

CHECKLIST DE ADEQUAÇÃO À LGPD - LEI GERAL DE PROTEÇÃO DE DADOS

- () Existe uma política de privacidade? Ela está de acordo com a LGPD?
- () Os contratos já foram revisados e estão de acordo com a LGPD?
- () Sua empresa faz coleta, produção, recepção, classificação, utilização, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração de dados pessoais (nome, email, telefone, CPF, etc.)?
- () Foi realizado o mapeamento geral de todas as atividades que envolvem tratamentos de dados pessoais?
 - Quais dados são coletados?
 - Quando são coletados?
 - Por quem são coletados?
 - Por que são coletados?
 - Onde são armazenados?
 - Quando e como são excluídos?
- () Foi indicado um responsável, encarregado de proteção de dados?
- () As informações do responsável estão publicadas no website?
- () Foi feita uma avaliação se somente os dados estritamente necessários estão sendo tratados?
- () Quais medidas para garantir a transparência são tomadas? Existe registro em procedimento?
- () A empresa trata dados pessoais sensíveis (origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural)?
- () Se são tratados dados de crianças, é obtido o consentimento de ao menos um dos responsáveis?
- () Os usuários do site são informados sobre quais dados são coletados, de forma ativa ou passiva, ao entrar no site?
- () Os procedimentos de proteção dos dados estão documentados?
- () Dados pessoais são compartilhados com terceiros, como softwares de gestão, gateway de pagamento ou empresas parceiras?
- () Foi elaborada ou revisada a política interna, planos de resposta a incidentes e outros documentos sobre privacidade e proteção de dados pessoais?

- () Os dados são eliminados ao fim do tratamento?
- () Existe procedimento que determine por quanto tempo os dados serão armazenados?
- () Quando dados pessoais são utilizados, é obtido o consentimento?
- () Existe registro deste consentimento (escrito ou eletrônico)?
- () Caso o consentimento seja por escrito, está em uma cláusula destacada das demais cláusulas contratuais?
- () Existe procedimento para informar o titular no caso de mudança de finalidade do uso dos dados pessoais?
- () Existe procedimento para revogar o consentimento?
- () Existe canal facilitando a consulta dos dados pelo titular?
- () Existe canal para fornecer ao titular informações sobre seus direitos?
- () Existe log (registro) de quem acessou e/ou alterou dados pessoais?
- () O acesso aos dados pessoais é protegido, ou seja, só pessoas autorizadas podem ter acesso?
- () Existe procedimento de informação aos titulares caso haja vazamento dos dados?
- () O armazenamento dos dados é feito com criptografia ou outro método que garanta o seu sigilo?
- () Existem regras de boas práticas e de governança que estabeleçam as condições de organização, processos e procedimentos, normas de segurança, padrões técnicos?
- () Existem regras e obrigações específicas para os envolvidos no tratamento de dados, ações educativas, mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais?