

Guia de Recomendações e Boas Práticas de Conformidade com a LGPD para Sites WordPress (2025)

O que é a Lei 13.709/2018?

A Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018, é o marco legal brasileiro que dispõe sobre o tratamento de dados pessoais, tanto em meios físicos quanto digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

A estruturação da LGPD foi fortemente inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, considerado a referência global mais robusta em privacidade, alinhando o Brasil às melhores práticas internacionais e facilitando as relações comerciais com mercados que exigem um nível adequado de proteção de dados.

O texto integral da lei pode ser consultado [clikando aqui](#).

Aviso Legal Importante: Este documento possui caráter orientativo e informativo. As recomendações aqui contidas representam boas práticas de mercado para a adequação básica de websites à Lei Geral de Proteção de Dados (LGPD). **Este guia não constitui e não substitui uma consultoria jurídica especializada.** Para uma conformidade completa e análise legal do seu negócio, é fundamental consultar um advogado ou escritório especializado em Direito Digital e Proteção de Dados.

1. Páginas Essenciais: A Base da Transparência

Todo site que coleta dados, mesmo que seja apenas um e-mail para newsletter, precisa ser transparente sobre como esses dados são tratados. Os dois pilares para isso são a Política de Privacidade e os Termos de Uso, que devem constar mesmo se você tiver apenas uma **Landing Page!**

Política de Privacidade vs. Termos de Uso: Qual a diferença?

Siga para a próxima página.

1.1 Termos de Uso

Pense neles como as "regras do jogo" para quem navega no seu site. Este documento estabelece os direitos e deveres tanto do visitante quanto do proprietário do site. Ele deve abordar tópicos como: propriedade intelectual do conteúdo (textos, imagens), limitações de responsabilidade, regras para comentários de usuários e as condições gerais para utilização do serviço ou produto oferecido.

Após desenvolvimento e revisão do texto (de preferência pelo seu advogado), seu desenvolvedor deverá incluir no site uma página de URL semelhante à:

<https://seusite.com.br/termos-de-uso/>

Recomendo a inserção desta página no **menu footer do site**, estando disponível em "all pages".

1.2 Política de Privacidade

Este documento é focado exclusivamente em **dados pessoais**. É uma exigência direta da LGPD. Ele deve explicar de forma clara e acessível:

- **Quais dados** são coletados (ex: nome, e-mail, telefone, IP, dados de navegação).
- **Para qual finalidade** cada dado é coletado (ex: enviar uma compra, responder a um contato, enviar e-mails de marketing).
- **Como** os dados são armazenados e por **quanto tempo** (o ciclo de vida do dado).
- Com **quem** os dados podem ser compartilhados (ex: gateways de pagamento, ferramentas de e-mail marketing, plataformas de anúncio).
- Quais são os **direitos do titular dos dados** e como ele pode exercê-los (correção, exclusão, canal de contato para tal, etc.).
- Informações sobre o uso de **cookies**.

Na Política de Privacidade, mencionar o Encarregado de Dados (DPO - Data Protection Officer).

A LGPD prevê a figura do Encarregado, que é o ponto de contato entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Para PMEs, a ANPD flexibilizou essa exigência, não sendo obrigatória a contratação de uma pessoa exclusiva para a função.

Mas, mesmo não sendo obrigatório ter um DPO formal, é uma excelente prática **designar internamente uma pessoa (ou o próprio dono do negócio) como o ponto focal responsável por assuntos de privacidade**.

O e-mail "privacidade@seusite.com.br" deve ser direcionado a essa pessoa.

Mencionar: "Para assuntos relacionados à proteção de dados, o responsável em nossa empresa pode ser contatado através do e-mail..."

Da mesma forma, após o desenvolvimento e revisão do texto (de preferência pelo seu advogado), seu desenvolvedor deverá incluir no site uma página de URL semelhante à:

<https://seusite.com.br/politica-de-privacidade/>

Recomendo a inserção desta página no **menu footer do site**, estando disponível em “all pages”.

1.3 Recomendação Adicional: A Página de "Aviso Legal" para Produtos Informacionais

Para sites que comercializam produtos ou serviços cujo **resultado depende da aplicação e esforço do cliente** (como cursos online, e-books, mentorias e consultorias), é altamente recomendável a criação de uma página de **Aviso Legal (Disclaimer)**.

Embora não seja um requisito direto da LGPD, esta página complementa os Termos de Uso e a Política de Privacidade, reforçando a **transparência e a boa-fé**, princípios basilares da lei.

A finalidade desta página é gerenciar as expectativas do consumidor e mitigar riscos jurídicos, deixando explícito que o sucesso do cliente não é garantido e depende de múltiplos fatores individuais.

Uma página de Aviso Legal eficaz deve conter, de forma clara e direta, os seguintes pontos:

- **Isenção de Responsabilidade de Resultados:** Afirmar que o produto ou serviço não garante a obtenção de resultados específicos, sejam eles financeiros, de performance ou qualquer outra natureza.
- **Responsabilidade do Cliente:** Enfatizar que o sucesso é condicionado ao empenho, dedicação, estudo e correta aplicação do conhecimento por parte do cliente, além de outros fatores que estão fora do controle da empresa.
- **Natureza Educacional do Conteúdo:** Esclarecer que as informações, técnicas e estratégias compartilhadas têm propósito educacional e informativo, não se configurando como uma promessa de ganho ou solução garantida.
- **Exemplos (Depoimentos) Não São Garantias:** Se utilizar depoimentos ou estudos de caso, ressaltar que os resultados apresentados são atípicos e não representam uma garantia de que o novo cliente alcançará o mesmo.

