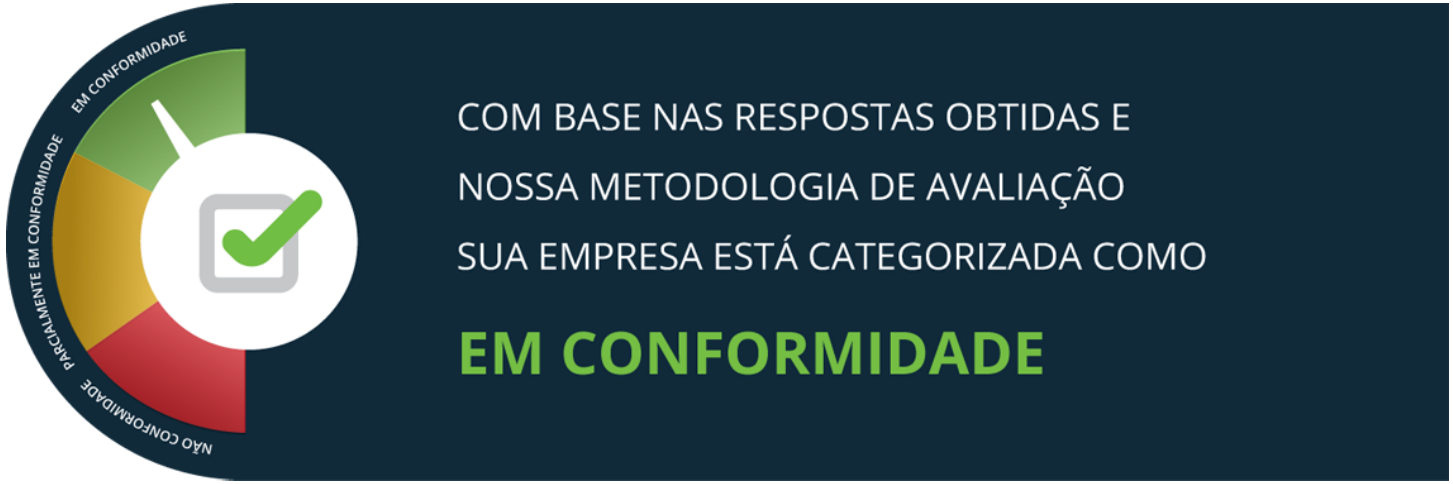
PREZADO USUÁRIO,

Obrigado por responder ao Diagnóstico LGPD!



COM UM RESULTADO DE **90%** DE CONFORMIDADE COM A LGPD COM BASE EM NOSSA METODOLOGIA.

Considerando o resultado obtido e as respostas enviadas, apresentamos abaixo nossas Recomendações para que sua empresa esteja em maior conformidade com a LGPD:

O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos por um dos pais ou pelo responsável legal.
Ainda, os controladores não deverão condicionar a participação de crianças em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

Elaborar uma Política de Retenção e Descarte de Dados. Esta política deve incluir os princípios de retenção e descarte apropriados de dados pessoais, observando os requisitos legais da LGPD. Além disso, a política deve conter:

- Uma tabela de temporalidade atualizada para armazenamento das informações levando em consideração os dados pessoais coletados;
- Procedimentos de descarte apropriado para ativos (papéis, computadores, mídias removíveis) que contenham dados pessoais;
- Processo de exclusão ou anonimização de dados quando estes não forem mais

necessários para a empresa, observando a necessidade de armazenamento de dados para atender obrigações legais;
- Processo de backup de dados pessoais armazenados em sistemas;
- Processo de pseudonimização para os dados sensíveis em repouso. Incorporar na cultura da empresa os princípios de minimização de dados, onde a empresa realiza a coleta apenas das informações estritamente necessárias, pelo período que for necessário.

Implementar um portal de privacidade (*front-end*) com uma solução de Gerenciamento dos Direitos dos Titulares de Dados com foco nos clientes da empresa, de forma tempestiva (15 dias para a LGPD). Esse portal gerenciará todo o *workflow* da solicitação e deve conter as seguintes funcionalidades:

- Formulário de preenchimento da solicitação, que pode ser apresentado em diversos produtos digitais da empresa;
- Validação da identidade dos titulares de dados;
- Controlar prazos, atividades e custos da solicitação;
- Identificar os dados pessoais dentro da empresa para proceder com a divulgação ao titular de dados, a correção, a exclusão ou portabilidade dos dados pessoais.

O portal também deve possuir materiais direcionados para o público externo informando como a empresa trata do tema de privacidade e proteção de dados, inclusive a política de privacidade contendo informações sobre direitos dos titulares, demonstrando as boas práticas adotadas para manter a proteção desses dados e os esforços da empresa em manter a conformidade com as leis de proteção de dados

pessoais.

Além disso, recomenda-se desenvolver modelos de respostas para solicitações de titulares de dados.

Definir um processo para avaliar se os dados transferidos internacionalmente pela empresa estão em conformidade com as leis de privacidade e proteção de dados, visando comprovar as medidas adotadas para cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na lei aos dados pessoais transferidos. Esse processo deve verificar se essa transferência atende aos requisitos definidos pela LGPD, tais como:

- Existência de cláusulas-padrão contratuais com os terceiros;
- Existência de normas corporativas globais definidas pela empresa;
- Existência de certificados, selos ou códigos de conduta regularmente emitidos e aprovados pela ANPD;
- Se o titular dos dados forneceu o devido consentimento;
- Para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado. A LGPD ainda não elaborou essa lista de países “seguros”, entretanto o GDPR já disponibilizou essa lista, conforme disponibilizado no seguinte link: (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)).

Além disso, sugerimos a revisão de contratos firmados com terceiros onde existe transferência internacional de dados pessoais para que sejam incluídas cláusulas padrão e termos voltados à privacidade e proteção de dados.

Estruturar, definir e formalizar um processo de Gestão de Incidentes, visando contemplar planos de resposta à incidentes relacionados ao tema de privacidade de dados. Esse plano deve conter procedimentos e diretrizes que orientem as áreas envolvidas na identificação, monitoramento, remediação e reporte de incidentes de violação de dados, bem como abordar a categorização de um incidente de violação de dados e o seu registro nas ferramentas. O processo de gestão de incidentes de violação deve ser testado e validado regularmente para avaliar a capacidade de atendimento aos requisitos de privacidade relevantes.

Recomenda-se que seja definido um processo de comunicação formal com as autoridades de proteção de dados e os titulares de dados. Essa comunicação deve ter o envolvimento do Encarregado de Dados (DPO) da empresa e deve ser realizada dentro dos prazos estabelecidos pela LGPD.

Além disso, deve-se ser estabelecido um processo de notificação de violação de dados que contenha:

- A identidade e o contato do encarregado de dados e outras partes relevantes da empresa;
- Descrição das possíveis consequências (riscos) da violação de dados;
- Descrição da natureza da violação, informando quais e a quantidade de titulares

que foram afetados;
- Medidas técnicas e organizacionais aplicadas para mitigar as consequências dessa violação.