros a respeito do tratamento de dados. Os feedbacks recebidos foram analisados e incorporados a este relatório e aos processos de tratamento de dados.

6. Previsão de revisão periódica

Este RIPD será revisado anualmente a fim de garantir sua atualização e aderência às mudanças nos processos de tratamento de dados da empresa.

9 CRIAÇÃO DE POLÍTICAS DE PRIVACIDADE:

DE DADOS, TRATAMENTO DE INCIDENTES E ADAPTAÇÃO DE DOCUMENTOS INTERNOS E EXTERNOS

Criar Políticas de Privacidade de Dados e Tratamento de Incidentes é um dos passos mais importantes para adequação à LGPD, que visa atender o princípio da transparência previsto na lei.

1. POLÍTICA DE PRIVACIDADE DE DADOS

A Política de Privacidade de Dados é um documento informativo que descreve ao usuário a forma, os processos e os procedimentos adotados no tratamento dos dados pessoais e as medidas de privacidade empregadas.

Com relação ao conteúdo, recomenda-se que contenham as seguintes informações:

- Informação sobre a empresa e pelo tratamento;
- Quais os dados pessoais coletados e respectivas finalidades do tratamento, inclusive os dados não informados pelo usuário (exemplo: IP, localização, etc.);
- Fundamento legal do tratamento;
- Prazo de retenção dos dados pessoais;
- Informações de contato do encarregado de proteção de dados;
- Como são atendidos os direitos do titular, informando como ele pode acessar, retificar, solicitar a exclusão de dados, transferir, limitar ou se opor ao tratamento, e retirar o consentimento. No caso da inviabilidade de alguma operação, é necessário deixar claro o motivo. Entretanto, aconselha-se que esses casos sejam avaliados e autorizados pela área jurídica, sendo justificados por algum outro requisito legal.
- Se há o compartilhamento de dados com terceiros e qual a finalidade;
- Se há transferência internacional de dados;
- Proteção de dados de menores de idade, se for o caso;
- Proteção de dados sensíveis.

10 Política de privacidade em conformidade com a Lei Geral de Proteção de Dados (LGPD):

Política de Privacidade

A empresa Contável Escritório de Contabilidade Ltda zela pela privacidade e proteção dos dados pessoais coletados de seus clientes e usuários. Esta política explica como seus dados são tratados de acordo com a LGPD.

Dados coletados

A empresa Contável Escritório de Contabilidade Ltda coleta os seguintes dados para fornecer seus produtos e serviços:

- Dados de identificação, como nome, CPF, RG, data de nascimento e gênero.
- Dados de contato, como endereço residencial, telefone e e-mail.
- Dados financeiros e de pagamento, como renda, dados bancários e histórico de pagamentos.
- Dados de contratos, como propostas comerciais e contratos firmados.
- Dados de navegação no nosso site e aplicativo.

Finalidades do tratamento dos dados

Os dados coletados têm as seguintes finalidades:

- Cumprimento de obrigações legais e regulatórias.
- Prestação de serviços solicitados pelo titular dos dados.
- Envio de comunicações sobre serviços, como boletins e alertas.
- Resposta a solicitações e suporte ao cliente.

Compartilhamento de dados com terceiros

A empresa Contável Escritório de Contabilidade Ltda não compartilha dados pessoais exceto quando necessário para:

- Cumprir obrigações legais e regulatórias.
- Execução de serviços por parte de fornecedores e parceiros.

Segurança dos dados

Adotamos medidas técnicas e organizacionais para proteger seus dados contra acessos não autorizados, perda acidental, destruição ou alteração.

Direitos do titular dos dados

Você pode exercer seus direitos de acesso, correção, exclusão, portabilidade e outros previstos na LGPD entrando em contato conosco pelo e-mail: privacidade@empresa.com.br.

Atualização da política

Reservamos o direito de modificar esta Política de Privacidade a qualquer momento, sendo as alterações devidamente publicadas em nossos canais.

Dúvidas sobre privacidade

Em caso de dúvidas sobre nossas práticas de privacidade, entre em contato pelo e-mail: dpo@empresa.com.br.