A adoção desta página demonstra profissionalismo e protege legalmente o negócio contra possíveis contestações, ao estabelecer um acordo transparente sobre o que o cliente pode esperar do produto ou serviço adquirido.

Igualmente, após o desenvolvimento e revisão do texto (de preferência pelo seu advogado), seu desenvolvedor deverá incluir no site uma página de URL semelhante à:

<https://seusite.com.br/aviso-legal/>

Recomendo a inserção desta página no **menu footer do site**, estando disponível em “all pages”.

2. Coleta de Dados e Gerenciamento de Consentimento

O consentimento é um dos pilares da LGPD. Ele precisa ser livre, informado e inequívoco.

2.1 Aviso e Gestão de Cookies

É fundamental ter um sistema que informe o usuário sobre o uso de **cookies** e permita que ele gerencie suas preferências.

Recomendação Técnica: Plugins como o **CookieYes (que eu utilizo)** ou **Complianz** para WordPress são excelentes para implementar banners de consentimento de forma profissional.

Nota sobre o GTM (Google Tag Manager): Atualmente, a prática mais rigorosa é condicionar o disparo de tags de marketing e análise (como as do Google Analytics 4, Meta Pixel, etc.) ao aceite explícito do usuário no banner de *cookies*.

Todavia não é um aspecto crítico (ainda) e pode trazer complicações para o funcionamento do seu sistema de *tracking*.

Neste viés sempre recomendo que você procure suporte profissional.

2.2 Formulários de Contato e Inscrição

Inclua um *checkbox* clicável (que **não venha pré-marcado**) com uma frase clara, como: "Li e concordo com a Política de Privacidade e autorizo o contato da equipe." ou "Aceito receber comunicações e novidades por e-mail da XPTO LTDA.".

O consentimento precisa ser uma ação ativa do usuário.

2.3 Automações e E-mail Marketing

Toda comunicação por e-mail deve conter um link de descadastro (opt-out) claro, visível e funcional. O processo de remoção da lista deve ser simples e imediato.

3. Segurança da Informação: Protegendo os Dados

A LGPD exige que medidas técnicas e administrativas sejam adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

3.1 Certificado de Segurança (SSL)

É obrigatório que o site utilize o protocolo HTTPS. Isso criptografa a comunicação entre o navegador do usuário e o servidor, garantindo que os dados enviados (como em formulários) não possam ser facilmente interceptados. Verifique se seu certificado SSL está ativo e válido.

Considere a utilização de um serviço consolidado de CDN (Content Delivery Network).

3.2 Proteção do Ambiente WordPress

A segurança vai além do SSL. Utilize plugins de segurança robustos para proteger as camadas de aplicação (*front-end*) e de dados (*back-end*).

Recomendação Técnica: Plugins como **Wordfence Security** ou **Solid Security** (antigo **iThemes Security**) oferecem recursos como *firewall* de aplicação (WAF), *scanner* de *malware*, proteção contra força bruta e monitoramento de integridade dos arquivos.

Os plugins podem constar de versões *premium* (com assinatura) e gratuitas. **Procure um profissional para a instalação e configuração dos parâmetros de acordo com as especificidades do seu negócio.**

Aspectos de segurança da sua infraestrutura como autenticação de dois fatores (2FA), manutenção do próprio sistema WordPress e setup do seu Servidor de Hospedagem são inegociáveis.

3.3 Canal para Solicitação dos Titulares

É um direito do usuário solicitar a visualização, correção ou exclusão de seus dados.

Defina e divulgue um canal oficial para isso (DPO - anteriormente mencionado), geralmente um e-mail dedicado, como o privacidade@seusite.com.br.

4. Direitos do Consumidor e Governança

4.1 Políticas de Devolução e Garantia

Para e-commerces (produtos físicos ou digitais), sites que vendem serviços e afins, deixe as **políticas de reembolso, cancelamento, devolução e garantia em local visível** e com texto claro, em conformidade com o Código de Defesa do Consumidor (**CDC**).

4.2 Transparência sobre a Empresa

Disponibilize informações claras sobre a identidade da sua empresa, como **CNPJ** (se aplicável), nome e informações de contato verificáveis.

Sempre recomendo que no rodapé do site (*container footer - all pages*) existam: número de telefone, endereço, CNPJ e ao menos um email de contato.

5. Ciclo de Vida e Tratamento Ético dos Dados

Esta é uma seção crucial para gerar confiança com seu público.

5.1 Definição do Ciclo de Vida

Comunique em sua Política de Privacidade como o ciclo de vida dos dados é gerenciado. Isso envolve:

- **Coleta:** Quais dados e por qual motivo.
- **Armazenamento e Retenção:** Onde são armazenados (ex: servidor da hospedagem, plataforma de automação de marketing CRM, etc.) e por quanto tempo serão mantidos (ex: "dados de leads inativos por mais de 2 anos serão excluídos de nossa base").
- **Uso:** Como são utilizados no dia a dia.
- **Compartilhamento:** Com quais operadores/parceiros são compartilhados e por quê.
- **Descarte:** Como são eliminados de forma segura ao final do ciclo.

5.2 Compromisso de Não Comercialização

Enfatize de forma explícita na sua Política de Privacidade:

"Nossa empresa se compromete a não vender, alugar ou negociar, sob qualquer hipótese, a sua base de contatos com terceiros."

Esta declaração tem um forte impacto positivo na percepção de confiança do usuário.

<Esta documentação termina aqui.>

Dúvidas?
Estamos à disposição.

