RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 20 de junho de 2024

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Lanchonete da Esquina Ltda.

Operador(es): João da Silva, Maria Oliveira, José Santos

Encarregado: Escritório Silva & Almeida

E-mail do Encarregado: encarregado@silvaalmeida.com

Telefone: (11) 91234-5678

2 - NECESSIDADE DE ELABORAR O RELATÓRIO

Atendimento ao artigo 5º, inciso II, artigo 10, parágrafo 3º, artigo 14, artigo 42, todos da Lei 13.709/2018 - Lei Geral de Proteção de Dados.

3 - DESCRIÇÃO DO TRATAMENTO

Relativamente à natureza, escopo, contexto e finalidade do tratamento, a CONTROLADORA informa que, diante de sua atividade principal de prestação de serviços alimentícios, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

a) Coleta e trata dados pessoais relativos ao CPF, nome e e-mail do cliente para identificação no sistema de pedidos.
b) Coleta e trata dados pessoais relativos ao CPF e nome do cliente para fins de processamento de pagamento via QR Code do Mercado Pago.
c) Trata dados pessoais do cliente para acompanhamento e entrega dos pedidos, garantindo a comunicação eficiente do status do pedido.
d) Trata dados pessoais para fins de campanhas promocionais e marketing direto, com base no legítimo interesse do controlador.

Todos os dados são coletados e tratados no contexto da prestação de serviços alimentícios, com a finalidade de cumprir obrigações contratuais e garantir a satisfação do cliente.

4 - PARTES INTERESSADAS CONSULTADAS

1. Entidades legais consultadas:

a) - Escritório Silva & Almeida, representado por Alice F., especialista em direito digital e proteção de dados; Marcelo S., especialista em avaliação de segurança de dados pessoais no contexto da LGPD.
b) - Secretaria Estadual de Segurança de Dados.

2. Encarregado dos dados: conforme citado na seção 1.

3. Especialistas de segurança da CONTROLADORA: Ana P., Roberto M., Clara B.

4. Time de operação de negócio da CONTROLADORA: Lucas R., responsável pelo treinamento e acompanhamento do time em questões de segurança de dados e qualidade da operação.

Todas as partes interessadas participaram, em diferentes momentos, do processo de criação do presente documento. O time de operação de negócio participou na identificação dos dados operados, no apoio à definição do contexto de operação dos dados, e foi treinado para operar os dados de acordo com a política de dados definida. Os especialistas de segurança preparam os relatórios técnicos que serviram de base à criação da política de dados e a este relatório. O Encarregado dos dados, junto aos representantes jurídicos do CONTROLADOR, elaboraram este documento, que foi posteriormente validado com as entidades competentes.

5 - NECESSIDADE E PROPORCIONALIDADE

Fundamentação legal: artigo 5º, inciso II, artigo 10, parágrafo 3º, artigo 14, artigo 42, todos da Lei 13.709/2018 - Lei Geral de Proteção de Dados.

Tendo em vista que o legítimo interesse do CONTROLADOR é uma das fundamentações em razão de sua responsabilidade solidária ao TITULAR em caso de irregularidade fiscal e tributária:

- O tratamento dos dados pessoais é indispensável para a correta operação do sistema de pedidos, processamento de pagamentos e acompanhamento de entregas.

- Não há outra base legal possível de se utilizar para alcançar o mesmo propósito.

- O processo atual de fato auxilia no propósito almejado.

Todos os dados coletados com essa finalidade são eliminados após o período exigido pela legislação, que é de 5 (cinco) anos. Enquanto perdurar esse prazo, o encarregado manterá

todos os dados criptografados com chaves assimétricas, armazenados em dois fornecedores de nuvem diferentes, com segurança de nuvem e de implementação, e duplo fator de autenticação, inclusive para fins de recuperação de arquivos de segurança e recibos de transmissão e evidência de cumprimento de obrigação acessória e principal.

As informações de privacidade aos titulares seguem as diretrizes da obrigatoriedade de se manterem arquivadas todas as evidências fiscais, tributárias e trabalhistas de todas as informações enviadas aos sistemas oficiais da autoridade tributária brasileira.

A entidade CONTROLADORA poderá, a pedido do TITULAR, transferir a ele a guarda de tais informações, ressalvadas aquelas que o próprio CONTROLADOR, por dever de ofício, deve possuir pelo período constante da legislação.

É importante constar que não há, por legislação, a retroatividade do processamento dos dados, em caso de transferência de guarda de informações. Para fins legais, o direito ao esquecimento será garantido para os dados usados em processos transacionais.

6 - IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Identificamos os seguintes riscos, classificados de acordo com sua probabilidade (P) e seu impacto (I). O nível de risco se dá pela multiplicação dos dois fatores. As gradações são 5 (baixo), 10 (médio) e 15 (alto).

N do Risco	Especificação do Risco	P	I	Nível de Risco
R01	Acesso não autorizado	10	15	150
R02	Operação incorreta dos dados	5	15	75
R03	Desfiguração de dados por falha de software	5	10	50
R04	Indisponibilidade do sistema de operação dos dados	5	5	25

7 - MEDIDAS PARA TRATAR OS RISCOS

N Risco	Medida	Efeito sobre o risco	Medida aprovada
R01	1. Controle do acesso lógico 2. Monitoramento ativo de ações suspeitas no ambiente de operação	Reduzir	Sim
R02	1. Treinamento 2. Redução de dados para operação	Reduzir	Sim
R03	1. Efetuar testes completos e documentados antes de iniciar o uso	Mitigar	Sim
R04	1. Controle de failover para falhas que causem indisponibilidade 2. Monitoramento de todos os componentes da solução	Reduzir	Sim

8 - APROVAÇÃO

Assinaturas:

_____

Representante do CONTROLADOR

_____

Encarregado dos dados ou seu representante