11

1. POLÍTICA DE TRATAMENTO DE INCIDENTES

Considera-se incidente com dados pessoais, o evento que leva à destruição, à perda, à alteração, à divulgação ou ao acesso não autorizados, de forma acidental ou ilícita, a dados pessoais transmitidos, armazenados ou processados pelos órgãos ou entidades.

Nesse contexto, é importante a elaboração de uma Política de Tratamento de Incidentes, que serve para orientar a todos da empresa acerca dos procedimentos mais adequados e a descrição dos canais de comunicação a serem executados quando da ocorrência de incidentes com dados pessoais.

Política de Tratamento de Incidentes em conformidade com a LGPD:

Política de Tratamento de Incidentes de Segurança

1. Objetivo

Esta política visa estabelecer diretrizes e procedimentos para lidar com incidentes de segurança relacionados a dados pessoais, em conformidade com a Lei Geral de Proteção de Dados.

2. Conceito de incidente

Incidente de segurança é qualquer evento adverso, confirmado ou sob suspeita, relacionado ao tratamento de dados pessoais que gere acesso, destruição, alteração, comunicação ou qualquer forma de uso inadequado ou ilícito desses dados.

3. Notificação ao Controlador

O Operador ou os colaboradores que identificarem um incidente real ou suspeito devem notificar imediatamente o Controlador, descrevendo detalhadamente o ocorrido e as medidas emergenciais adotadas.

4. Análise e contenção

O Controlador irá conduzir uma análise para determinar a natureza e extensão do incidente. Buscará avaliar os riscos envolvidos e adotar medidas para conter os impactos e prevenir novos danos.

5. Notificação à ANPD e aos titulares

Conforme exigido na LGPD, o Controlador notificará a Autoridade Nacional de Proteção de Dados e aos titulares afetados sobre incidentes que possam gerar riscos ou danos relevantes.

6. Investigação e documentação

Todas as causas e efeitos do incidente deverão ser detalhadamente investigados e documentados pelo Controlador.

7. Ações corretivas

Caberá ao Controlador adotar medidas corretivas para eliminar vulnerabilidades técnicas e administrativas identificadas durante a análise do incidente.

8. Prevenção

A empresa deverá continuamente investir em treinamentos, controles, segurança da informação e outras ações para prevenir incidentes de segurança no tratamento de dados pessoais.

9. Revisão das políticas

Esta Política de Tratamento de Incidentes será revisada anualmente ou sempre que necessário para garantir sua efetividade.

12 1. ADAPTAÇÕES DE DOCUMENTOS INTERNOS E EXTERNOS

Todos os documentos da empresa devem estar em conformidade com os demais pertinentes à LGPD. Assim, deve ser feita a revisão de contratos e demais documentos (impressos e digitais) para a realização de uma atualização e padronização.

CANAIS DE COMUNICAÇÃO

1. DOS TITULARES DE DADOS

O titular de dados ou seu representante legal, serão atendidas eletronicamente, junto à Ouvidoria- Geral da empresa, onde os dados se encontram, mediante a apresentação de documentos oficiais que permitam a identificação.

1. DOS ENCARREGADOS DE DADOS

Os questionamentos dos encarregados de dados dos órgãos e entidades a respeito da implementação da LGPD poderão ser realizados por meio do e-mail: lgpd@empresa.com.br, cujas respostas serão encaminhadas dentro do prazo de 10 dias úteis.

13 TREINAMENTO DAS EQUIPES QUE TRATAM DADOS PESSOAIS

É imprescindível que todos os colaboradores conheçam as regras estabelecidas na LGPD, particularmente aqueles que tratam diretamente os dados pessoais. Esse alinhamento garante que todos estejam a par das mudanças, afastando eventuais irregularidades.

Nesse contexto, a empresa vem desenvolvendo um conjunto de ações, que envolvem cursos e capacitações, visando disseminar informações e orientações aos colaboradores da empresa sobre a LGPD, a fim de reorientar a implementação da Lei.

Em paralelo, compete ao controlador de dados de cada setor, conforme, e em atenção aos respectivos sistemas de dados, orientar os operadores por meio de termos de uso, manuais e treinamentos quanto ao tratamento de dados sob sua responsabilidade.

14 COMPLIANCE E LGPD

O significado sintético de Compliance, é agir de acordo com uma regra, e **"estar em Compliance"**, é estar em conformidade com leis e regulamentos internos e externos, por meio de métodos e técnicas que visam prevenir, detectar e responder a possíveis problemas de desvio entre as normas estabelecidas e a prática das instituições públicas ou privadas.

