RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 28 de agosto de 2024

# 1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

**Controlador:** EasyFood

**Operador(es):** Lucas Fernandes Lima, Luis Guilherme, Rafael Casadei, Rodrigo Lima

**Encarregado:** Lucas Fernandes Lima

**E-mail do Encarregado:** lucas.lima@email.com  
**Telefone:** (11) 91111-2222

# 2 - NECESSIDADE DE ELABORAR O RELATÓRIO

Atendimento ao 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 preparo e vendas de lanche, bebidas e outros produtos alimentícios, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

1. Coleta e trata dados pessoais do cliente, especificamente nome, email e CPF, para identificação do TITULAR no contexto do sistema de pedidos e emissão de comprovantes fiscais.
2. O nome e email do cliente é utilizado para a identificação durante o processo de atendimento, enquanto o CPF é coletado para fins de emissão de notas fiscais e para garantir o cumprimento das obrigações fiscais e tributárias da empresa.

Todos dados são coletados e tratados no contexto da prestação de serviços de alimentação, com a finalidade de garantir a precisão dos pedidos, 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 Moraes & Fernandes, representado por Lispector, C., especialista em tributação no contexto da LGPD; Meireles, 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: Joyce J.; Cervantes, M.; Mendes Campos, P.
4. Time de operação de negócio (e, por conseguinte, dos dados) da CONTROLADORA, representados por Sagan, C., 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 pessoais é indispensável ao cumprimento das exigências da legislação tributária e fiscal;
* 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 serão 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 e tributárias 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 | 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

| 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 da equipe  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