

LGPD NO E-COMMERCE

Como usar dados para vender sem
transformar informação em risco

GUIA PRÁTICO • ATUALIZADO EM 2026



INTRODUÇÃO

Dados fazem a venda acontecer e também concentram risco

Cadastro, *checkout*, pagamento, antifraude, entrega, atendimento e marketing dependem de dados pessoais. A LGPD não proíbe esse uso: ela exige que a empresa saiba por que trata cada informação, limite excessos e consiga demonstrar suas escolhas.

A IDEIA CENTRAL

Conformidade não começa com uma política de privacidade. Começa com um mapa da operação: quais dados entram, para qual finalidade, quem acessa, com quem são compartilhados e quando devem ser eliminados.

Este guia foi elaborado para lojas virtuais, sellers, marketplaces e prestadores de tecnologia. Ele apresenta controles práticos sobre bases legais, fornecedores, direitos, segurança, retenção e incidentes.

O conteúdo considera a transformação da ANPD em agência reguladora pela Lei nº 15.352/2026 e as regulamentações vigentes. Não substitui análise da operação concreta.

01 O mapa de dados

ETAPA	DADOS E PERGUNTA DE CONTROLE
Navegação	Cookies, IP e eventos: o que é necessário e o que é marketing?
Cadastro	Identificação e contato: todos os campos são indispensáveis?
Checkout	Endereço e pagamento: quem recebe e quem armazena?
Antifraude	Sinais, score e decisão: há transparência e revisão adequada?
Entrega	Destinatário e rastreo: quais parceiros acessam?
Atendimento	Conversas e anexos: por quanto tempo são retidos?
Pós-venda	Histórico e marketing: a nova finalidade é compatível?

02 Quem decide e quem executa

PAPEL	NA PRÁTICA
Controlador	Define finalidades e elementos essenciais do tratamento. A loja costuma ser controladora dos dados de seus clientes.
Operador	Trata dados em nome do controlador e conforme instruções, dentro do papel contratado.
Controladoria conjunta	Duas ou mais organizações participam de decisões relevantes; depende da realidade, não do rótulo contratual.
Encarregado	Canal de comunicação e apoio à governança, conforme a LGPD e a regulamentação.
Suboperador	Fornecedor contratado pelo operador para parte do tratamento, sujeito a controle e transparência.
CONTRATO NÃO ALTERA OS FATOS Chamar toda empresa de “operadora” não elimina decisões próprias sobre dados. Gateway, marketplace e antifraude podem assumir papéis diferentes conforme o fluxo.	

03 Consentimento não é regra universal

FINALIDADE	BASE A AVALIAR
Processar e entregar o pedido	Execução de contrato ou procedimentos preliminares.
Emitir documento fiscal	Cumprimento de obrigação legal ou regulatória.
Prevenir fraude e proteger a conta	Legítimo interesse ou outra hipótese adequada, com necessidade e salvaguardas.
Defender direito em processo	Exercício regular de direitos.
Enviar campanha promocional	Consentimento ou legítimo interesse, conforme contexto, expectativa e controles.
Dado sensível	Somente uma hipótese específica do art. 11, quando aplicável.
CONSENTIMENTO VÁLIDO Quando utilizado, deve ser livre, informado, inequívoco, específico e revogável.	

04 Princípios que reduzem risco

- finalidade: trate para objetivos legítimos, específicos e informados;
- adequação: mantenha compatibilidade entre uso e contexto;
- necessidade: limite dados ao mínimo pertinente;
- livre acesso e transparência: permita compreensão e consulta;
- qualidade: mantenha informações corretas e atualizadas;
- segurança e prevenção: reduza riscos de acesso, perda e alteração;
- não discriminação: impeça usos abusivos;
- responsabilização: guarde evidências das medidas adotadas.

EXEMPLO

Data de nascimento obrigatória para comprar um produto comum pode ser excesso. Para item com restrição etária, a necessidade muda e deve ser documentada.

05 Privacidade, cookies e marketing

A política de privacidade deve explicar a operação em linguagem acessível. Banner de cookies e formulário não corrigem fluxos excessivos nem compartilhamentos desconhecidos.

- separe cookies estritamente necessários dos opcionais;
- evite ativar tecnologias não essenciais antes da escolha quando ela for exigida;
- ofereça mecanismo simples para rever preferências;
- identifique categorias de parceiros e finalidades;
- registre origem da lista e oposição ao marketing;
- não compre bases sem verificar licitude, qualidade e transparência;
- alinhe política, banner, tags e configuração técnica.

MARKETING RESPONSÁVEL

Legítimo interesse exige teste de finalidade, necessidade e balanceamento. O titular deve ter oposição simples e efetiva.

06 Fornecedores e plataformas

Hospedagem, ERP, gateway, antifraude, logística, CRM, agência e analytics podem acessar dados. A contratação precisa acompanhar o risco do serviço.

- ☐ mapear dados, finalidade, papel e localização do tratamento;
- ☐ definir instruções, confidencialidade e controle de acesso;
- ☐ prever subcontratação e cooperação com direitos dos titulares;
- ☐ exigir comunicação rápida de incidentes;
- ☐ regular devolução, eliminação e portabilidade ao encerrar;
- ☐ avaliar transferências internacionais;
- ☐ guardar evidências de diligência e monitoramento.

MARKETPLACE

A plataforma não é automaticamente operadora do seller. Ela pode decidir finalidades próprias e atuar como controladora em parte da jornada.