Nesse sentido, ao "estar em Compliance" com as boas práticas e padrões existentes, isto é, cobrindo comportamentos futuros inadequados que podem macular a sua reputação, da empresa se fortalece e promove a transparência de suas ações, garantindo uma gestão eficiente e confiável no tratamento de dados pessoais.

15 PLANO DE AÇÃO LGPD

Anexo I Deve ser implementado e arquivado pela empresa.

16 DIAGNÓSTICO CULTURA ORGANIZACIONAL – LGPD

Anexo I Deve ser implementado e arquivado pela empresa.

Anexo I

PROCESSOS	RESPONSÁVEL	DATA INÍCIO	DATA FIM
Diagnóstico da cultura organizacional			
Diagnóstico da governança de dados			
Elaboração do inventário de dados pessoais - guia de elaboração de inventário de dados			
Mapeamento de dados pessoais			
Levantamento de Riscos/ Elaboração do RIPD			
Criação de Políticas de Privacidade de Dados, Tratamento de Incidentes e adaptação de documentos internos e externos			
Designação do Encarregado de Dados			
Treinamento das equipes que tratam dos dados pessoais			

DIAGNÓSTICO - CULTURA ORGANIZACIONAL – LGPD

Este diagnóstico inicial identificar o conhecimento de todos os colaboradores, sobre a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018. São 10 (dez) perguntas e não há identificação das pessoas. Prazo para resposta: *Obrigatório

1. Insira sua unidade/setor: *

2. Você já participou de capacitação sobre a Lei Geral de Proteção de Dados dentro ou fora da empresa? *

Palestra, Seminário, Curso (Presencial ou EaD), Leitura de textos e documentos;

Não possuo capacitação no assunto Outro: 3. Você sabe o que são dados pessoais? Sim Não

4. Em seu trabalho, você realiza alguma atividade que envolve dados pessoais? *

Sim, Não, Não sei.

5. Por quais meios você trabalha com dados pessoais? *

Sistemas, Planilhas Eletrônicas, Documentos Eletrônicos, Documentos Físicos. Não sei dizer se trabalho com dados pessoais no dia a dia Outro:

6. Dos fluxos que fazem parte do seu trabalho, em quais você faz uso de dados pessoais? *

Distribuição, Requisição de informações, Análise jurídica, Requerimentos diversos. Solicitação de cumprimento de decisões, Não sei informar Outro:

7. Por quais meios você recebe as solicitações para trabalhar com dados pessoais na empresa? *

E-mail, Físico, Telefone, Não sei responder Outro:

8. Há alguma orientação a respeito do tratamento dos dados pessoais que instruem as solicitações ou requerimentos? *

Sim, Não, Não é necessária orientação, pois o uso da informação é institucional Outro:

9. Somente os dados pessoais estritamente necessários são acessados? *

Sim, Não, Não sei informar.

10. Deseja fazer alguma consideração sobre o assunto Proteção de Dados?

Sim, Não, Se sim, descreva.

Considerações finais sobre implementação da LGPD

- Alinhe a cultura de sua empresa e reflita para garantir que o gerenciamento da privacidade seja incorporado às suas operações diárias.
- Implementar uma política de privacidade clara e concisa, refletindo seu compromisso com a LGPD e garantindo que os documentos internos/externos sejam atualizados de acordo.
- Forneça canais de comunicação adequados para que os titulares dos dados relatem dúvidas e incidentes e garanta a implementação de processos abrangentes de gerenciamento de incidentes.
- Realizar treinamento para todos os funcionários para aumentar a conscientização sobre privacidade, com ênfase nos indivíduos que lidam com dados pessoais.
- Formar e gerenciar equipes responsáveis pela conformidade com todos os requisitos da LGPD.

Empresa: Contável Escritório de Contabilidade Ltda

CNPJ: 05.499.833/0001-62

Data: 07/08/2023

Autor do Manual

Márcio Alves Pimentel

Advogado Tributarista - OABRJ129778

Consultor Empresarial

Instagram @marciopimenteltributarista

www.studiotax.com.br

www.ignicaoempreendedora.com.br/tlmFTFW