RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 30 de agosto de 2024

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Restaurante FIAP Tech Challenge by Fabiano Góes

Operador(es): Equipe de desenvolvimento de Software

Encarregado: Fabiano Góes

E-mail do Encarregado: (fabianogoes@gmail.com)
Telefone: (11) 98590-4071

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 **venda de lanches no formato fast food e a possibilidade de entrega em residência**, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

3.1 - DADOS DE CLIENTES

a) coleta e trata dados pessoais e sensíveis relativos à documentação fiscal e regulatória, bem como os dados pessoais nome, email e do TITULAR, para identificação do TITULAR no contexto do pedido, também o endereço em casos que o CLIENTE opte pela opção de delivery.

b) coleta e trata dados pessoais e sensíveis relativos à documentação fiscal (CPF), endereço e nome do TITULAR, quando for identificado como cliente, e quando este efetuar uma compra através da loja eletrônica, para fins de efetuar a entrega do produto e efetuar a cobrança correta.

c) trata dados pessoais do TITULAR, seja este identificado como cliente no contexto do interesse legítimo do controlador em razão de sua responsabilidade na comunicação de dados fiscais às autoridades competentes.

d) 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 serviços prestados pela CONTROLADORA ao TITULAR.

e) trata dados que podem causar danos patrimoniais ao TITULAR, quando este identificado como CLIENTE, referente a sigilo fiscal, bancário e tributário, para receber pagamentos relativos a produtos vendidos e/ou serviços prestados pela CONTROLADORA ao TITULAR.

3.2 - DADOS DE FUNCIONÁRIOS

a) **Dados coletados**: Nome, CPF, telefone e e-mail.
b) **Finalidade**: Gerenciamento de recursos humanos, comunicação interna, e cumprimento de obrigações trabalhistas.
c) **Base legal**: Execução de contrato e cumprimento de obrigação legal.

Todos dados são coletados e tratados no contexto da prestação de serviços e venda de produtos, com a finalidade do cumprimento de obrigações fiscais e tributárias, além de obrigações acessórias exigidas pela legislação brasileira. A título exemplificativo, porém não exaustivo, segue link das principais que envolvem dados do TITULAR - http://www.fiapfoodtechchallenge.com.br

4 - PARTES INTERESSADAS CONSULTADAS

1. Restaurante FIAP Tech Challenge by Fabiano Góes e equipe jurídica especializada em LGPD.
2. Encarregado dos dados, como citado na seção 1.
3. Especialistas de segurança da CONTROLADORA, notadamente: dra Grace Hopper..
4. Provedores de serviços de TI para hospedagem e manutenção do software.
5. Empresas de marketing digital para envio de e-mails promocionais e comunicação com clientes.

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, fiscal e trabalhista 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 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 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

Medidas de Segurança:

- Armazenamento seguro dos dados com criptografia.
- Controle de acesso restrito a funcionários autorizados.
- Implementação de autenticação multifator para acesso ao sistema que gerencia os dados.

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

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 2. redução de dados para operação	reduzir	sim
R03	1. efetuar testes completos e documentados antes de iniciar o uso	mitigar	sim

APROVAÇÃO

Assinaturas:

Representante do CONTROLADOR

Encarregado dos dados ou seu representante