RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 01 de julho de 2024

# 1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

**Controlador:** Lanchonete do bairro

**Operador(es):** TeamG11 Technology

**Encarregado:** Silva & Silva Advogados

**E-mail do Encarregado:** (lgpd@silvasadvogados.com)   
**Telefone:** (11) 93333-4444

# 2 - NECESSIDADE DE ELABORAR O RELATÓRIO

A elaboração deste relatório é essencial para demonstrar a conformidade da lanchonete do bairro com a Lei Geral de Proteção de Dados (LGPD), garantindo que todas as práticas de tratamento de dados estejam em conformidade com a legislação vigente. artigo 5o, inciso II, artigo 10, parágrafo 3o., artigo 14, artigo 42 todos da Lei 13.907/2018 - 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 produção e venda de lanches, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

1. coleta e trata dados pessoais e sensíveis relativos à documentação fiscal (CPF), bem como o nome completo do TITULAR, para identificação do TITULAR no contexto da empresa.
2. coleta e trata dados pessoais e sensíveis relativos à documentação fiscal (CPF) e nome completo do TITULAR, quando for identificado como cliente, e quando este efetuar uma compra através da loja física, para fins de efetuar a entrega do produto e efetuar a cobrança correta.
3. trata dados pessoais do TITULAR, seja este identificado como cliente no contexto do interesse legítimo do controlador em razão do histórico de pedidos na loja.
4. trata dados que podem causar danos patrimoniais ao TITULAR, quando este identificado como cliente, referente a sigilo fiscal, bancário e tributário, para efetuar pagamentos relativos a produção e vendas de lanches pela CONTROLADORA ao TITULAR.

Todos os dados são coletados e tratados no contexto de produção e vendas de lanches, com a finalidade do cumprimento de obrigações fiscais e tributárias, além de obrigações acessórias exigidas pela legislação brasileira.

# 4 - PARTES INTERESSADAS CONSULTADAS

1. Entidades legais consultadas
   1. Escritório Silva & Silva Advogados, representado por João, C., especialista em tributação no contexto da LGPD; Maria, C., especialista em avaliação de segurança de dados pessoais no contexto da LGPD;
   2. Secretaria Estadual de Segurança de Dados.
2. Encarregado dos dados, como citado na seção 1.
3. Especialistas de segurança da CONTROLADORA, notadamente: Otavio Costa.
4. Time de operação de negócio (e, por conseguinte, dos dados) da CONTROLADORA, representados por Lucas junior, 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 13.907/2018 - 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 sensíveis é indispensável ao cumprimento das exigências da legislação tributária e fiscal brasileira;
* 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 mediante solicitação do TITULAR via canal disponibilizado para tal. Enquanto os dados estiverem em posse da CONTROLADORA, 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 àquelas 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 | Vazamento de Dados Pessoais | 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 |
| R05 | Erro Humano no Cadastro de Dados | 15 | 5 | 75 |
| R06 | Uso Indevido dos Dados por Funcionários | 10 | 15 | 150 |

# 7 - MEDIDAS PARA TRATAR OS RISCOS

| Risco | Medida | Efeito sobre o risco | Medida aprovada |
| --- | --- | --- | --- |
| R01 | 1. Autenticação Forte (MFA);  2. monitoramento ativo de ações suspeitas no ambiente de operação;  3. Firewalls e IPS; 4. Políticas de Senha. | mitigar | sim |
| R02 | 1. Criptografia;  2.Controle de Acesso;  3. Monitoramento e Auditoria | mitigar | sim |
| R03 | 1. efetuar testes completos e documentados antes de iniciar o uso | mitigar | sim |
| R04 | 1. Backups Regulares;  2. Plano de Contingência;  3. Acordo de Nível de Serviço (SLA) | reduzir | sim |
| R05 | 1.Treinamento;  2. Validação de Dados;  3. Revisão Manual. | reduzir | sim |
| R06 | 1. Políticas de Uso;  2. Monitoramento de Acessos;  3. Sanções e Consequências | reduzir | sim |

# 8 - APROVAÇÃO

## Assinaturas:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Mario gomes   
Representante do CONTROLADOR

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

João da silva

Encarregado dos dados