07 Direitos dos titulares

SOLICITAÇÃO	RESPOSTA OPERACIONAL
Confirmação e acesso	Validar identidade, localizar sistemas e fornecer resposta adequada.
Correção	Atualizar o dado e propagar a correção quando necessário.
Eliminação ou anonimização	Analisar excesso, base legal e obrigações de retenção.
Informação sobre compartilhamento	Explicar entidades ou categorias de destinatários.
Revogação e oposição	Interromper o fluxo correspondente quando cabível.
Revisão de decisão automatizada	Explicar critérios e permitir tratamento compatível com a lei.

PRAZO E FORMATO

A resposta depende do direito exercido e da regulamentação. Tenha protocolo, verificação de identidade, responsáveis e registro da decisão.

08 Segurança aplicada ao e-commerce

CONTROLE	APLICAÇÃO
Acesso	Privilegio mínimo, revisão periódica e desligamento imediato.
Autenticação	Múltiplos fatores para painéis, e-mail e fornecedores críticos.
Criptografia	Proteção em trânsito e, conforme risco, em armazenamento.
Desenvolvimento	Atualizações, testes, segredos protegidos e revisão de código.
Monitoramento	Logs, alertas, antifraude e detecção de comportamento anômalo.
Continuidade	Backup testado, recuperação e responsáveis pela crise.
PAGAMENTO Evite armazenar dados completos de cartão quando não for necessário. Use fornecedores adequados e limite o ambiente exposto.	

09 Incidente de segurança

- conter o evento sem destruir evidências;
- acionar jurídico, tecnologia, liderança e fornecedores;
- identificar sistemas, dados, titulares e período afetado;
- avaliar risco ou dano relevante;
- documentar decisões e medidas de mitigação;
- preparar comunicação clara, quando obrigatória;
- preservar relatório e registros do tratamento do incidente.

PRAZO REGULAMENTAR

O controlador deve comunicar à ANPD e aos titulares o incidente que possa acarretar risco ou dano relevante, em três dias úteis contados do conhecimento de que dados pessoais foram afetados, ressalvada legislação específica.

Referência: Resolução CD/ANPD nº 15/2024.

10 Retenção e descarte

GRUPO	CRITÉRIO
Cadastro	Relação ativa, finalidade e solicitações do titular.
Pedido e fiscal	Obrigações legais, contratuais e defesa de direitos.
Atendimento	Finalidade, histórico da relação e risco de conflito.
Marketing	Base legal, oposição, inatividade e origem do contato.
Logs	Obrigações específicas, segurança e Marco Civil.
Candidatos e equipe	Relação trabalhista, recrutamento e obrigações próprias.

MATRIZ DE RETENÇÃO

Defina categoria, sistema, responsável, fundamento, prazo e método de eliminação. Backup e cópias exportadas também precisam entrar no plano.

11 Checklist LGPD

- ☐ Existe mapa atualizado dos dados e sistemas?
- ☐ Cada finalidade possui base legal documentada?
- ☐ Campos obrigatórios são realmente necessários?
- ☐ Política, cookies e configurações técnicas coincidem?
- ☐ Fornecedores críticos têm contrato e avaliação de risco?
- ☐ Direitos dos titulares possuem canal e responsáveis?
- ☐ A empresa sabe localizar e corrigir dados em todos os sistemas?
- ☐ Acessos são individuais, revisados e protegidos por MFA?
- ☐ Há matriz de retenção e descarte executável?
- ☐ O plano de incidente prevê avaliação e prazo de três dias úteis?
- ☐ Transferências internacionais foram identificadas?
- ☐ Pequeno porte e dispensa de encarregado foram avaliados corretamente?

COMO PRIORIZAR

Comece por dados financeiros, autenticação, crianças, sensíveis, grande escala e fornecedores que concentram a operação.

CONCLUSÃO

LGPD é governança da operação, não coleção de documentos

Uma loja em conformidade não é aquela que apenas publica política de privacidade. É aquela que conhece seus fluxos, limita a coleta, controla acessos, contrata fornecedores com critério e consegue responder ao titular ou a um incidente.

A maturidade deve acompanhar novos canais, integrações, campanhas e produtos. Cada tecnologia adicionada pode alterar finalidades, destinatários e riscos.

PRÓXIMO PASSO

Mapeie um único fluxo do anúncio à entrega e transforme as lacunas em plano de ação com responsável, prioridade e prazo.

Fontes oficiais essenciais

- LGPD, atualizada pela Lei nº 15.352/2026.
- Resoluções CD/ANPD nº 2/2022, nº 15/2024 e nº 18/2024.

HSL DIREITO DIGITAL

Proteção jurídica para negócios orientados por dados

A HSL Direito Digital atua na proteção jurídica de empresas, profissionais e operações da economia digital. Integramos as dimensões contratual, regulatória, preventiva e contenciosa para oferecer soluções compatíveis com a realidade de quem vende e opera na internet.

COMO PODEMOS ATUAR

Adequação à LGPD • mapa de dados • políticas e cookies • contratos com operadores • resposta a titulares • incidentes • defesa em processos administrativos.

Se sua empresa precisa estruturar ou revisar a proteção de dados, a HSL Direito Digital pode analisar a operação e indicar os caminhos juridicamente adequados.

WHATSAPP

+55 45 99107-2115

E-MAIL

hsl@hsldireitodigital.com • resposta em até 1 dia útil

SITE

hsldireitodigital.com

INSTAGRAM

@hsldireitodigital

ATENDIMENTO

100% digital • atuação nacional

HSL DIREITO DIGITAL

Segurança jurídica para negócios digitais.