RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Porto Alegre, 1 de agosto de 2024

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Empresa Fiap Pos G53

Operador(es): Mauricio Holler Guntzel, Franklin Vinicius Silva de Moraes

Encarregado: Escritório Moraes & Guntzel

E-mail do Encarregado: (fiapg3@fiap.com)
Telefone: (51) 99999-0000

2 - NECESSIDADE DE ELABORAR O RELATÓRIO

Este relatório é elaborado em conformidade com os artigos 5º, inciso II, 10, parágrafo 3º, 14 e 42 da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD).

3 - DESCRIÇÃO DO TRATAMENTO

Considerando a natureza, escopo, contexto e finalidade do tratamento de dados, a CONTROLADORA informa que, devido à sua atividade principal de venda de alimentos e bebidas, bem como os fundamentos legais para a elaboração deste relatório, esclarece que:

a) **Coleta e tratamento de dados pessoais e sensíveis**: Inclui informações como documentação fiscal e regulatória, além de nome e data de nascimento do TITULAR, para identificação no contexto do restaurante, conforme os artigos 7º e 11 da LGPD.

b) **Coleta e tratamento de dados para entrega e cobrança**: Inclui CPF, endereço e nome do TITULAR ao realizar uma compra online, para fins de entrega do pedido e correta cobrança, conforme os artigos 7º, inciso V e 11, inciso II, alínea "a" da LGPD.

c) **Tratamento de dados para comunicação de informações fiscais**: Inclui dados pessoais do TITULAR, seja como cliente ou associado, no contexto do legítimo interesse do controlador para comunicação de dados fiscais às autoridades competentes, conforme o artigo 7º, inciso IX da LGPD.

d) **Tratamento de dados para pagamentos a associados**: Inclui informações que podem causar danos patrimoniais ao TITULAR, como sigilo fiscal, bancário e tributário, para efetuar pagamentos por serviços prestados, conforme os artigos 7º, inciso II e 11, inciso II, alínea "c" da LGPD.

e) **Tratamento de dados para recebimento de pagamentos**: Inclui informações que podem causar danos patrimoniais ao TITULAR, como sigilo fiscal, bancário e tributário, para receber pagamentos por produtos vendidos e/ou serviços prestados, conforme os artigos 7º, inciso II e 11, inciso II, alínea "c" da LGPD.

Todos os dados são coletados e tratados no contexto da prestação de serviços e venda de produtos, visando o cumprimento de obrigações fiscais e tributárias, além de obrigações acessórias exigidas pela legislação brasileira. Para mais informações, consulte este link.

4 - PARTES INTERESSADAS CONSULTADAS

1. **Consultoria jurídica**:
    - Escritório Moraes & Guntzel, representado por:
        - Guntzel, M., especialista em tributação no contexto da LGPD.
        - Moraes, F., especialista em segurança de dados pessoais no contexto da LGPD.
    - Secretaria Estadual de Segurança de Dados.
2. **Encarregado dos dados**: Conforme citado na seção 1, de acordo com o artigo 41 da LGPD.
3. **Especialistas de segurança da CONTROLADORA**:
    - Guntzel, M.
    - Moraes, F.
4. **Equipe operacional da CONTROLADORA**:
    - Moraes, F., responsável pelo treinamento e acompanhamento da equipe em questões de segurança de dados e qualidade da operação.

Todas as partes interessadas participaram em diferentes momentos da criação deste documento. A equipe operacional ajudou na identificação dos dados processados, na definição do contexto de operação e foi treinada para operar os dados conforme a política definida.

Os especialistas de segurança elaboraram relatórios técnicos que fundamentaram a criação da política de dados e deste relatório. O encarregado dos dados, junto aos representantes jurídicos do controlador, redigiram este documento, que foi posteriormente validado com as entidades competentes.

5 - NECESSIDADE E PROPORCIONALIDADE

Fundamentação legal: Artigos 5º, inciso II, 10, parágrafo 3º, 14 e 42 da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD).

O legítimo interesse do controlador é uma das fundamentações devido à sua responsabilidade solidária com o titular em caso de irregularidade fiscal e tributária:

- **Indispensabilidade do tratamento**: O tratamento de dados sensíveis é indispensável para o cumprimento das exigências da legislação tributária, fiscal e trabalhista brasileira, conforme os artigos 7º, inciso II e 11, inciso II, alínea "a" da LGPD.
- **Inexistência de alternativas**: Não há outra base legal possível para alcançar o mesmo objetivo, conforme determinado pela LGPD.
- **Eficiência do processo**: O processo atual é eficaz para alcançar o propósito desejado, conforme as boas práticas recomendadas pela Autoridade Nacional de Proteção de Dados (ANPD).

Todos os dados coletados para esta finalidade são eliminados após o período exigido pela legislação, que é de cinco anos, conforme o artigo 16 da LGPD. Durante esse período, o encarregado manterá todos os dados criptografados com chaves assimétricas, armazenados em dois fornecedores de nuvem diferentes, com segurança de nuvem e implementação, e duplo fator de autenticação, inclusive para recuperação de arquivos de segurança, recibos de transmissão e evidências de cumprimento de obrigações acessórias e principais.

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

A CONTROLADORA poderá, a pedido do titular, transferir a guarda dessas informações para ele, exceto aquelas que a própria CONTROLADORA, por dever de ofício, deve manter pelo período estipulado pela legislação, conforme os artigos 18 e 20 da LGPD.

É importante destacar que não há retroatividade no processamento dos dados em caso de transferência de guarda de informações. Para fins legais, o direito ao esquecimento será garantido para os dados utilizados em processos transacionais, conforme o artigo 18, inciso VI da LGPD.

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 é determinado 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
R05	Perda de dados	5	10	50

R06	Roubo de dados através de dispositivos físicos	10	10	100

7 - MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida	Efeito sobre o risco	Medida aprovada
R01	1. Implementar controles de acesso rigorosos. 2. Monitorar ativamente atividades suspeitas.	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
R03	1. Atualizar regularmente o software de segurança. 2. Realizar auditorias de segurança periódicas.	Reduzir	Sim
R05	1. Manter backups frequentes dos dados. 2. Implementar controles de acesso para o banco de dados.	Mitigar	Sim

R01	1. Estabelecer protocolos de resposta rápida a incidentes de segurança. 2. Realizar simulações de incidentes de segurança para preparar a equipe.	Reduzir	Sim
R1	1. Utilizar criptografia para dados sensíveis durante a transmissão e armazenamento. 2. Realizar avaliações de vulnerabilidade regularmente.	Reduzir	Sim
R06	1. Implementar políticas rigorosas de controle de acesso físico. 2. Utilizar criptografia em dispositivos móveis.	Reduzir	Sim

8 - APROVAÇÃO

Assinaturas:

_____

Representante do CONTROLADOR

_____

Encarregado dos dados ou seu representante